
EnergySOAR Documentation

Release latest

Jan 05, 2024

CONTENTS

1	Overview	1
1.1	About	1
2	Energy SOAR installation guide	3
2.1	Install	3
3	Architecture	5
3.1	Logical architecture	5
4	Configuration	7
4.1	Cortex	7
4.2	TheHive	16
4.3	SSL	18
4.4	Change system language	18
5	User guide	19
5.1	Administration	19
5.2	Reports	25
5.3	Cases	27
5.4	Organisation	30
5.5	Reports	30
5.6	Workflows	30
6	Operations	55
7	Integrations	57
7.1	Responders	57
7.2	Analyzers	130
7.3	How to Write and Submit an Analyzer	310
7.4	Creating Your First Node	321
7.5	Energy Logserver SIEM	333
7.6	Microsoft Exchange	336
8	API	339
8.1	Base API Guide	339
8.2	Automation API Guide	354

OVERVIEW**1.1 About**

Energy SOAR will make your life not only easier but also safer. By connecting with security tools and by analyzing IP, URL, files and others elements, Energy SOAR will take significant place in your imagination about working in IT Security business.

[Read more](#)

1.1.1 Components

Components	Description
Case	A tool to organize information from multiple alerts.
Task	A piece of work assigned to an analyst.
Case template	Provides list of standard tasks that analyst can follow when evaluating cases.

ENERGY SOAR INSTALLATION GUIDE

2.1 Install

Supported OSes:

- Oracle Linux 8
- Red Hat Linux 8
- Centos Linux/Stream 8

Non-interactive

Warning: Run this command as root user in installation package directory

```
# ./install.sh -n
```

Non-interactive mode install this services by default:

- TheHive
- Cortex
- Elasticsearch 7
- Cassandra 4

After service installation it load some sample data.

- create sample users
- load analyzers template
- configure Cortex integration
- import MISP Taxonomies
- load sample Playbooks
- create Cortex database schema

Interactive

Warning: Run this command as root user in installation package directory

```
# ./install.sh -i
```

Minimal single node architecture services:

- TheHive
- Cortex
- Elasticsearch 7
- Cassandra 4

Example *interactive* installation

```
====> Do You wish to install the ENERGY SOAR TheHive, as well as the other TheHive_
↳dependencies? [y/n] y
[..]
====> Do You wish to install the ENERGY SOAR Cortex, as well as the other Cortex_
↳dependencies? [y/n] y
[..]
====> Do You wish to install the Cassandra 4? [y/n] y
[..]
====> Do You wish to install the Elasticsearch 7? [y/n] y
[..]
====> Do You wish to initialize Cortex data? [y/n] y
[..]
====> Do You wish to initialize TheHive data? [y/n] y
[..]
```

Note: Initialize Cortex data is needed to integrate with TheHive. During this step is created api user and configured in TheHive configuration.

Initialize TheHive data:

- import MISP Taxonomies
- create sample users
- create sample case/alert
- import Analyzer templates
- configure Cortex plugin

Table 1: Sample users

User	Password
<i>admin@energysoar.local</i>	secret
<i>socadmin@energysoar.local</i>	socadmin
<i>socuser@energysoar.local</i>	socuser
<i>socro@energysoar.local</i>	socro

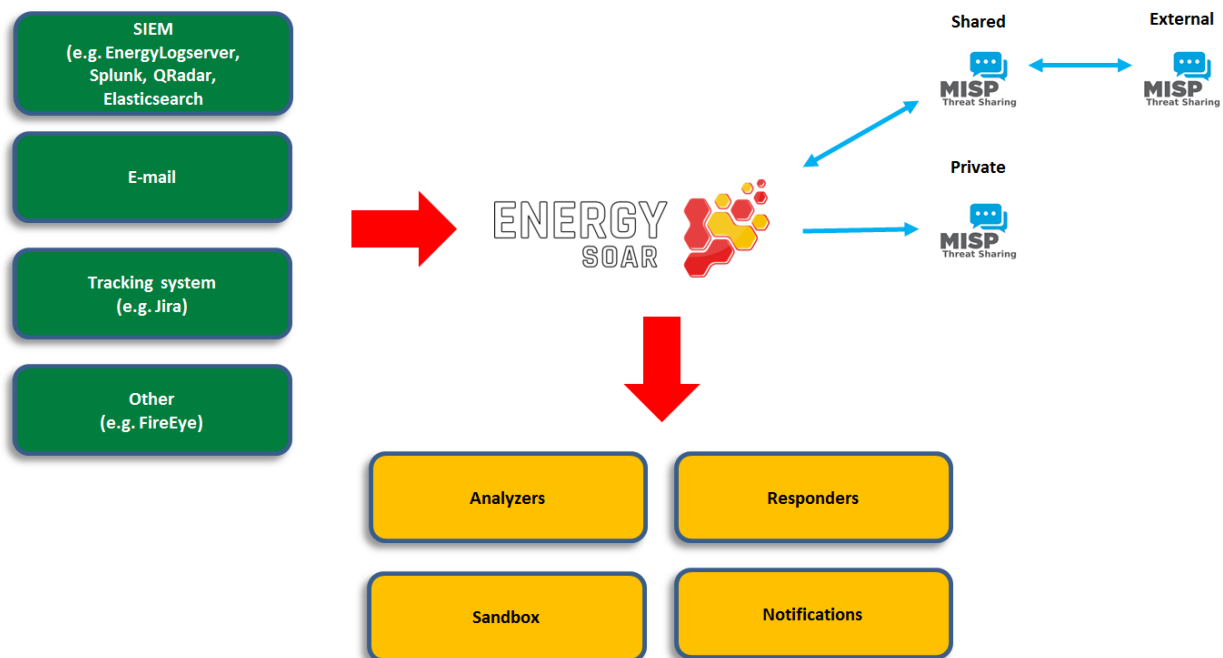
ARCHITECTURE

Energy SOAR is built from scallable services. Depending on the requirements, it is possible to create a cluster for high availability or high performance.

Additional services in case High avability architecture:

- Redis
- MySQL or Postgres 13+
- Min.io

3.1 Logical architecture



CONFIGURATION

4.1 Cortex

As described in the section above, Analyzers can only be configured using the Web interface and their associated configuration is stored in the underlying Elasticsearch database. However, the Cortex application configuration is stored in the `/etc/cortex/application.conf` file.

4.1.1 Database

Cortex relies on the Elasticsearch 7.x search engine to store all persistent data. Elasticsearch is not part of the Cortex package. It must be installed and configured as a standalone instance which can be located on the same machine.

Three settings are required to connect to Elasticsearch:

- the base name of the index
- the name of the cluster
- the address(es) and port(s) of the Elasticsearch instance

The default settings are:

```
### Elasticsearch
search {
  # Name of the index
  index = cortex
  # Name of the Elasticsearch cluster
  cluster = hive
  # Address of the Elasticsearch instance
  host = ["127.0.0.1:9300"]
  # Scroll keepalive
  keepalive = 1m
  # Size of the page for scroll
  pagesize = 50
  # Number of shards
  nbshards = 5
  # Number of replicas
  nbreplicas = 1
  # Arbitrary settings
  settings {
    # Maximum number of nested fields
    mapping.nested_fields.limit = 100
  }
}
```

(continues on next page)

(continued from previous page)

```

}

### XPack SSL configuration
# Username for XPack authentication
#user = ""
# Password for XPack authentication
#password = ""
# Enable SSL to connect to Elasticsearch
ssl.enabled = false
# Path to certificate authority file
#ssl.ca = ""
# Path to certificate file
#ssl.certificate = ""
# Path to key file
#ssl.key = ""

### SearchGuard configuration
# Path to JKS file containing client certificate
#guard.keyStore.path = ""
# Password of the keystore
#guard.keyStore.password = ""
# Path to JKS file containing certificate authorities
#guard.trustStore.path = ""
## Password of the truststore
#guard.trustStore.password = ""
# Enforce hostname verification
#guard.hostVerification = ""
# If hostname verification is enabled specify if hostname should be resolved
#guard.hostVerificationResolveHostname = ""
}

```

If you use a different configuration, please make sure to modify the parameters accordingly in the *application.conf* file.

If multiple Elasticsearch nodes are used as a cluster, addresses of the master nodes must be used for the *search.host* setting. All cluster nodes must use the same cluster name:

```

search {
  host = ["node1:9300", "node2:9300"]
}

```

Cortex uses the [TCP transport](https://www.elastic.co/guide/en/elasticsearch/reference/5.6/modules-network.html#_transport_and_http_protocols) port (9300/tcp by default). Cortex cannot use the HTTP transport as of this writing (9200/tcp).

Cortex creates specific index schema (mapping) versions in Elasticsearch. Version numbers are appended to the index base name (the 8th version of the schema uses the index *cortex_8* if *search.index = cortex*). When too many documents are requested, it uses the [scroll](<https://www.elastic.co/guide/en/elasticsearch/reference/5.6/search-request-scroll.html>) feature: the results are retrieved through pagination. You can specify the size of the page (*search.pagesize*) and how long pages are kept in Elasticsearch (*search.Keepalive*) before purging.

XPack and SearchGuard are optional and exclusive. If Cortex finds a valid configuration for XPack, SearchGuard configuration is ignored.

4.1.2 Analyzers and Responders

Cortex is able to run workers (analyzers and responders) installed locally or available as Docker image. Settings *analyzer.urls* and in *responder.urls* list paths or urls where Cortex looks for analyzers and responders. These settings accept: 1. a path to a directory that Cortex scans to locate workers 1. a path or an URL to a JSON file containing a JSON array of worker definitions

Worker definition is a JSON object that describe the worker, how to configure it and how to run it. If it contains a field “command”, worker can be run using process runner (i.e. the command is executed). If it contains a field “dockerImage”, worker can be run using docker runner (i.e. a container based on this image is started). If it contains both, the runner is chosen according to *job.runners* settings (*[docker, process]* by default).

For security reason, if worker definitions fetched from remote url (http/https) contain command, they are ignored.

You can control the number of simultaneous jobs that Cortex executes in parallel using the *analyzer.fork-join-executor* configuration item. The value depends on the number of CPU cores (*parallelism-factor* * nbCores), with a minimum (*parallelism-min*) and a maximum (*parallelism-max*).

Similar settings can also be applied to responders.

```
analyzer {
  # Directory that holds analyzers
  urls = [
    "/path/to/default/analyzers",
    "/path/to/my/own/analyzers"
  ]

  fork-join-executor {
    # Min number of threads available for analyze
    parallelism-min = 2
    # Parallelism (threads) ... ceil(available processors * factor)
    parallelism-factor = 2.0
    # Max number of threads available for analyze
    parallelism-max = 4
  }
}

responder {
  # Directory that holds responders
  urls = [
    "/path/to/default/responders",
    "/path/to/my/own/responders"
  ]

  fork-join-executor {
    # Min number of threads available for analyze
    parallelism-min = 2
    # Parallelism (threads) ... ceil(available processors * factor)
    parallelism-factor = 2.0
    # Max number of threads available for analyze
    parallelism-max = 4
  }
}
```

4.1.3 Authentication

Like TheHive, Cortex supports local, LDAP, Active Directory (AD), X.509 SSO and/or API keys for authentication and OAuth2.

Please note that API keys can only be used to interact with the Cortex API (for example when TheHive is interfaced with a Cortex instance, it must use an API key to authenticate to it). API keys cannot be used to authenticate to the Web UI. By default, Cortex relies on local credentials stored in Elasticsearch.

Authentication methods are stored in the *auth.provider* parameter, which is multi-valued. When a user logs in, each authentication method is tried in order until one succeeds. If no authentication method works, an error is returned and the user cannot log in.

The default values within the configuration file are:

```
auth {
    # "provider" parameter contains authentication provider. It can be multi-valued.
    ↪(useful for migration)
    # available auth types are:
    # services.LocalAuthSrv : passwords are stored in user entity (in Elasticsearch). No
    ↪configuration is required.
    # ad : use ActiveDirectory to authenticate users. Configuration is under "auth.ad"
    ↪key
    # ldap : use LDAP to authenticate users. Configuration is under "auth.ldap" key
    # oauth2 : use OAuth/OIDC to authenticate users. Configuration is under "auth.oauth2
    ↪" and "auth.sso" keys
    provider = [local]

    # By default, basic authentication is disabled. You can enable it by setting "method.
    ↪basic" to true.
    method.basic = false

    ad {
        # The name of the Microsoft Windows domain using the DNS format. This parameter
        ↪is required.
        #domainFQDN = "mydomain.local"

        # Optionally you can specify the host names of the domain controllers. If not
        ↪set, Cortex uses "domainFQDN".
        #serverNames = [ad1.mydomain.local, ad2.mydomain.local]

        # The Microsoft Windows domain name using the short format. This parameter is
        ↪required.
        #domainName = "MYDOMAIN"

        # Use SSL to connect to the domain controller(s).
        #useSSL = true
    }

    ldap {
        # LDAP server name or address. Port can be specified (host:port). This parameter
        ↪is required.
        #serverName = "ldap.mydomain.local:389"

        # If you have multiple ldap servers, use the multi-valued settings.
```

(continues on next page)

(continued from previous page)

```

#serverNames = [ldap1.mydomain.local, ldap2.mydomain.local]

# Use SSL to connect to directory server
#useSSL = true

# Account to use to bind on LDAP server. This parameter is required.
#bindDN = "cn=cortex,ou=services,dc=mydomain,dc=local"

# Password of the binding account. This parameter is required.
#bindPW = "****secret*password****"

# Base DN to search users. This parameter is required.
#baseDN = "ou=users,dc=mydomain,dc=local"

# Filter to search user {0} is replaced by user name. This parameter is required.
#filter = "(cn={0})"
}

oauth2 {
  # URL of the authorization server
  #clientId = "client-id"
  #clientSecret = "client-secret"
  #redirectUri = "https://my-cortex-instance.example/api/ssoLogin"
  #responseType = "code"
  #grantType = "authorization_code"

  # URL from where to get the access token
  #authorizationUrl = "https://auth-site.com/OAuth/Authorize"
  #tokenUrl = "https://auth-site.com/OAuth/Token"

  # The endpoint from which to obtain user details using the OAuth token, after
  ↪successful login
  #userUrl = "https://auth-site.com/api/User"
  #scope = ["openid profile"]
}

# Single-Sign On
sso {
  # Autocreate user in database?
  #autocreate = false

  # Autoupdate its profile and roles?
  #autoupdate = false

  # Autologin user using SSO?
  #autologin = false

  # Name of mapping class from user resource to backend user ('simple' or 'group')
  #mapper = group
  #attributes {
  #  login = "user"
  #  name = "name"

```

(continues on next page)

(continued from previous page)

```

# groups = "groups"
# organization = "org"
#}
#defaultRoles = ["read"]
#defaultOrganization = "csirt"
#groups {
# # URL to retrieve groups (leave empty if you are using OIDC)
# #url = "https://auth-site.com/api/Groups"
# # Group mappings, you can have multiple roles for each group: they are merged
# mappings {
#   admin-profile-name = ["admin"]
#   editor-profile-name = ["write"]
#   reader-profile-name = ["read"]
# }
#}

#mapper = simple
#attributes {
# login = "user"
# name = "name"
# roles = "roles"
# organization = "org"
#}
#defaultRoles = ["read"]
#defaultOrganization = "csirt"
}
}

### Maximum time between two requests without requesting authentication
session {
  warning = 5m
  inactivity = 1h
}

```

4.1.4 OAuth2/OpenID Connect

To enable authentication using OAuth2/OpenID Connect, edit the *application.conf* file and supply the values of *auth.oauth2* according to your environment. In addition, you need to supply:

- *auth.sso.attributes.login*: name of the attribute containing the OAuth2 user's login in retrieved user info (mandatory)
- *auth.sso.attributes.name*: name of the attribute containing the OAuth2 user's name in retrieved user info (mandatory)
- *auth.sso.attributes.groups*: name of the attribute containing the OAuth2 user's groups (mandatory using groups mappings)
- *auth.sso.attributes.roles*: name of the attribute containing the OAuth2 user's roles in retrieved user info (mandatory using simple mapping)

Important notes

Authenticate the user using an external OAuth2 authenticator server. The configuration is:

- `clientId` (string) client ID in the OAuth2 server.
- `clientSecret` (string) client secret in the OAuth2 server.
- `redirectUri` (string) the url of TheHive OAuth2 page (`.../api/ssoLogin`).
- `responseType` (string) type of the response. Currently only “code” is accepted.
- `grantType` (string) type of the grant. Currently only “authorization_code” is accepted.
- `authorizationUrl` (string) the url of the OAuth2 server.
- `authorizationHeader` (string) prefix of the authorization header to get user info: Bearer, token, ...
- `tokenUrl` (string) the token url of the OAuth2 server.
- `userUrl` (string) the url to get user information in OAuth2 server.
- `scope` (list of string) list of scope.

Example

```
auth {

  provider = [local, oauth2]

  [...]

  sso {
    autcreate: false
    autoupdate: false
    mapper: "simple"
    attributes {
      login: "login"
      name: "name"
      roles: "role"
    }
    defaultRoles: ["read", "analyze"]
    defaultOrganization: "demo"
  }
  oauth2 {
    name: oauth2
    clientId: "Client_ID"
    clientSecret: "Client_ID"
    redirectUri: "http://localhost:9001/api/ssoLogin"
    responseType: code
    grantType: "authorization_code"
    authorizationUrl: "https://github.com/login/oauth/authorize"
    authorizationHeader: "token"
    tokenUrl: "https://github.com/login/oauth/access_token"
    userUrl: "https://api.github.com/user"
    scope: ["user"]
  }
}

[...]
```

4.1.5 Performance

In order to increase Cortex performance, a cache is configured to prevent repetitive database solicitation. Cache retention time can be configured for users and organizations (default is 5 minutes). If a user is updated, the cache is automatically invalidated.

4.1.6 Analyzer Results

Analyzer results (job reports) can also be cached. If an analyzer is executed against the same observable, the previous report can be returned without re-executing the analyzer. The cache is used only if the second job occurs within *cache.job* (the default is 10 minutes).

```
cache {  
  job = 10 minutes  
  user = 5 minutes  
  organization = 5 minutes  
}
```

Note: The global *cache.job* value can be overridden for each analyzer in the analyzer configuration Web dialog.

Note: It is possible to bypass the cache altogether (for example to get extra fresh results) through the API as explained in the [API Guide](#) or by setting the cache to *Custom* in the Cortex UI for each analyzer and specifying 0 as the number of minutes.

4.1.7 Streaming (a.k.a The Flow)

The user interface is automatically updated when data is changed in the back-end. To do this, the back-end sends events to all the connected front-ends. The mechanism used to notify the front-end is called long polling and its settings are:

- *refresh* : when there is no notification, close the connection after this

duration (the default is 1 minute). * *cache* : before polling a session must be created, in order to make sure no event is lost between two polls. If there is no poll during the cache setting, the session is destroyed (the default is 15 minutes). * *nextItemMaxWait*, *globalMaxWait* : when an event occurs, it is not immediately sent to the front-ends. The back-end waits *nextItemMaxWait* and up to *globalMaxWait* in case another event can be included in the notification. This mechanism saves many HTTP requests.

The default values are:

```
### Streaming  
stream.longpolling {  
  # Maximum time a stream request waits for new element  
  refresh = 1m  
  # Lifetime of the stream session without request  
  cache = 15m  
  nextItemMaxWait = 500ms  
  globalMaxWait = 1s  
}
```

4.1.8 Entity Size Limit

The Play framework used by Cortex sets the HTTP body size limit to 100KB by default for textual content (json, xml, text, form data) and 10MB for file uploads. This could be too small in some cases so you may want to change it with the following settings in the *application.conf* file:

```
### Max textual content length
play.http.parser.maxMemoryBuffer=1M
### Max file size
play.http.parser.maxDiskBuffer=1G
```

Note: If you are using a NGINX reverse proxy in front of Cortex, be aware that it doesn't distinguish between text data and a file upload. So, you should also set the *client_max_body_size* parameter in your NGINX server configuration to the highest value among the two: file upload and text size as defined in Cortex *application.conf* file.

4.1.9 HTTPS

Enable HTTPS directly on Cortex is not supported anymore. You must install a reverse proxy in front of Cortex. Below an example of NGINX configuration:

```
server {
    listen 443 ssl;
    server_name cortex.example.com;

    ssl_certificate      ssl/cortex_cert.pem;
    ssl_certificate_key  ssl/cortex_key.pem;

    proxy_connect_timeout 600;
    proxy_send_timeout    600;
    proxy_read_timeout    600;
    send_timeout          600;
    client_max_body_size  2G;
    proxy_buffering off;
    client_header_buffer_size 8k;

    location / {
        add_header Strict-Transport-Security "max-age=31536000;␣
↪includeSubDomains";
        proxy_pass http://127.0.0.1:9001/;
        proxy_http_version 1.1;
        proxy_set_header Connection "";
    }
}
```

4.2 TheHive

4.2.1 *secret.conf* file

This file contains a secret that is used to define cookies used to manage the users session. As a result, one instance of TheHive should use a unique secret key.

Example

```
## Play secret key
play.http.secret.key="dgngu325mbnbc39cxas415kb24503836y2vsvsg465989fbsvop9d09ds6df6"
```

Warning: In the case of a cluster of Energy SOAR nodes, all nodes should have the same *secret.conf* file with the same secret key. The secret is used to generate user sessions.

4.2.2 License

License path

License path is set in configuration file `/etc/thehive/application.conf.d/license.conf`. By default it is `license.path: "/etc/thehive/"`.

4.2.3 Listen address & port

By default the application listens on all interfaces and port 9000. This is possible to specify listen address and ports with following parameters in the *application.conf* file:

```
http.address=127.0.0.1
http.port=9000
```

4.2.4 Context

If you are using a reverse proxy, and you want to specify a location (ex: `/thehive`), updating the configuration of TheHive is also required

Example

```
play.http.context: "/thehive"
```

4.2.5 Specific configuration for streams

If you are using a reverse proxy like Nginx, you might receive error popups with the following message: *StreamSrv 504 Gateway Time-Out*.

You need to change default setting for long polling refresh, Set *stream.longPolling.refresh* accordingly.

Example

```
stream.longPolling.refresh: 45 seconds
```

4.2.6 Manage content length

Content length of text and files managed by the application are limited by default.

These values are set with default parameters:

```
# Max file size
play.http.parser.maxDiskBuffer: 128MB
```

```
# Max textual content length
play.http.parser.maxMemoryBuffer: 256kB
```

If you feel that these should be updated, edit `/etc/thehive/application.conf` file and update these parameters accordingly.

Tip: If you are using a NGINX reverse proxy in front of Energy SOAR, be aware that it doesn't distinguish between text data and a file upload.

So, you should also set the `client_max_body_size` parameter in your NGINX server configuration to the highest value among the two: file upload and text size defined in TheHive `application.conf` file.

4.2.7 Manage configuration files

Energy SOAR uses HOCON as configuration file format. This format gives enough flexibility to structure and organise the configuration of Energy SOAR.

TheHive is delivered with following files, in the folder `/etc/thehive`:

`logback.xml` containing the log policy

`secret.conf` containing a secret key used to create sessions. This key should be unique per instance (in the case of a cluster, this key should be the same for all nodes of this cluster) `application.conf`

HOCON file format let you organise the configuration to have separate files for each purpose. It is possible to create a `/etc/thehive/application.conf.d` folder and have several files inside that will be included in the main file `/etc/thehive/application.conf`.

At the end, the following configuration structure is possible:

```
/etc/thehive
|-- application.conf
|-- application.conf.d
|   |-- secret.conf
|   |-- service.conf
|   |-- database.conf
|   |-- storage.conf
|   |-- cluster.conf
|   |-- authentication.conf
|   |-- cortex.conf
|   |-- misp.conf
|   |-- webhooks.conf
|-- logback.xml
```

And the content of `/etc/thehive/application.conf`:

```
## Include Play secret key
# More information on secret key at https://www.playframework.com/documentation/2.8.x/
↳ ApplicationSecret
include "/etc/thehive/application.conf.d/secret.conf"

## Service
include "/etc/thehive/application.conf.d/service.conf"

## Database
include "/etc/thehive/application.conf.d/database.conf"

## Storage
include "/etc/thehive/application.conf.d/storage.conf"

## Cluster
include "/etc/thehive/application.conf.d/cluster.conf"

## Authentication
include "/etc/thehive/application.conf.d/authentication.conf"

## Cortex
include "/etc/thehive/application.conf.d/cortex.conf"

## MISP
include "/etc/thehive/application.conf.d/misp.conf"

## Webhooks
include "/etc/thehive/application.conf.d/webhooks.conf"
```

4.3 SSL

Energy SOAR instalation script create self-signed certificates. Those certificates are stored under `/etc/thehive/ssl/` directory.

You can setup your own path in `/etc/nginx/conf.d/energysoar.conf`.

```
ssl_certificate      /etc/thehive/ssl/nginx-selfsigned.crt;
ssl_certificate_key  /etc/thehive/ssl/nginx-selfsigned.key;
```

4.4 Change system language

To change a system language you need override provided jar files.

```
cp -R EnergySOAR_*/jar/* /opt
```

To get your language pack please [contact with us](#).

5.1 Administration

5.1.1 Manage analyzer template

Energy SOAR will display the analysis summary the same way for all analyzers: display a tag using taxonomies and level color.

List analyzer templates

The management page is accessible from the header menu through the Admin > Analyzer templates menu and required a use with the `manageAnalyzerTemplate` permission (refer to Profiles and permissions).

Analyzer template management

[Import templates](#)

Download the official templates archive
You can download the latest archive of the official analyzer templates [from here](#)

Name	Long template
AbuseIPDB_1_0 Determine whether an IP was reported or not as malicious by AbuseIPDB	Default template
CIRCLPassiveDNS_2_0 Check CIRCL's Passive DNS for a given domain or URL.	Default template
CIRCLPassiveSSL_2_0 Check CIRCL's Passive SSL for a given IP address or a X509 certificate hash.	Default template
DShield_lookup_1_0 Query the SANS ISC DShield API to check for an IP address reputation.	Default template
EmergingThreats_IPInfo_1_0 Retrieve ET reputation, related malware, and IDS requests for a given IP address.	Default template
EmlParser_1_2 Parse Eml message	Default template
FileInfo_7_0 Parse files in several formats such as OLE and OpenXML to detect VBA macros, extract their source code, generate useful information on PE, PDF files...	Default template
GreyNoise_2_3 Determine whether an IP has known scanning activity using GreyNoise.	Default template
Hashdd_Detail_1_0	Default template

Analyzer templates are still customisable via the UI and can also be imported.

5.1.2 User Profiles management

Permissions

A Profile is a set of permissions attached to a User and an Organisation. It defines what the user can do on an object hold by the organisation. Energy SOAR has a finite list of permissions:

- `manageOrganisation (1)` : the user can create, update an organisation
- `manageConfig (1)`: the user can update configuration
- `manageProfile (1)`: the user can create, update and delete profiles
- `manageTag (1)`: the user can create, update and delete tags

- `manageCustomField` (1): the user can create, update and delete custom fields
- `manageCase`: the user can create, update and delete cases
- `manageObservable`: the user can create, update and delete observables
- `manageAlert`: the user can create, update and import alerts
- `manageUser`: the user can create, update and delete users
- `manageCaseTemplate`: the user can create, update and delete case template
- `manageTask`: the user can create, update and delete tasks
- `manageShare`: the user can share case, task and observable with other organisation
- `manageAnalyse` (2): the user can execute analyse
- `manageAction` (2): the user can execute actions
- `manageAnalyzerTemplate` (2): the user can create, update and delete analyzer template (previously named report template)
- `manageWorkflows`: the user can create, update and delete workflows
- `listWorkflows`: the user can see a list of workflows
- `viewWorkflows`: the user can see workflow details
- `manageReports`: the user can create, update and delete reports
- `listReports`: the user can see a list of reports

(1) Organisations, configuration, profiles and tags are global objects. The related permissions are effective only on “admin” organisation. (2) Actions, analysis and template is available only if Energy SOAR Automation connector is enabled

NOTE

Read information doesn’t require specific permission. By default, users in an organisation can see all data shared with that organisation (cf. shares, discussed in Organisations,Users and sharing).

Profiles

We distinguish two types of profiles:

- Administration Profiles
- Organisation Profiles

The management page is accessible from the header menu through the Admin > Profiles menu and required a use with the `manageProfile` permission (refer to the section above).

Energy SOAR comes with default profiles but they can be updated and removed (if not used). New profiles can be created.

ENERGY SOAR

Admin DAU admin/Default admin user

List of profiles

[+ New Profile](#)

Name	Permissions	
admin	manageAnalyzerTemplate, manageConfig, manageCustomField, manageObservableTemplate, manageOrganisation, managePattern, managePlatform, manageProfile, manageTaxonomy, manageUser	
analyst	accessTheHiveFS, manageAction, manageAlert, manageAnalyse, manageCase, manageObservable, managePlugins, manageShare, manageTag, manageTask, manageWorkfolws, viewWorkflows	Edit Delete
full-org-admin	accessTheHiveFS, manageAction, manageAlert, manageAnalyse, manageCase, manageCaseTemplate, manageObservable, managePlugins, manageShare, manageTag, manageTask, manageUser, manageWorkfolws, viewWorkflows	Edit Delete
org-admin	accessTheHiveFS, manageAction, manageAlert, manageAnalyse, manageCase, manageCaseTemplate, manageConfig, manageObservable, managePage, manageProcedure, manageShare, manageTag, manageTask, manageUser	
power_analyst	accessTheHiveFS, manageAction, manageAlert, manageAnalyse, manageCase, manageCaseTemplate, manageObservable, managePlugins, manageShare, manageTag, manageTask, manageUser, manageWorkfolws, viewWorkflows	Edit Delete
read-only	No permissions	Edit Delete

Once the New Profile button is clicked, a dialog is opened asking for the profile type, a name for the profile and a selection of permissions. Multiple selection can be made using CTRL+click.

ENERGY SOAR

Admin DAU admin/Default admin user

Add profile

Profile type * Administration Profile Organisation Profile

Permissions for organisation user profiles

Name *

Permissions *

- Manage users
- Manage case templates
- Manage custom tags
- Manage alert
- Manage case
- Manage sharing
- Manage observables
- Manage tasks
- Run Cortex responders
- Run Cortex analyzer
- Access to TheHiveFS service
- Manage plugins
- Manage workflows
- View workflows

Selected (0)

Cancel * Required field Save profile

List of profiles

+ New Profile

Name	Permissions	Actions
admin		Edit Delete
analyst		Edit Delete
full-org-admin		Edit Delete
org-admin		Edit Delete
power_analyst		Edit Delete
read-only	No permissions	Edit Delete

If it is used, a profile can't be remove but can be updated.

Default profiles are:

- admin: can manage all global objects and users. Can't create case.
- analyst: can manage cases and other related objects (observables, tasks, ...), including shring them
- org-admin: all permissions except those related to global objects
- read-only: no permission

Observable types

You can edit observable types in the administrator panel.

ENERGY SOAR

Admin DAU admin/Default admin u

Observable types management

Specify the datatype to add. Ex: domain, ip, email [Add dataType](#)

dataType	Action
autonomous-system	
domain	
file	
filename	
fqdn	
hash	
hostname	
ip	
mail	
mail-subject	
other	
regexp	
registry	
uri_path	
url	
user-agent	

Admin > Observable

5.1.3 Kill user session

Everytime you can manage logged user sessions as admin user. In organizations administration page you can kill user session. This user will be immediatelly logout.

Name ⬆

admin

organisation for administration

Linked organisations: *None*

SOC

SOC

Linked organisations: *None*

Select user organization

User List (3 of 3)

Status	Login ⬆	Full Name ⬆	Profile ⬆	Password	API Key	MFA	Dates C. ⬆ U. ⬆
Active	socadmin@energysoar.local	socadmin	org-admin	Edit password	Create API Key	No	C. 02/07/22 11:26
Active	socro@energysoar.local	socro	read-only	Edit password	Create API Key	No	C. 02/07/22 11:26
Active	socuser@energysoar.local	socuser	analyst	Edit password	Create API Key	No	C. 02/07/22 11:26

And click “Kill session” button.

5.2 Reports

5.2.1 Create and edit

Go to Reports on top menu

Click Create new report on the left

Create new Report

Now you can see New Report view.

New Report

Select dashboard *

SOC

Schedule *

Run once

Send Email *

☐

Select dashboard: there you should select existing dashboard.

Schedule types:

- Run once
- Daily
- Weekly
- Monthly
- Cron format (UNIX cron format)

Send Email: select if you would like to receive report on e-mail.

5.2.2 List

On reports list you see all created reports.

Status	Enabled	Dashboard	Schedule	Send Email	Owned By	Dates C. U.	
Report generated	true	SOC	Run once	false	S SOC/SOC	C. 01/26/22 10:16	<input type="button" value="Disable"/> <input type="button" value="Edit"/> <input type="button" value="Download"/> <input type="button" value="Delete"/>

Reports statuses:

- Created: Going to create the report
- Generated: Report was generated and you can download or it was sent
- Error: An error occurs. Please check logs

Actions:

- Enable/Disable
- Edit
- Download
- Delete

5.3 Cases

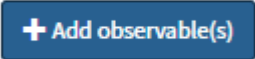
5.3.1 Observables

Observables are pieces of information added to a case.

How to add observables into Case

Perform the following steps to add an observable:

1. Click Add observable(s) button:

A blue rectangular button with rounded corners. It contains a white plus sign followed by the text "Add observable(s)" in white.

Create new observable(s)

Type * ip ▾

Value * 81.169.146.181
101.32.192.174

☒ One observable per line (2 unique observables)
☐ One single multiline observable

TLP * WHITE GREEN **AMBER** RED

Is IOC ☆

Has been sighted ☐

Ignore for similarity ☐

Tags ** Add tags

Description ** Observable(s) description

* Required field

Cancel

2. Create new observable(s) window appears:

3. Select type e.g. ip, domain, url, mail. If you choose file type, you can upload a file. Zipped archives are supported.

Type * file ▾

File * Drop file or click

☐ The file is a zipped archive

4. You can add one single observables or many observables at once - one observable per line.

5. Select appropriate TLP flag.

6. (Optional) IOC flag indicates observables classified as True Positive. Only IOC-flagged observables are exported to MISP instances.

7. (Optional) You can also set “Has been sighted” toggle to mark observables which have been seen.



















8. (Optional) If you click “Ignore for similarity”, you will disable “Observable seen in other cases” list.

9. Add tags and/or description.

10. Click Create observable(s). On Observable List you can check if observables have been seen in other cases:

- Black eye: Observable seen in other cases,
- Red eye: Observable seen in other cases and flagged as IOC there.

Observable List (3 of 3)

<input type="checkbox"/>	Flags	Type ↕	Value/Filename ↕
<input type="checkbox"/>	   	file	order[.]pdf  None  No reports available
<input type="checkbox"/>	   	ip	101[.]32[.]192[.]174  None  No reports available
<input type="checkbox"/>	   	ip	81[.]169[.]146[.]181  None  No reports available

You can display details and check cases where the observable has been seen:

[IP]: 101[.]32[.]192[.]174

 No reports available

Basic Information

 Sharing

 Responders

Links

TLP

TLP:AMBER

Date added

08/20/21 15:00

Is IOC



Has been sighted



Ignored for similarity















Tags

Not Specified

Description

phishtank

Observable seen in 4 other case(s)

Flags	Case	Date added
  	#38 - Strange email from ACME	07/23/21 14:34
  	#19 - Strange email from ACME	07/06/21 10:42
  	#20 - Strange email	07/06/21 10:48
  	#14 - Malicious URL Request Attempt	08/11/21 08:19

[FILE]: *order.pdf*

⚙️ *No reports available*

Basic Information

TLP

TLP:AMBER

Hash

SHA256: baae041b0282bc59f0d1bfb60b14

SHA1: 4e656cf7a0ae44b5ff93d0954bc412f

MD5: 36dd061dc6da24d9b11d58cdaa977c

After uploading file-type observables hashes are automatically calculated:

If you want to download file observable, it will be zipped and password protected:



Zip are protected with password "malware"

You can run various analyzers (e.g. VirusTotal, MaxMind_GeoIP) and responders (e.g. block IP, domain, e-mail) against observables.

5.4 Organisation

5.5 Reports

5.6 Workflows

SOC analysts have to handle many repetitive tasks. With Energy SOAR you can build workflows to automatically execute all relevant actions.

Workflows helps you to interconnect different apps with an API with each other to share and manipulate its data without a single line of code. It is an easy to use, user-friendly and highly customizable module, which uses an intuitive user interface for you to design your unique scenarios very fast. A workflow is a collection of nodes connected together to automate a process. A workflow can be started manually (with the Start node) or by Trigger nodes. When a workflow is started, it executes all the active and connected nodes. The workflow execution ends when all the nodes have processed their data. You can view your workflow executions in the Execution log, which can be helpful for debugging.

Activating a workflow Workflows that start with a Trigger node or a Webhook node need to be activated in order to be executed. This is done via the Active toggle in the Workflow UI. Active workflows enable the Trigger and Webhook nodes to receive data whenever a condition is met (e.g., Monday at 10:00, an update in a Trello board) and in turn trigger the workflow execution. All the newly created workflows are deactivated by default.

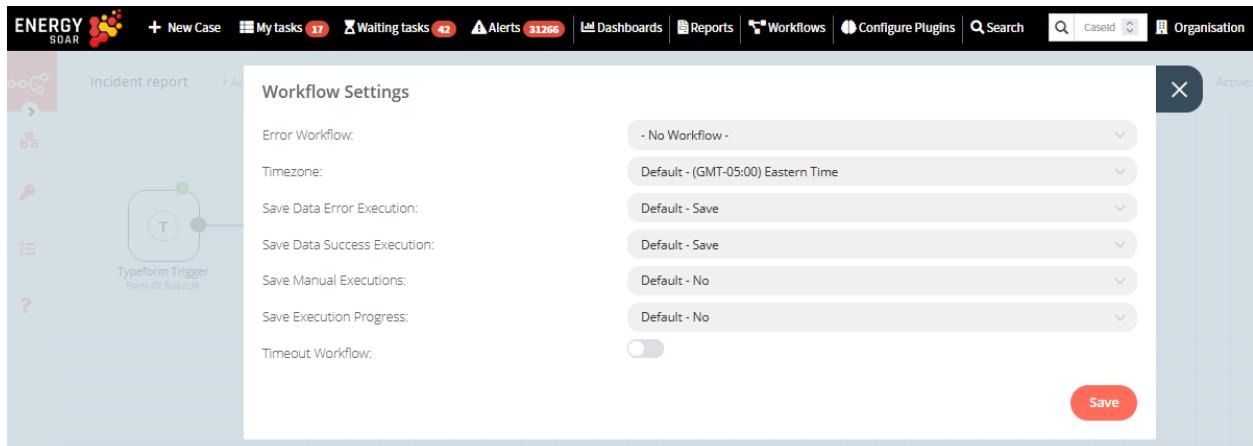
Sharing a workflow

Workflows are saved in JSON format. You can export your workflows as JSON files or import JSON files into your system. You can export a workflow as a JSON file in two ways:

- **Download:** Click the Download button under the Workflow menu in the sidebar. This will download the workflow as a JSON file.
- **Copy-Paste:** Select all the workflow nodes in the Workflow UI, copy them (Ctrl + c), then paste them (Ctrl + v) in your desired file. You can import JSON files as workflows in two ways:
- **Import:** Click Import from File or Import from URL under the Workflow menu in the sidebar and select the JSON file or paste the link to a workflow.
- **Copy-Paste:** Copy the JSON workflow to the clipboard (Ctrl + c) and paste it (Ctrl + v) into the Workflow UI.

Workflow settings

On each workflow, it is possible to set some custom settings and overwrite some of the global default settings from the Workflow > Settings menu.



The following settings are available:

- **Error Workflow:** Select a workflow to trigger if the current workflow fails.
- **Timezone:** Sets the timezone to be used in the workflow. The Timezone setting is particularly important for the Cron Trigger node.
- **Save Data Error Execution:** If the execution data of the workflow should be saved when the workflow fails.
- **Save Data Success Execution:** If the execution data of the workflow should be saved when the workflow succeeds.
- **Save Manual Executions:** If executions started from the Workflow UI should be saved.
- **Save Execution Progress:** If the execution data of each node should be saved. If set to “Yes”, the workflow resumes from where it stopped in case of an error. However, this might increase latency.
- **Timeout Workflow:** Toggle to enable setting a duration after which the current workflow execution should be cancelled.
- **Timeout After:** Only available when Timeout Workflow is enabled. Set the time in hours, minutes, and seconds after which the workflow should timeout.

Failed workflows

If your workflow execution fails, you can retry the execution. To retry a failed workflow:

1. Open the Executions list from the sidebar.
2. For the workflow execution you want to retry, click on the refresh icon under the Status column.
3. Select either of the following options to retry the execution:

- **Retry with currently saved workflow:** Once you make changes to your workflow, you can select this option to execute the workflow with the previous execution data.
- **Retry with original workflow:** If you want to retry the execution without making changes to your workflow, you can select this option to retry the execution with the previous execution data.

You can also use the Error Trigger node, which triggers a workflow when another workflow has an error. Once a workflow fails, this node gets details about the failed workflow and the errors.

5.6.1 Crate your first workflow

Automate Incident Reporting with Typeform

Let's create your first workflow in Energy SOAR. The workflow will create a new alert and promote it to a case whenever a user submits a high severity incident.

Prerequisites

You'll need to obtain the credentials for the Typeform Trigger node.

1. Create a Typeform account: <https://www.typeform.com/>
2. Open the Typeform dashboard: <https://admin.typeform.com/>
3. Click on your avatar on the top right and select 'Settings'.
4. Click on Personal tokens under the Profile section in the sidebar.
5. Click on the Generate a new token button.
6. Enter a name in the Token name field.
7. Click on the Generate token button.
8. Click on the Copy button to copy the access token.
9. In Energy SOAR choose Workflows > Credentials > New > Typeform API.
10. Enter a name for your credentials in the Credentials Name field.
11. Paste the access token in the Access Token field.
12. Click the Create button to save your credentials in Energy SOAR.

You will also need to create a form in Typeform to collect incident reports with the following questions:

- What is your name? (optional) (Short Text)
- What is your email address? (optional) (Email)
- What is incident's category? (Multiple Choice)

3→ What is incident's category? *

☐ A Data Theft

☐ B Unauthorized Access

☐ C Malware

☐ D Compromized Account

☐ E Breach of EU law (Whistleblowing Directive)

☐ F Other

OK ✓

- Severity (Multiple Choice)

4→ Severity

1 - Low, 2-Medium, 3-High

☐ A 1

☐ B 2

☐ C 3

OK ✓

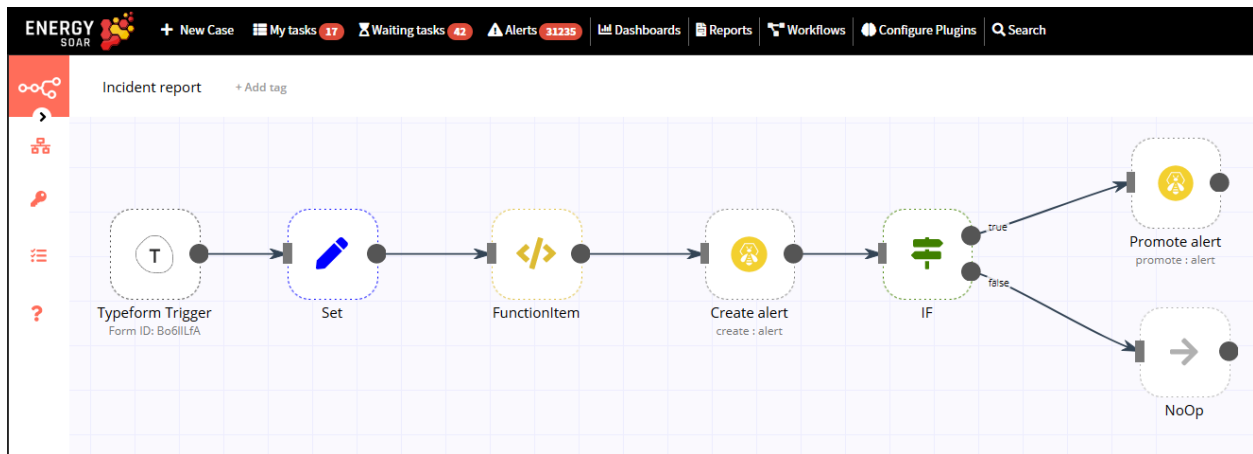
- Description (Long Text)

Building the Workflow

This workflow would use the following nodes:

- Typeform Trigger - Start the workflow when a form receives a report
- Set - Set the workflow data
- FunctionItem - Calculate severity and alert reference
- Energy SOAR Base - Create alert and case
- IF - Conditional logic to decide the flow of the workflow
- NoOp - Do nothing (optional)

The final workflow should look like the following image:



1. Typeform Trigger node

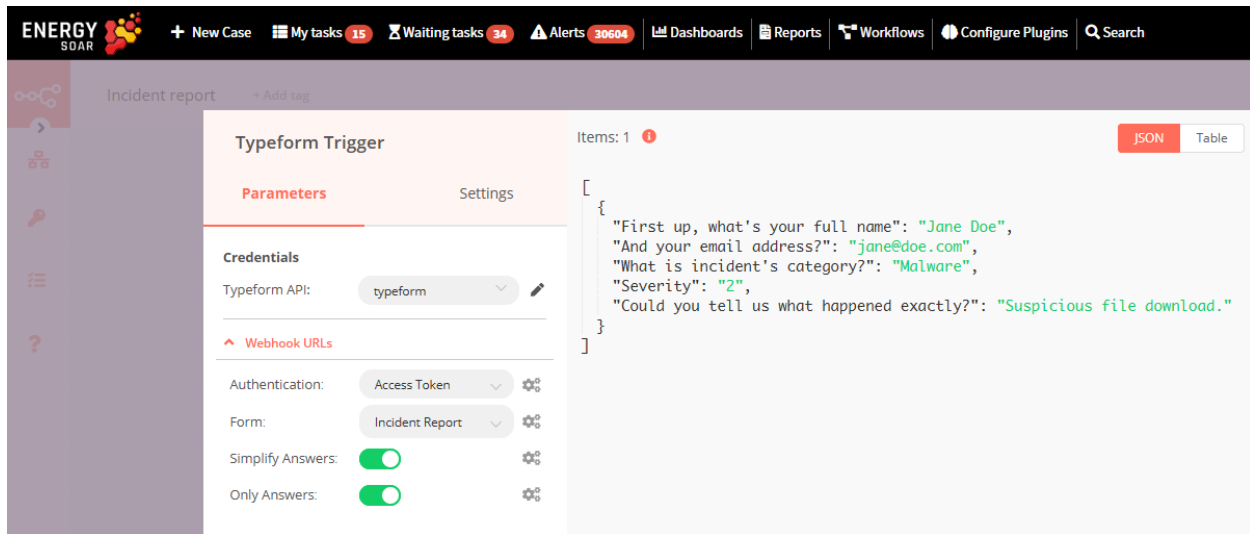
We'll use the Typeform Trigger node for starting the workflow. Add a Typeform Trigger node by clicking on the + button on the top right of the Workflow UI. Click on the Typeform Trigger node under the section marked Trigger.

Double click on the node to enter the Node Editor. Select Credentials from the Typeform API dropdown list.

Select the form that you created from the Form dropdown list. We'll let the other fields stay as they are.

Now save your workflow so that the webhook in the Typeform Trigger node can be activated. Since you'll be using the test webhooks while building the workflow, the node only stays active for 120 seconds after you click the Execute Node button.

After clicking on the Execute Node button, submit a response to your form in Typeform.



2. Set node

We'll use the Set node to ensure that only the data that we set in this node gets passed on to the next nodes in the workflow.

Add the Set node by clicking on the + button and selecting the Set node. Click on Add Value and select String from the dropdown list. Enter title in the Name field. Since the Value (title) would be a dynamic piece of information, click on the gears icon next to the field, and select Add Expression.

This will open up the Variable Selector. From the left panel, select the following variable: Nodes > Typeform Trigger > Output Data > JSON > What is incident's category? Also add Incident Report prefix, so the expression would look like this: Incident Report - {{\$node["Typeform Trigger"].json["What is incident's category?"]}}

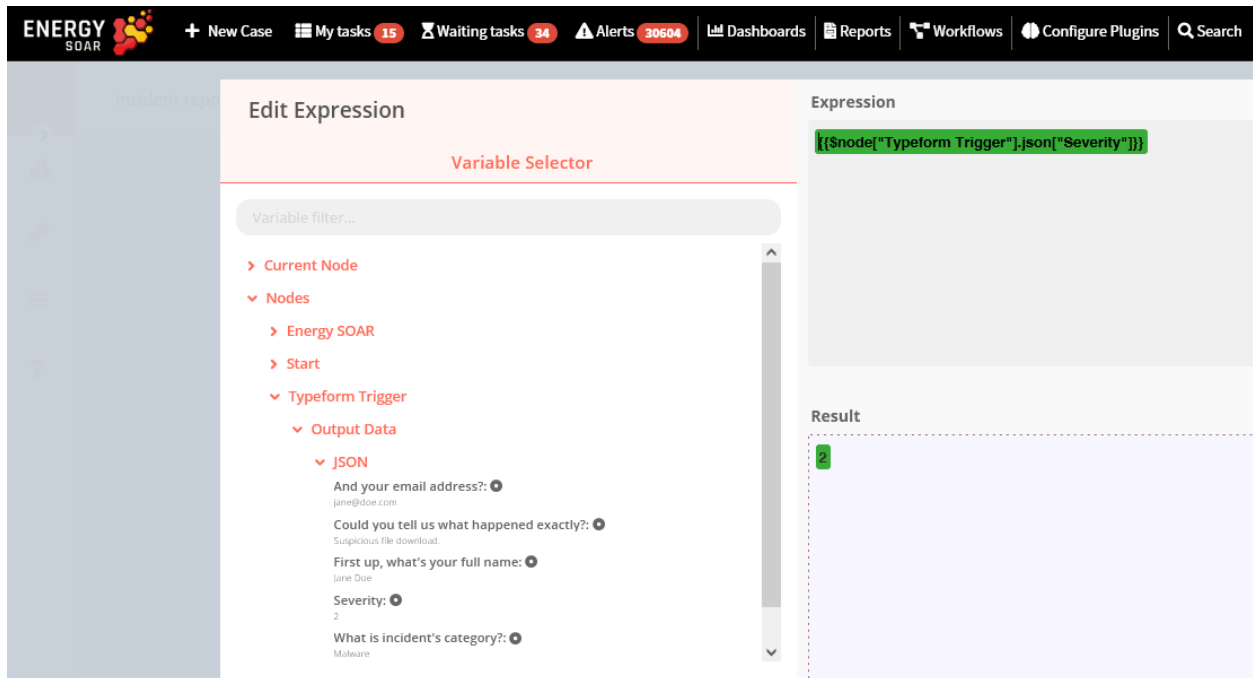
Close the Edit Expression window. Click on Add Value and select String from the dropdown list. Enter description in the Name field. Since the Value (description) would be a dynamic piece of information, click on the gears icon next to the field, and select Add Expression. This will open up the Variable Selector. From the left panel, select the following variables: Nodes > Typeform Trigger > Output Data > JSON > What is your name? Nodes > Typeform Trigger > Output Data > JSON > What is your email address? Nodes > Typeform Trigger > Output Data > JSON > Description?

Also add Name, E-mail, Details prefixes. Full expression: Name: {{\$node["Typeform Trigger"].json["First up, what's your full name"]}}

E-mail: {{\$node["Typeform Trigger"].json["And your email address?"]}}

Details: {{\$node["Typeform Trigger"].json["Could you tell us what happened exactly?"]}}

Close the Edit Expression window. Click on Add Value and select Number from the dropdown list. Enter severity in the Name field. Since the Value (severity) would be a dynamic piece of information, click on the gears icon next to the field, and select Add Expression. This will open up the Variable Selector. Delete the 0 in the Expression field on the right. From the left panel, select the following variable: Nodes > Typeform Trigger > Output Data > JSON > Severity Toggle Keep Only Set to true. We set this option to true to ensure that only the data that we have set in this node get passed on to the next nodes in the workflow. Click on the Execute Node button on the top right to set the data for the workflow.



3. FunctionItem node

To create Energy SOAR alert in workflow we have to provide SourceRef number. We'll use the FunctionItem node to generate that random number. Add the FunctionItem node by clicking on the + button and selecting the FunctionItem node. Clear JavaScript Code window and insert the following code:

```
function getRandomInt(max) {
  return Math.floor(Math.random() * max);
}
item.number= getRandomInt(200000000);
item.number=item.number.toString(16);
item.severity=parseInt(item.severity);
return item;
```

We use parseInt function to convert string severity value into an integer.

4. Create alert node Add Energy SOAR Base node by clicking on the + button and selecting the Energy SOAR Base node. Double click on the node and click on Energy SOAR Base name to change it to Create alert.

Since the Title would be a dynamic piece of information, click on the gears icon next to the field, and select Add Expression.

This will open up the Variable Selector. From the left panel, select the following variable: Nodes > Set > Output Data > JSON > title

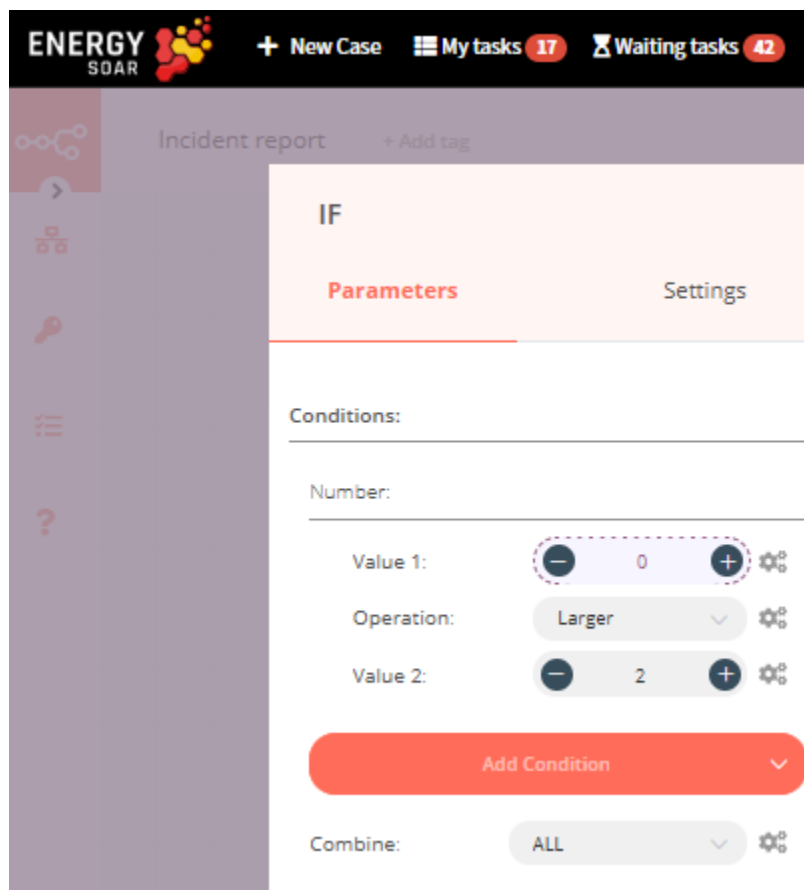
Close the Edit Expression window. In Description field add expression: Nodes > Set > Output Data > JSON > description

Close the Edit Expression window. In Severity field add expression: Nodes > FunctionItem > Output Data > JSON > severity

Close the Edit Expression window. In SourceRef field add expression: Nodes > FunctionItem > Output Data > JSON > number

Click on the Execute Node button on the top right to create alert.

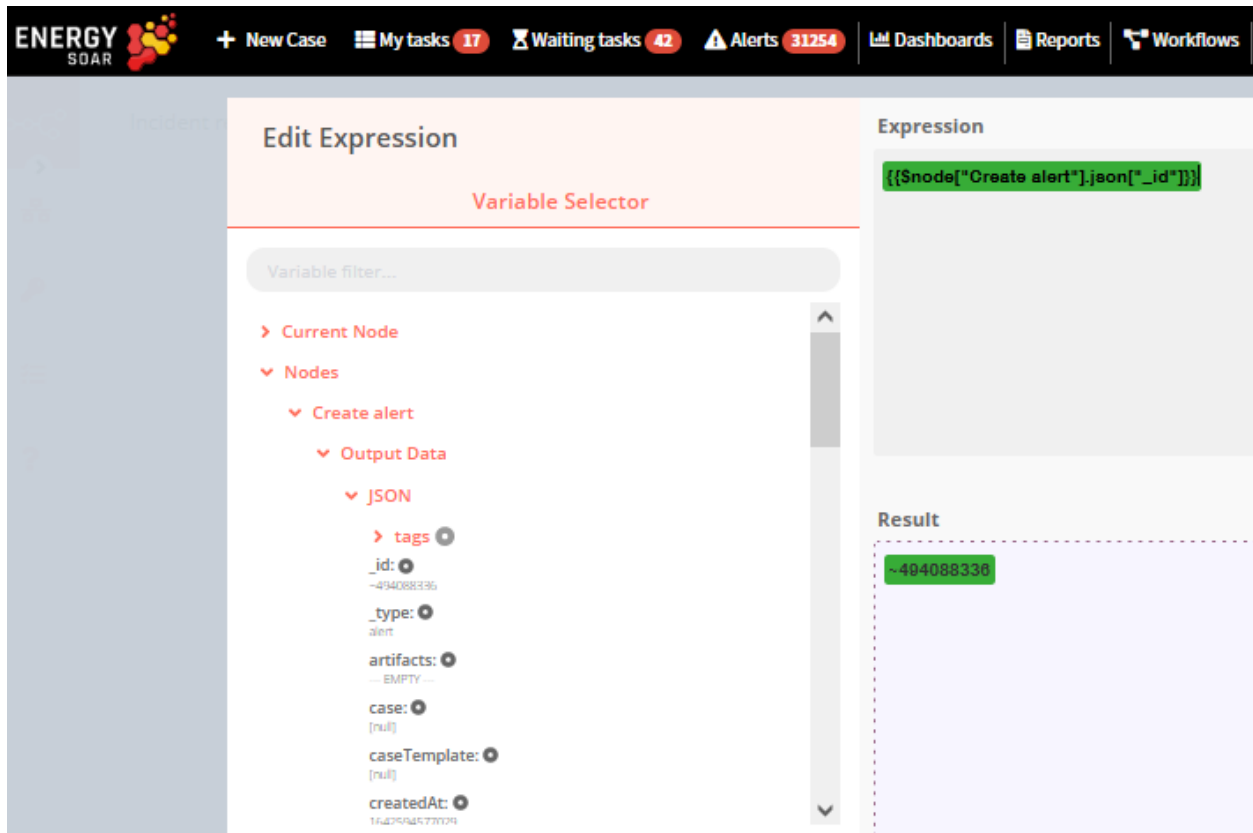
5. IF node Add the IF node by clicking on the + button and selecting the IF node. This is a conditional logic node that allows us to alter the flow of the workflow depending on the data that we get from the previous node(s). Double click on the node, click on the Add Condition button and select Number from the menu. Since the Value 1 (severity) would be a dynamic piece of information, click on the gears icon next to the field, and select Add Expression. This will open up the Variable Selector. Delete the 0 in the Expression field on the right. From the left panel, select the following variable: Nodes > Create alert > Output Data > JSON > severity For the Operation field, we'll set it to 'Larger'. For Value 2, enter 2. This will ensure that the IF node returns true only if the severity is higher than 2 (above medium level). Feel free to change this to some other value. Click on the Execute Node button on the top right to check if the severity is larger than 2 or not.



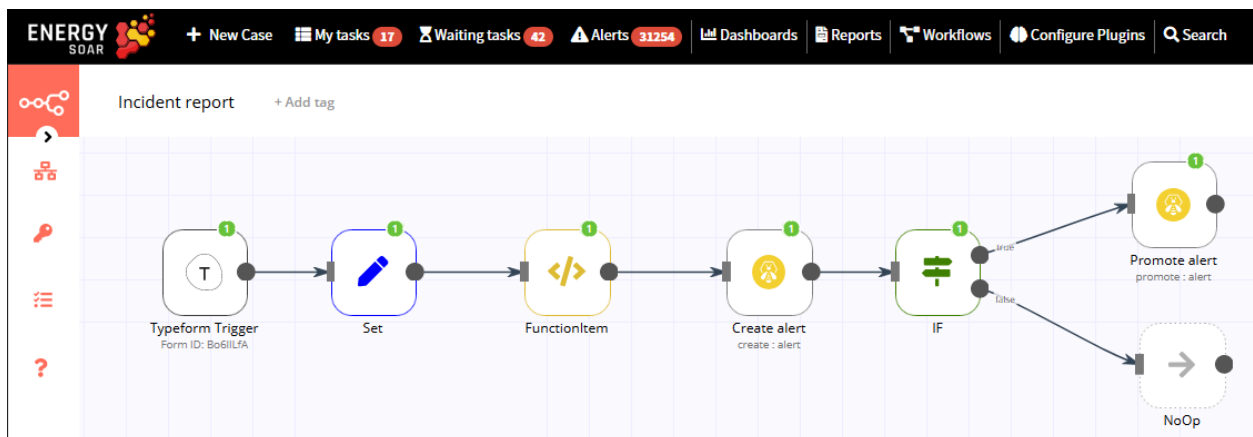
6. Promote alert node

Add Energy SOAR Base node by clicking on the + button and selecting the Energy SOAR node. Double click on the node and click on Energy SOAR name to change it to Promote alert.

Select 'Promote' from the Operation dropdown list. In Alert ID field add expression: Nodes > Create alert > Output Data > JSON > _id



7. NoOp node If the score is smaller than 3, we don't want the workflow to do anything. We'll use the NoOp node for that. Adding this node here is optional, as the absence of this node won't make a difference to the functioning of the workflow. Add the NoOp node by clicking on the + button and selecting the NoOp node. Connect this node with the false output of the IF node. To test the workflow, click on the Execute Workflow button at the bottom of the Workflow UI. Don't forget to save the workflow and then click on the Activate toggle on the top right of the screen to set it to true and activate the workflow. Green checkmarks indicate successful workflow execution:



Congratulations on creating your first workflow with Energy SOAR.

5.6.2 Connection

A connection establishes a link between nodes to route data through the workflow. A connection between two nodes passes data from one node's output to another node's input. Each node can have one or multiple connections.

To create a connection between two nodes, click on the grey dot on the right side of the node and slide the arrow to the grey rectangle on the left side of the following node.

Example

An IF node has two connections to different nodes: one for when the statement is true and one for when the statement is false.

5.6.3 Workflows List

This section includes the operations for creating and editing workflows.

- **New:** Create a new workflow
- **Open:** Open the list of saved workflows
- **Save:** Save changes to the current workflow
- **Save As:** Save the current workflow under a new name
- **Rename:** Rename the current workflow
- **Delete:** Delete the current workflow
- **Download:** Download the current workflow as a JSON file
- **Import from URL:** Import a workflow from a URL
- **Import from File:** Import a workflow from a local file
- **Settings:** View and change the settings of the current workflow

5.6.4 Credentials

This section includes the operations for creating credentials.

Credentials are private pieces of information issued by apps/services to authenticate you as a user and allow you to connect and share information between the app/service and the n8n node.

- **New:** Create new credentials
- **Open:** Open the list of saved credentials

5.6.5 Executions

This section includes information about your workflow executions, each completed run of a workflow.

You can enabling logging of your failed, successful, and/or manually selected workflows using the Workflow > Settings page.

5.6.6 Node

A node is an entry point for retrieving data, a function to process data, or an exit for sending data. The data process performed by nodes can include filtering, recomposing, and changing data.

There may be one or several nodes for your API, service, or app. By connecting multiple nodes, you can create simple and complex workflows. When you add a node to the Editor UI, the node is automatically activated and requires you to configure it (by adding credentials, selecting operations, writing expressions, etc.).

There are three types of nodes:

- Core Nodes
- Regular Nodes
- Trigger Nodes

Core nodes


















Core nodes are functions or services that can be used to control how workflows are run or to provide generic API support.

Use the Start node when you want to manually trigger the workflow with the **Execute Workflow** button at the bottom of the Editor UI. This way of starting the workflow is useful when creating and testing new workflows.

If an application you need does not have a dedicated Node yet, you can access the data by using the HTTP Request node or the Webhook node. You can also read about creating nodes and make a node for your desired application.

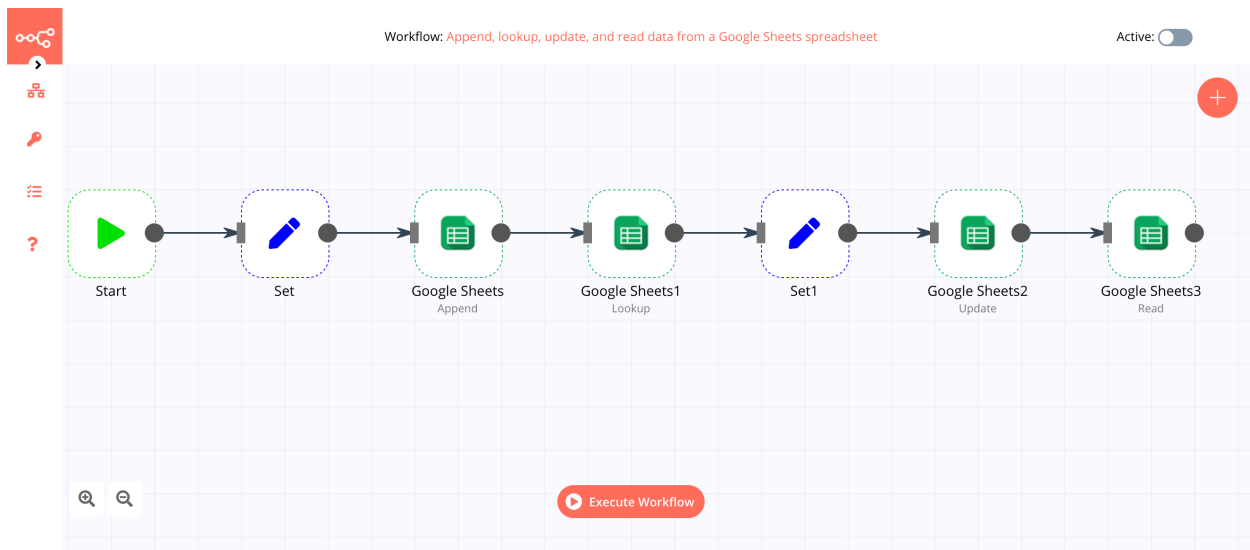
Regular nodes

Regular nodes perform an action, like fetching data or creating an entry in a calendar. Regular nodes are named for the application they represent and are listed under Regular Nodes in the Editor UI.

 Search nodes...		
All	Regular	Trigger
CORE NODES 		
Data Transformation 		
Manipulate data fields, run code		
Files 		
Work with CSV, XML, text, images etc.		
Flow 		
Branches, core triggers, merge data		
Helpers 		
HTTP Requests (API calls), date and time, scrape HTML		
ANALYTICS 		
COMMUNICATION 		
DATA & STORAGE 		
DEVELOPMENT 		
FINANCE & ACCOUNTING 		
MARKETING & CONTENT 		
MONITORING 		
PRODUCTIVITY 		
SALES 		
UTILITY 		
MISCELLANEOUS 		

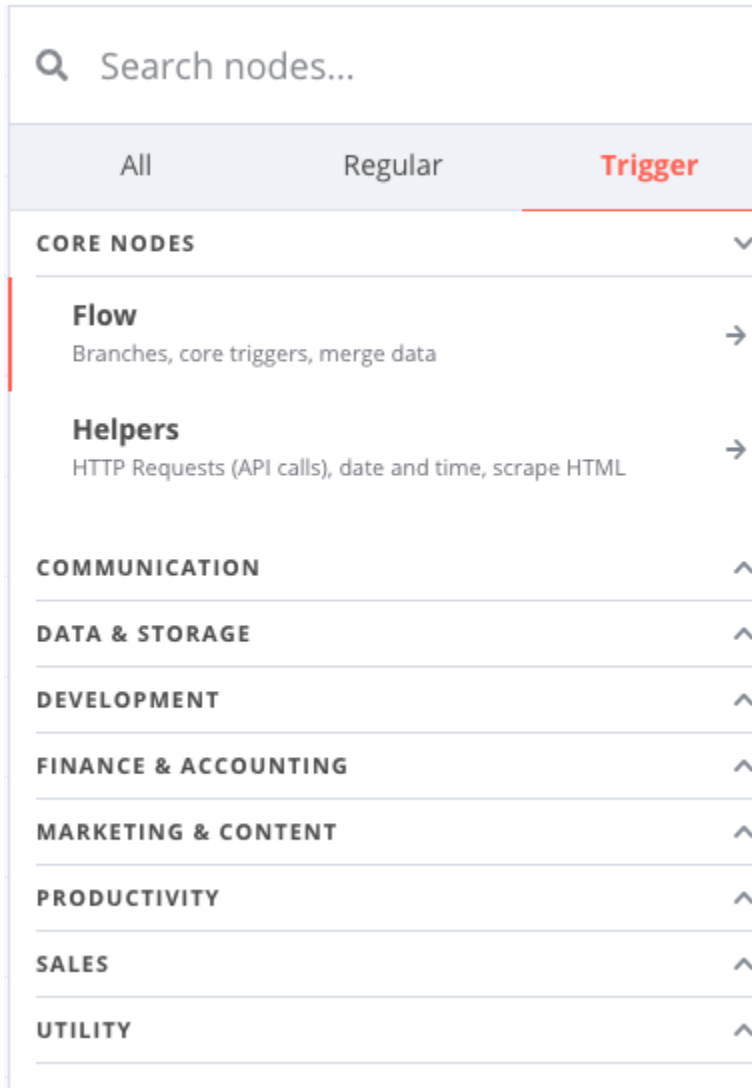
Example

A Google Sheets node can be used to retrieve or write data to a Google Sheet.



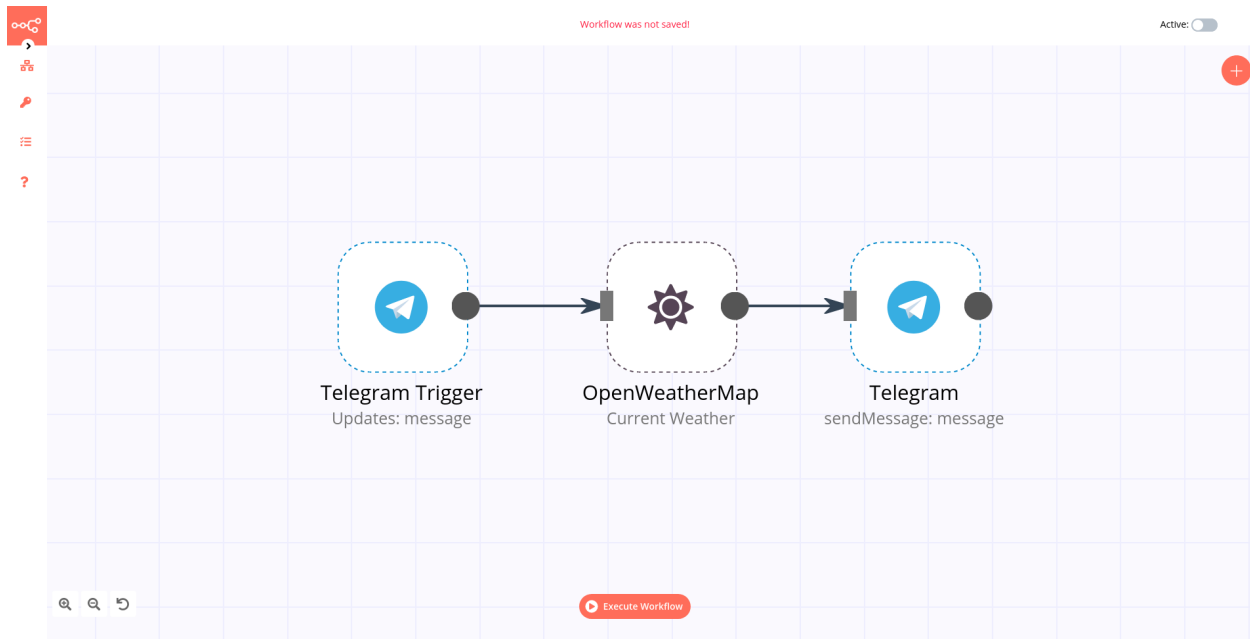
Trigger nodes

Trigger nodes start workflows and supply the initial data.



Trigger nodes can be app or core nodes.

- **Core Trigger nodes** start the workflow at a specific time, at a time interval, or on a webhook call. For example, to get all users from a Postgres database every 10 minutes, use the Interval Trigger node with the Postgres node.
- **App Trigger nodes** start the workflow when an event happens in an app. App Trigger nodes are named like the application they represent followed by “Trigger” and are listed under Trigger Nodes in the Editor. For example, a Telegram trigger node can be used to trigger a workflow when a message is sent in a Telegram chat.



Node settings

Nodes come with global **operations** and **settings**, as well as app-specific **parameters** that can be configured.

Operations

The node operations are illustrated with icons that appear on top of the node when you hover on it:

- **Delete:** Remove the selected node from the workflow
- **Pause:** Deactivate the selected node
- **Copy:** Duplicate the selected node
- **Play:** Run the selected node

To access the node parameters and settings, double-click on the node.

Parameters

The node parameters allow you to define the operations the node should perform. Find the available parameters of each node in the node reference.

Settings

The node settings allow you to configure the look and execution of the node. The following options are available:

- **Notes:** Optional note to save with the node
- **Display note in flow:** If active, the note above will be displayed in the workflow as a subtitle
- **Node Color:** The color of the node in the workflow
- **Always Output Data:** If active, the node will return an empty item even if the node returns no data during an initial execution. Be careful setting this on IF nodes, as it could cause an infinite loop.
- **Execute Once:** If active, the node executes only once, with data from the first item it receives.
- **Retry On Fail:** If active, the node tries to execute a failed attempt multiple times until it succeeds
- **Continue On Fail:** If active, the workflow continues even if the execution of the node fails. When this happens, the node passes along input data from previous nodes, so the workflow should account for unexpected output data.

If a node is not correctly configured or is missing some required information, a **warning sign** is displayed on the top right corner of the node. To see what parameters are incorrect, double-click on the node and have a look at fields marked with red and the error message displayed in the respective warning symbol.

5.6.7 Workflow integration nodes

To boost your workflow automation you can connect with widely external nodes.

List of automation nodes:

- Action Network
- Activation Trigger
- ActiveCampaign
- ActiveCampaign Trigger
- Acuity Scheduling Trigger
- Affinity
- Affinity Trigger
- Agile CRM
- Airtable
- Airtable Trigger
- AMQP Sender
- AMQP Trigger
- APITemplate.io
- Asana
- Asana Trigger
- Automizy

- Autopilot
- Autopilot Trigger
- AWS Comprehend
- AWS DynamoDB
- AWS Lambda
- AWS Rekognition
- AWS S3
- AWS SES
- AWS SNS
- AWS SNS Trigger
- AWS SQS
- AWS Textract
- AWS Transcribe
- Bannerbear
- Baserow
- Beeminder
- Bitbucket Trigger
- Bitly
- Bitwarden
- Box
- Box Trigger
- Brandfetch
- Bubble
- Calendly Trigger
- Chargebee
- Chargebee Trigger
- CircleCI
- Clearbit
- ClickUp
- ClickUp Trigger
- Clockify
- Clockify Trigger
- Cockpit
- Coda
- CoinGecko
- Compression

- Contentful
- ConvertKit
- ConvertKit Trigger
- Copper
- Copper Trigger
- Cortex
- CrateDB
- Cron
- Crypto
- Customer Datastore (n8n training)
- Customer Messenger (n8n training)
- Customer Messenger (n8n training)
- Customer.io
- Customer.io Trigger
- Date & Time
- DeepL
- Demio
- DHL
- Discord
- Discourse
- Disqus
- Drift
- Dropbox
- Dropcontact
- E-goi
- Edit Image
- Elastic Security
- Elasticsearch
- EmailReadImap
- Emelia
- Emelia Trigger
- ERPNext
- Error Trigger
- Eventbrite Trigger
- Execute Command
- Execute Workflow

- Facebook Graph API
- Facebook Trigger
- Figma Trigger (Beta)
- FileMaker
- Flow
- Flow Trigger
- Form.io Trigger
- Formstack Trigger
- Freshdesk
- Freshservice
- Freshworks CRM
- FTP
- Function
- Function Item
- G Suite Admin
- GetResponse
- GetResponse Trigger
- Ghost
- Git
- GitHub
- Github Trigger
- GitLab
- GitLab Trigger
- Gmail
- Google Analytics
- Google BigQuery
- Google Books
- Google Calendar
- Google Calendar Trigger
- Google Cloud Firestore
- Google Cloud Natural Language
- Google Cloud Realtime Database
- Google Contacts
- Google Docs
- Google Drive
- Google Drive Trigger

- Google Perspective
- Google Sheets
- Google Slides
- Google Tasks
- Google Translate
- Gotify
- GoToWebinar
- Grafana
- GraphQL
- Grist
- Gumroad Trigger
- Hacker News
- Harvest
- HelpScout
- HelpScout Trigger
- Home Assistant
- HTML Extract
- HTTP Request
- HubSpot
- HubSpot Trigger
- Humantic AI
- Hunter
- iCalendar
- IF
- Intercom
- Interval
- Invoice Ninja
- Invoice Ninja Trigger
- Item Lists
- Iterable
- Jira Software
- Jira Trigger
- JotForm Trigger
- Kafka
- Kafka Trigger
- Keap

- Keap Trigger
- Kitemaker
- Lemlist
- Lemlist Trigger
- Line
- LingvaNex
- LinkedIn
- Local File Trigger
- Magento 2
- Mailcheck
- Mailchimp
- Mailchimp Trigger
- MailerLite
- MailerLite Trigger
- Mailgun
- Mailjet
- Mailjet Trigger
- Mandrill
- Marketstack
- Matrix
- Mattermost
- Mautic
- Mautic Trigger
- Medium
- Merge
- MessageBird
- Microsoft Dynamics CRM
- Microsoft Excel
- Microsoft OneDrive
- Microsoft Outlook
- Microsoft SQL
- Microsoft Teams
- Microsoft To Do
- Mindee
- MISP
- Mocean

- Monday.com
- MongoDB
- Monica CRM
- Move Binary Data
- MQTT
- MQTT Trigger
- MSG91
- MySQL
- n8n Trigger
- NASA
- Netlify
- Netlify Trigger
- Nextcloud
- No Operation, do nothing
- NocoDB
- Notion (Beta)
- Notion Trigger (Beta)
- One Simple API
- OpenThesaurus
- OpenWeatherMap
- Orbit
- Oura
- Paddle
- PagerDuty
- PayPal
- PayPal Trigger
- Peekalink
- Phantombuster
- Philips Hue
- Pipedrive
- Pipedrive Trigger
- Plivo
- Postgres
- PostHog
- Postmark Trigger
- ProfitWell

- Pushbullet
- Pushcut
- Pushcut Trigger
- Pushover
- QuestDB
- Quick Base
- QuickBooks Online
- RabbitMQ
- RabbitMQ Trigger
- Raindrop
- Read Binary File
- Read Binary Files
- Read PDF
- Reddit
- Redis
- Rename Keys
- Respond to Webhook
- RocketChat
- RSS Read
- Rundeck
- S3
- Salesforce
- Salesmate
- SeaTable
- SeaTable Trigger
- SecurityScorecard
- Segment
- Send Email
- SendGrid
- Sendy
- Sentry.io
- ServiceNow
- Set
- Shopify
- Shopify Trigger
- SIGNAL4

- Slack
- sms77
- Snowflake
- Split In Batches
- Splunk
- Spontit
- Spotify
- Spreadsheet File
- SSE Trigger
- SSH
- Stackby
- Start
- Stop and Error
- Storyblok
- Strapi
- Strava
- Strava Trigger
- Stripe
- Stripe Trigger
- SurveyMonkey Trigger
- Switch
- Taiga
- Taiga Trigger
- Tapfiliate
- Telegram
- Telegram Trigger
- TheHive
- TheHive Trigger
- TimescaleDB
- Todoist
- Toggl Trigger
- TravisCI
- Trello
- Trello Trigger
- Twake
- Twilio

- Twist
- Twitter
- Typeform Trigger
- Unleashed Software
- Uplead
- uProc
- UptimeRobot
- urlscan.io
- Vero
- Vonage
- Wait
- Webex by Cisco
- Webex by Cisco Trigger
- Webflow
- Webflow Trigger
- Webhook
- Wekan
- Wise
- Wise Trigger
- WooCommerce
- WooCommerce Trigger
- Wordpress
- Workable Trigger
- Workflow Trigger
- Write Binary File
- Wufoo Trigger
- Xero
- XML
- Yourls
- YouTube
- Zendesk
- Zendesk Trigger
- Zoho CRM
- Zoom
- Zulip

OPERATIONS

INTEGRATIONS

7.1 Responders

7.1.1 AMPforEndpoints

AMPforEndpoints_IsolationStart

Details

Author	Cisco Security
Version	1.0
License	MIT
Website	https://github.com/CiscoSecurity
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	thehive:case_artifact

Description

Start host isolation for an AMP for Endpoints connector

Configuration

Name	Description
amp_cloud	FQDN of the AMP for Endpoints cloud to interact with
client_id	Client ID for AMP for Endpoints
api_key	API Key for AMP for Endpoints
unlock_code	Custom unlock code used to stop isolation from the endpoint (Maximum 24 characters)

AMPforEndpoints_IsolationStop

Details

Author	Cisco Security
Version	1.0
License	MIT
Website	https://github.com/CiscoSecurity
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	thehive:case_artifact

Description

Stop host isolation for an AMP for Endpoints connector

Configuration

Name	Description
amp_cloud	FQDN of the AMP for Endpoints cloud to interact with
client_id	Client ID for AMP for Endpoints
api_key	API Key for AMP for Endpoints

AMPforEndpoints_MoveGUID

Details

Author	Cisco Security
Version	1.0
License	MIT
Website	https://github.com/CiscoSecurity
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	thehive:case_artifact

Description

Move an AMP for Endpoints connector GUID to a different Group

Configuration

Name	Description
amp_cloud	FQDN of the AMP for Endpoints cloud to interact with
client_id	Client ID for AMP for Endpoints
api_key	API Key for AMP for Endpoints
group_guid	AMP for Endpoints Group GUID for the group connectors will be moved to

AMPforEndpoints_SCDAdd

Details

Author	Cisco Security
Version	1.0
License	MIT
Website	https://github.com/CiscoSecurity
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	thehive:case_artifact

Description

Add a SHA256 to an AMP for Endpoints Simple Custom Detection list

Configuration

Name	Description
amp_cloud	FQDN of the AMP for Endpoints cloud to interact with
client_id	Client ID for AMP for Endpoints
api_key	API Key for AMP for Endpoints
scd_guid	AMP for Endpoints Simple Custom Detection GUID

AMPforEndpoints_SCDRemove

Details

Author	Cisco Security
Version	1.0
License	MIT
Website	https://github.com/CiscoSecurity
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	thehive:case_artifact

Description

Remove a SHA256 to an AMP for Endpoints Simple Custom Detection list

Configuration

Name	Description
amp_cloud	FQDN of the AMP for Endpoints cloud to interact with
client_id	Client ID for AMP for Endpoints
api_key	API Key for AMP for Endpoints
scd_guid	AMP for Endpoints Simple Custom Detection GUID

7.1.2 AzureTokenRevoker

AzureTokenRevoker

Details

Author	Daniel Weiner @dmweiner
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	thehive:case

Description

Revoke all Microsoft Azure authentication session tokens for a list of User Principal Names

Configuration

Name	Description
redirect_uri	Azure AD Application URI (Example: https://login.microsoftonline.com/TENANTIDHERE/oauth2/token)
client_id	Client ID/Application ID of Azure AD Registered App
client_secret	Secret for Azure AD Registered Application

7.1.3 CheckPoint

CheckPoint_Lock

Details

Author	@dadokkio LDO-CERT
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	thehive:case_artifact

Description

Lock ip on CheckPoint Gaia

Configuration

Name	Description
server	Checkpoint API server
username	CheckPoint username
password	CheckPoint password
group_name	CheckPoint group name ip will be added/removed from
exclusions	ip/subnet that cannot be locked or unlocked
added_tag	Tag added to observable when adding to FW
removed_tag	Tag added to observable when removing from FW

CheckPoint_Unlock

Details

Author	@dadokkio LDO-CERT
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	thehive:case_artifact

Description

Unlock ip on CheckPoint Gaia

Configuration

Name	Description
server	Checkpoint API server
username	CheckPoint username
password	CheckPoint password
group_name	CheckPoint group name ip will be added/removed from
exclusions	ip/subnet that cannot be locked or unlocked
added_tag	Tag added to observable when adding to FW
removed_tag	Tag added to observable when removing from FW

Additional details from the README file:

CheckPoint

This responder permits you to add/remove selected observable from a specific group.

Some notes:

- API must permit access **from cortex** machine.
- First login **from API** must be manual because it needs fingerprint acceptance. This will generate a fingerprints.txt file that must be placed near to the analyzer python file.
- It doesn't work in dockerized analyzer!
- If group doesn't exist it'll be created [when blocking]. At the moment without any default rule.

Requirements

The following options are required in CheckPoint Responder configuration:

- **server** : URL of CheckPoint instance
- **username**: user accessing CheckPoint instance
- **password**: password for the user accessing CheckPoint instance
- **group_name**: name of the group ip will be added to or removed

7.1.4 CheckPointBlockIP

Check Point Block IP

Details

Author	EMCA Software
Version	0.1
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	thehive:case_artifact

Description

CheckPoint Firewall IP Block

Configuration

Name	Description
base_url	CheckPoint URL
username	API user
password	API user Password
sessiontimeout	API Session Timeout
BlockGroupName	Block Group Name

7.1.5 CheckPointUnblockIP

Check Point Unblock IP

Details

Author	EMCA Software
Version	0.1
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	thehive:case_artifact

Description

CheckPoint Firewall IP Unblock

Configuration

Name	Description
base_url	CheckPoint URL
username	API user
password	API user Password
sessiontimeout	API Session Timeout

7.1.6 DNS-RPZ

DNS-RPZ

Details

Author	Michael Hornung; Expeditors International of Washington, Inc.
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	thehive:case_artifact

Description

Add a dynamic DNS entry to a Response Policy Zone, blackholing or redirecting a FQDN.

Configuration

Name	Description
bind_server	IP or FQDN of RPZ master BIND server
tsig_keyname	Name of TSIG key to access BIND server
tsig_keyval	TSIG key value to access BIND server
tsig_hashalg	TSIG hash algorithm to use
rpz_zonename	Fully qualified RPZ zone name (don't forget the trailing dot)
remediation_ip	IP to resolve RPZ names to

7.1.7 DomainToolsIris_AddRiskyDNSTag

DomainToolsIris_AddRiskyDNSTag

Details

Author	DomainTools
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	thehive:case_artifact

Description

Add Tag saying that the case contains a risky DNS.

Configuration

Name	Description
high_risk_threshold	Risk score threshold to be considered high risk.

7.1.8 DomainToolsIris_CheckMaliciousTags

DomainToolsIris_CheckMaliciousTags

Details

Author	DomainTools
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	thehive:case_artifact

Description

Add Tag saying that the observable and case have a malicious tag in their Iris Tags.

Configuration

Name	Description
monitored_iris_tags	Monitored Iris tags.

7.1.9 Duo_Security

DuoLockUserAccount

Details

Author	Sven Kutzer / Gyorgy Acs, @oscd_initiative
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	thehive:case_artifact

Description

Lock User Account in Duo Security via AdminAPI (The user will not be able to log in)

Configuration

Name	Description
API_hostname	Duo Admin API hostname, api-XXXXXXXXX.duosecurity.com
Integration_Key	Integration Key
Secret_Key	Secret Key

DuoUnlockUserAccount

Details

Author	Sven Kutzer / Gyorgy Acs, @oscd_initiative
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	thehive:case_artifact

Description

Unlock User Account in Duo Security via AdminAPI (The user must complete secondary authentication)

Configuration

Name	Description
API_hostname	Duo Admin API hostname, api-XXXXXXXXX.duosecurity.com
Integration_Key	Integration Key
Secret_Key	Secret Key

Additional details from the README file:

CortexResponder_DuoUserAccount

Rep. for Cortex Responder (TheHive project - <https://github.com/TheHive-Project/CortexDocs>) to Lock/Unlock User Accounts in the Duo Admin Portal (Cisco Security)

There are two Responder available in order to change the status of a User in Duo Security via the AdminAPI (<https://duo.com/docs/adminapi>)

DuoLockUserAccount -> changes the “status” to “disabled” - The user will not be able to log in.

DuoUnlockUserAccount -> changes the “status” to “active” - The user must complete secondary authentication.

The Responder is looking for a “username” as input and queries the Duo Admin API, to receive the associated UserID. The UserID is used to change the “status” of the particular user.

How to install:

- copy the folders “DuoLockUserAccount” & “DuoUnlockUserAccount” into your Cortex responders path
- install necessary python modules from the requirements.txt (**pip install -r requirements.txt**)
- restart Cortex to initialize the new Responder “**systemctl restart cortex**”
- add the ResponderConfig



07-0-0-Integrations/Responders/Duo_Security/assets/ResponderConfig.jpg

-
- enable the Responder Actions



07-0-0-Integrations/Responders/Duo_Security/assets/Responders.jpg

-

Add Observable type in TheHive**

- per default TheHive has no “username” Observable type, so we have to add this in the Admin settings



07-0-0-Integrations/Responders/Duo_Security/assets/AddObservableType.jpg

-

Run the Responder action in TheHive

If you have add an observable, you can now take action and lock/unlock the User in Duo Security

-

7.1.10 Eset

EsetMachineIntegration

Details

Author	EMCA Software Sp. z o.o.
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	thehive:case_artifact

Description

Integrate a machine in Eset

Configuration

Name	Description
eset_console_url	Eset console URL
eset_user	Eset User
eset_password	Eset Password
eset_verify_ssl	Verify SSL Certificate

EsetMachineIsolation

Details

Author	EMCA Software Sp. z o.o.
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	thehive:case_artifact

Description

Isolate a machine in Eset

Configuration

Name	Description
eset_console_url	Eset console URL
eset_user	Eset User
eset_password	Eset Password
eset_verify_ssl	Verify SSL Certificate

EsetAddSHA1ToBlacklist

Details

Author	EMCA Software Sp. z o.o.
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	thehive:case_artifact

Description

Add SHA1 to ESET blacklist

Configuration

Name	Description
eset_console_url	Eset console URL
eset_user	Eset User
eset_password	Eset Password
eset_verify_ssl	Verify SSL Certificate

7.1.11 FalconCustomIOC

Crowdstrike_Falcon_Custom_IOC_API

Details

Author	Michael
Version	1.0
License	MIT
Website	https://www.crowdstrike.com/blog/tech-center/import-iocs-crowdstrike-falcon-host-platform-via-api/
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	thehive:alert, thehive:case_artifact

Description

Submit observables to the Crowdstrike Falcon Custom IOC api

Configuration

Name	Description
falconapi_url	Crowdstrike Falcon host url
falconapi_user	Crowdstrike Falcon query api user
falconapi_key	Crowdstrike Falcon query api key

7.1.12 FortiMailBlockRecipient

FortiMailBlockRecipient

Details

Author	EMCA Software
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	thehive:case_artifact:mail

Description

Block Recipient Mail on FortiMail

Configuration

Name	Description
FortiMail_IP	FortiMail IP
username	Username of Admin account that connects to FortiMail
password	Password of Admin account that connects to FortiMail
VerifySSL	set to false to bypass SSL verification

Additional details from the README file:

Simple responder to block recipient on FortiMail

7.1.13 FortiMailBlockSender

FortiMailBlockSender

Details

Author	EMCA Software
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	thehive:case_artifact:mail

Description

Block Sender Mail on FortiMail

Configuration

Name	Description
FortiMail_IP	FortiMail IP
username	Username of Admin account that connects to FortiMail
password	Password of Admin account that connects to FortiMail
VerifySSL	set to false to bypass SSL verification

Additional details from the README file:

Simple responder to block sender on FortiMail

7.1.14 FortiMailConnectionTest

FortiMailConnectionTest

Details

Author	EMCA Software
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	thehive:case_artifact:mail

Description

Test API Connection for FortiMail

Configuration

Name	Description
FortiMail_IP	FortiMail IP
username	Username of Admin account that connects to FortiMail
password	Password of Admin account that connects to FortiMail
VerifySSL	set to false to bypass SSL verification

Additional details from the README file:

Simple responder to test FortiMail connection

7.1.15 FortiMailUnblockRecipient

FortiMailUnblockRecipient

Details

Author	EMCA Software
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	thehive:case_artifact:mail

Description

Block Recipient Mail on FortiMail

Configuration

Name	Description
FortiMail_IP	FortiMail IP
username	Username of Admin account that connects to FortiMail
password	Password of Admin account that connects to FortiMail
VerifySSL	set to false to bypass SSL verification

Additional details from the README file:

Simple responder to unblock recipient on FortiMail

7.1.16 FortiMailUnblockSender

FortiMailUnblockSender

Details

Author	EMCA Software
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	thehive:case_artifact:mail

Description

Unblock Sender Mail on FortiMail

Configuration

Name	Description
FortiMail_IP	FortiMail IP
username	Username of Admin account that connects to FortiMail
password	Password of Admin account that connects to FortiMail
VerifySSL	set to false to bypass SSL verification

Additional details from the README file:

Simple responder to unblock sender on FortiMail

7.1.17 Gmail

Gmail_BlockDomain

Details

Author	David Strassegger, @oscd_initiative
Version	1.0
License	MIT
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	thehive:case_artifact

Description

Move emails from a given domain to trash

Configuration

Name	Description
thehive_url	URL for thehive instance
thehive_api_key	API key for TheHive instance
gmail_domain	Gsuite Domain
gmail_project_id	GCP Project ID
gmail_private_key_id	Service account private key id
gmail_private_key	Service Account private key (PEM Format)
gmail_client_email	Service Account E-Mail address
gmail_client_id	OAuth Client ID

Gmail_BlockSender

Details

Author	David Strassegger, @oscd_initiative
Version	1.0
License	MIT
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	thehive:case_artifact

Description

Move emails from a given sender to trash

Configuration

Name	Description
thehive_url	URL for thehive instance
thehive_api_key	API key for TheHive instance
gmail_domain	Gsuite Domain
gmail_project_id	GCP Project ID
gmail_private_key_id	Service account private key id
gmail_private_key	Service Account private key (PEM Format)
gmail_client_email	Service Account E-Mail address
gmail_client_id	OAuth Client ID

Gmail_DeleteMessage

Details

Author	David Strassegger, @oscd_initiative
Version	1.0
License	MIT
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	thehive:case_artifact

Description

Move a given message into the trash folder

Configuration

Name	Description
thehive_url	URL for thehive instance
thehive_api_key	API key for TheHive instance
gmail_domain	Gsuite Domain
gmail_project_id	GCP Project ID
gmail_private_key_id	Service account private key id
gmail_private_key	Service Account private key (PEM Format)
gmail_client_email	Service Account E-Mail address
gmail_client_id	OAuth Client ID

Gmail_UnblockDomain

Details

Author	David Strassegger, @oscd_initiative
Version	1.0
License	MIT
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
Data Type Supported	thehive:case_artifact

Description

Remove a message filter for a given domain

Configuration

Name	Description
thehive_url	URL for thehive instance
thehive_api_key	API key for TheHive instance
gmail_domain	Gsuite Domain
gmail_project_id	GCP Project ID
gmail_private_key_id	Service account private key id
gmail_private_key	Service Account private key (PEM Format)
gmail_client_email	Service Account E-Mail address
gmail_client_id	OAuth Client ID

Gmail_UnblockSender

Details

Author	David Strassegger, @oscd_initiative
Version	1.0
License	MIT
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	thehive:case_artifact

Description

Remove a message filter for a given sender

Configuration

Name	Description
thehive_url	URL for thehive instance
thehive_api_key	API key for TheHive instance
gmail_domain	Gsuite Domain
gmail_project_id	GCP Project ID
gmail_private_key_id	Service account private key id
gmail_private_key	Service Account private key (PEM Format)
gmail_client_email	Service Account E-Mail address
gmail_client_id	OAuth Client ID

Additional details from the README file:

Gmail responder

This responder allows mailbox manipulation of Gsuite / Google Workspace accounts. The responder can be used to implement message filters and delete message in a mailbox of a Gmail user.

Usage:

- You can block mail and domain observables
- Operations are carried out against all gmail addresses (dataType mail) in the case
 - Example: `john.doe@gmail.com` or `peter.parker@custom.domain`
 - Custom domain can be set in the responder config
- The *message ID* of deleted messages is added as tag to the respective gmail address (dataType mail)
 - Messages can only be deleted via Gmail query syntax (datatype other); this enables one to bulk delete a lot of messages
- The *filter ID* of a blocked domain or mail gets added as tag to respective gmail address (dataType mail)
- All observables that get blocked/unblocked get a `gmail:handled` tag

Constraints:

- TheHive API key needs to provide **read** AND **write** permissions
- The Gmail user **MUST** be part of a Gsuite domain.
- Gsuite domain **MUST** have an *service account* enabled with domain-wide delegation.
- The *service account* **MUST** be configured with the following OAuth Scopes:
 - <https://mail.google.com/>
 - <https://www.googleapis.com/auth/gmail.settings.basic>

How to setup a Gmail service account

The responder needs a Gmail *service account* with domain-wide delegation. The rough setup steps are:

1. enable a *service account* via GCP
2. enable Gmail API
3. get service account `client_id` (*oauth approval screens + domain-wide delegation needed*)
4. change to Gsuite Admin panel
5. add third party app (security->API controls) with `client_id`
6. add domain-wide delegation with `client_id`

A detailed guideline for a *service account* setup can be found in the [Google OAuth Python Client Docs](#).

7.1.18 KnowBe4**KnowBe4****Details**

Author	Kyle Parrish
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	thehive:case_artifact

Description

Add 'Clicked Event' to User via User Events API.

Configuration

Name	Description
api_url	Base API url
hive_url	Specify The Hive Instance URL
api_key	Api Key
re-required_tag	Specify a tag that must be present for responder to run.
event_type	Specify the Event Type for the new event. https://developer.knowbe4.com/events/#tag/Event-Types
risk_level	Specify the desired risk level. https://developer.knowbe4.com/events/#tag/Events/paths/~1events/post

7.1.19 LDAP

LDAP_ChangePWD

Details

Author	EMCA Software Sp. z o.o.
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	thehive:case_artifact:mail, thehive:case_artifact:other

Description

Reset User Password (New pass have to be configured in responder configs, as hive doesn't support passing data on reponder invocation).

Configuration

Name	Description
AD_Address	Example -> ldaps://ldaphost.example.com
AD_port	ldaps port. Example -> 636
username	Username of account that will query Active Directory server
password	Password of account that will query Active Directory server
base_DN	The base DN to use. Example -> dc=myorg,dc=com
NewPassword	The new Password to be changed to
VerifySSL	set to false to bypass SSL verification

LDAP_UnblockUser

Details

Author	EMCA Software Sp. z o.o.
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	thehive:case_artifact:mail, thehive:case_artifact:other

Description

Unblock Normal Active Directory User

Configuration

Name	Description
AD_Address	Example -> ldaps://ldaphost.example.com
AD_port	ldap port. Example -> 389 or 636
username	Username of account that will query Active Directory server
password	Password of account that will query Active Directory server
base_DN	The base DN to use. Example -> dc=myorg,dc=com
VerifySSL	set to false to bypass SSL verification

LDAP_BlockUser

Details

Author	EMCA Software Sp. z o.o.
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	thehive:case_artifact:mail, thehive:case_artifact:other

Description

Block Normal Active Directory User

Configuration

Name	Description
AD_Address	Example -> ldaps://ldaphost.example.com
AD_port	ldap port. Example -> 389 or 636
username	Username of account that will query Active Directory server
password	Password of account that will query Active Directory server
base_DN	The base DN to use. Example -> dc=myorg,dc=com
VerifySSL	set to false to bypass SSL verification

Additional details from the README file:

This module provides responders for TheHive Cortex to interface with LDAP services, enabling automated actions such as changing user passwords, locking and unlocking user accounts.

Responders Included:

1. **LDAP_ChangePWD:** This responder enables the automated reset or change of a user's password on an LDAP server. Note: This function requires the use of LDAPS (LDAP over SSL) for secure transmission of the new password.
2. **LDAP_BlockUser:** This responder allows for the locking of a user's account in an LDAP directory.
3. **LDAP_UnblockUser:** Similar to the block function, but this responder unlocks a user account in an LDAP directory.

Important Note:

For security and safety:

- Ensure that the credentials provided have the minimal necessary permissions.
- Regularly rotate the provided credentials.
- Always use LDAPS when transmitting sensitive information like passwords.

7.1.20 MSDefenderEndpoints

MSDefender-IsolateMachine

Details

Author	Keijo Korte
Version	1.0
License	AGPL-V3
Requires Registration	Yes
Requires Subscription	Yes
Free Subscription Available	No
DataType Supported	thehive:case_artifact
Service Homepage	MSDefender-IsolateMachine

Description

Isolate machine with Microsoft Defender for Endpoints

Configuration

Name	Description
tenantId	Azure tenant ID
appId	Azure app ID
appSecret	Azure app secret
resourceAppIdUri	Security Center URI, usually doesn't need to change
oAuthUri	Azure oAuth2 authentication endpoint

MSDefender-PushIOC-Alert

Details

Author	Keijo Korte
Version	1.0
License	AGPL-V3
Requires Registration	Yes
Requires Subscription	Yes
Free Subscription Available	No
DataType Supported	thehive:case_artifact
Service Homepage	MSDefender-PushIOC-Alert

Description

Push IOC to Defender client. Alert mode

Configuration

Name	Description
tenantId	Azure tenant ID
appId	Azure app ID
appSecret	Azure app secret
resourceAppIdUri	Security Center URI, usually doesn't need to change
oAuthUri	Azure oAuth2 authentication endpoint

MSDefender-PushIOC-Block

Details

Author	Keijo Korte
Version	1.0
License	AGPL-V3
Requires Registration	Yes
Requires Subscription	Yes
Free Subscription Available	No
Data Type Supported	thehive:case_artifact
Service Homepage	MSDefender-PushIOC-Block

Description

Push IOC to Defender client. Blocking mode

Configuration

Name	Description
tenantId	Azure tenant ID
appId	Azure app ID
appSecret	Azure app secret
resourceAppIdUri	Security Center URI, usually doesn't need to change
oAuthUri	Azure oAuth2 authentication endpoint

MSDefender-UnisolateMachine

Details

Author	Keijo Korte
Version	1.0
License	AGPL-V3
Requires Registration	Yes
Requires Subscription	Yes
Free Subscription Available	No
DataType Supported	thehive:case_artifact
Service Homepage	MSDefender-UnisolateMachine

Description

Unisolate machine with Microsoft Defender for Endpoints

Configuration

Name	Description
tenantId	Azure tenant ID
appId	Azure app ID
appSecret	Azure app secret
resourceAppIdUri	Security Center URI, usually doesn't need to change
oAuthUri	Azure oAuth2 authentication endpoint

MSDefender-FullVirusscan

Details

Author	Keijo Korte
Version	1.0
License	AGPL-V3
Requires Registration	Yes
Requires Subscription	Yes
Free Subscription Available	No
DataType Supported	thehive:case_artifact
Service Homepage	MSDefender-FullVirusscan

Description

Run full virus scan to machine with Microsoft Defender for Endpoints

Configuration

Name	Description
tenantId	Azure tenant ID
appId	Azure app ID
appSecret	Azure app secret
resourceAppIdUri	Security Center URI, usually doesn't need to change
oAuthUri	Azure oAuth2 authentication endpoint

Additional details from the README file:

Cortex responder for Microsoft Defender for Endpoints (formerly know as Microsoft ATP)

With this responder you can

- Isolate machine
- Unisolate machine
- Run full antivirus scan
- Push IoC to Microsoft defender
 - Alert
 - BlockAndAlert
- (future: Collect investigation package)

NOTE: Microsoft API for finding machines via IP-addresses is little bit limited “Find Machines seen with the requested internal IP in the time range of 15 minutes prior and after a given timestamp.”, because of this “host-name” is preferable observable type”

Responder needs one of the following licenses:

- Windows 10 Enterprise E5
- Microsoft 365 E5 (M365 E5) which includes Windows 10 Enterprise E5
- Microsoft 365 E5 Security

In general, you'll need to take the following steps to use the responder

- Create an Azure AD application
- Grant permissions to App

Steps

With your Global administrator credentials, login to the Azure portal.

- Azure Active Directory > App registrations > New registration.

In the registration form:

- Name - Name your application.
- Supported account type – leave the default setting.
- Redirect Uri – leave empty.

API permission

On your new application page, click API Permissions > Add permission > APIs my organization uses > type **WindowsDefenderATP** and click on WindowsDefenderATP Choose Application permissions, select **Alert.Read.All** AND **TI.ReadWrite.All** AND **Machine.ReadAll** AND **Machine.Isolate** AND **Machine.Scan** > Click on Add permissions.

After clicking the Add Permissions button, on the next screen we need to grant consent for the permission to take effect. Press the “Grant admin consent for {your tenant name}” button.

To get client credentials:

- In your application page, Click Certificate & Secrets
- Specify a key description and set an expiration for 1 year.
- Click Add and the application key will appear.

IMPORTANT: Copy and store this key in a safe place. Treat it like a password.

Detailed permissions:



How to create Azure App (link to MS blog)

7.1.21 MSDefenderOffice365



MSDefenderOffice365_block

Details

Author	Joe Lazaro
Version	1.0
License	AGPL-V3
Requires Registration	Yes
Requires Subscription	Yes
Free Subscription Available	No
DataType Supported	thehive:case_artifact
Service Homepage	MSDefenderOffice365_block

Description

Add entries to the Tenant Allow/Block List in the Microsoft 365 Defender

Configuration

Name	Description
certificate_base64	Base64-encoded PFX certificate to be used for certificate-based authentication.
certificate_password	Password for the certificate used to authenticate
app_id	The application ID of the service principal that's used in certificate based authentication
organization	Tenant ID. Example: something.onmicrosoft.com
block_expiration_days	How many days out should we set the expiration? A value ≤ 0 means to set no expiration.

MSDefenderOffice365_unblock

Details

Author	Joe Lazaro
Version	1.0
License	AGPL-V3
Requires Registration	Yes
Requires Subscription	Yes
Free Subscription Available	No
DataType Supported	thehive:case_artifact
Service Homepage	MSDefenderOffice365_unblock

Description

Add entries to the Tenant Allow/Block List in the Microsoft 365 Defender

Configuration

Name	Description
certificate_base64	Base64-encoded PFX certificate to be used for certificate-based authentication.
certificate_password	Password for the certificate used to authenticate
app_id	The application ID of the service principal that's used in certificate based authentication
organization	Tenant ID. Example: something.onmicrosoft.com

Additional details from the README file:

Microsoft Defender for Office 365 safeguards your organization against malicious threats posed by email messages, links (URLs), and collaboration tools. Defender for Office 365 includes:

- Threat protection policies: Define threat-protection policies to set the appropriate level of protection for your organization.
- Reports: View real-time reports to monitor Defender for Office 365 performance in your organization.
- Threat investigation and response capabilities: Use leading-edge tools to investigate, understand, simulate, and prevent threats.
- Automated investigation and response capabilities: Save time and effort investigating and mitigating threats.

This responder implements support for the Tenant Allow/Block List which is used during mail flow for incoming messages to manually override the Microsoft 365 filtering verdicts. An observable with dataType 'mail' is used to block/unblock a sender, while dataType 'domain' is used to block/unblock a domain.

You can also block or unblock multiple entries at once by using a multi-line observable with one entry per line.

The configuration allows you to specify the number of days for a block entry to live before expiration with a value of 0 meaning no expiration.

For further reference on this capability, see the Microsoft documentation [Allow or block emails using the Tenant Allow/Block List](#).

7.1.22 MailIncidentStatus

MailIncidentStatus

Details

Author	Manuel Krucker
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	thehive:case

Description

Mail a detailed status information of an incident case. The mail is sent to recipients specified by tags prefixed with 'mail='. The responder respects tlp definitions. For tlp:amber mail addresse and for tlp:green mail domains must be pre-defined in the configuration. For tlp:red sending mails is denied. The responder also uses thehive4py to collect information about the status of the tasks of the incidents.

Configuration

Name	Description
from	email address from which the mail is send
smtp_host	SMTP server used to send mail
smtp_port	SMTP server port
smtp_user	SMTP server user
smtp_pwd	SMTP server password
mail_subject_prefix	Prefix of the mail subject
mail_html_style_tag_con	The css content of the style tag for the HTML mail body. Define table, th, hd, .first, and .second elements.
tlp_amber_mail_addresse	Mail addresses which are allowed to receive tlp:amber classified incidents
tlp_green_mail_domains	Mail domains which are allowed to receive tlp:green classified incidents
thehive_url	URL pointing to your TheHive installation, e.g. ' http://127.0.0.1:9000 '
thehive_apikey	TheHive API key which is used get tasks and other elements of the incident

7.1.23 Mailer

Mailer

Details

Author	CERT-BDF
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	thehive:case, thehive:alert, thehive:case_task

Description

Send an email with information from a TheHive case or alert

Configuration

Name	Description
from	email address from which the mail is send
smtp_host	SMTP server used to send mail
smtp_port	SMTP server port
smtp_user	SMTP server user
smtp_pwd	SMTP server password

7.1.24 Minemeld



Minemeld

Details

Author	Wes Lambert, Security Onion Solutions
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	thehive:case_artifact
Service Homepage	Minemeld

Description

Submit indicator to Minemeld

Configuration

Name	Description
minemeld_url	URL for Minemeld instance
minemeld_user	User for Minemeld
minemeld_password	Password for Minemeld
minemeld_indicator_list	Name of indicator list to which indicators will be added
minemeld_share_level	Share level for indicator
minemeld_confidence	Confidence level for indicator
minemeld_ttl	TTL for indicator

Additional details from the README file:

Palo Alto Minemeld

This responder sends observables you select to a [Palo Alto Minemeld](#) instance.

Requirements

The following options are required in the Palo Alto Minemeld Responder configuration:

- `minemeld_url` : URL of the Minemeld instance to which you will be posting indicators
- `minemeld_user`: user accessing the Minemeld instance
- `minemeld_password`: password for the user accessing the Minemeld instance
- `minemeld_indicator_list`: name of Minemeld indicator list (already created in Minemeld)
- `minemeld_share_level`: share level for indicators (defaults to red)
- `minemeld_confidence`: confidence level for indicators (defaults to 100)
- `minemeld_ttl`: TTL for indicators (defaults to 86400 seconds)

7.1.25 PaloAltoCortexXDR



PaloAltoCortexXDR_isolate

Details

Author	Joe Lazaro
Version	1.0
License	AGPL-V3
Requires Registration	Yes
Requires Subscription	Yes
Free Subscription Available	No
DataType Supported	thehive:case_artifact
Service Homepage	PaloAltoCortexXDR_isolate

Description

Isolate endpoints identified by hostname or IP list

Configuration

Name	Description
api_key	API key
api_key_id	API key ID
advanced_security	Set True if the API key was generated with Advanced security level. False for a Standard security key.
api_host	Fully qualified domain name for the API host. Example: api-example.xdr.us.paloaltonetworks.com
iso-polling_interval	Interval, in seconds between requests for isolate or unisolate actions.
iso-max_polling_attempts	Maximum number of time to retry action status when the isolate or unisolate action is still in progress.
allow_multiple_endpoints	Allow the responder to send multiple targets for isolation/unisolation in one multi-line observable.
low_multiple_endpoints	Set to false as a safety mechanism to allow only a single endpoint to be affected while refusing requests to operate on multiple endpoints.

PaloAltoCortexXDR_scan

Details

Author	Joe Lazaro
Version	1.0
License	AGPL-V3
Requires Registration	Yes
Requires Subscription	Yes
Free Subscription Available	No
DataType Supported	thehive:case_artifact
Service Homepage	PaloAltoCortexXDR_scan

Description

Scan endpoints identified by hostname or IP list

Configuration

Name	Description
api_key	API key
api_key_id	API key ID
advanced_security	Set True if the API key was generated with Advanced security level. False for a Standard security key.
api_host	Fully qualified domain name for the API host. Example: api-example.xdr.us.paloaltonetworks.com
scan_polling_interval	Interval, in seconds between requests for scan actions.
scan_max_polling_retri	Maximum number of time to retry action status when a scan action is still in progress.

PaloAltoCortexXDR_unisolate

Details

Author	Joe Lazaro
Version	1.0
License	AGPL-V3
Requires Registration	Yes
Requires Subscription	Yes
Free Subscription Available	No
DataType Supported	thehive:case_artifact
Service Homepage	PaloAltoCortexXDR_unisolate

Description

Unisolate endpoints identified by hostname or IP list

Configuration

Name	Description
api_key	API key
api_key_id	API key ID
advanced_security	Set True if the API key was generated with Advanced security level. False for a Standard security key.
api_host	Fully qualified domain name for the API host. Example: api-example.xdr.us.paloaltonetworks.com
isolate_polling_interval	Interval, in seconds between requests for isolate or unisolate actions.
isolate_max_polling_attempts	Maximum number of time to retry action status when the isolate or unisolate action is still in progress.
allow_multiple_targets	Allow the responder to send multiple targets for isolation/unisolation in one multi-line observable.
low_multiple_targets_safety	Set to false as a safety mechanism to allow only a single endpoint to be affected while refusing requests to operate on multiple endpoints.

Additional details from the README file:

Palo Alto Cortex XDR: Extended Detection and Response

Cortex XDR is the industry's first extended detection and response platform that integrates network, endpoint, cloud, and third-party data to stop sophisticated attacks. Cortex XDR has been designed from the ground up to help organizations secure their digital assets and users while simplifying operations. Using behavioral analytics, it identifies unknown and highly evasive threats targeting your network. Machine learning and AI models uncover threats from any source, including managed and unmanaged devices.

This responder interacts with the Cortex XDR API to support three actions:

- Isolate an endpoint from the network. Prevents a suspected compromised system from causing any further harm to the network.
- Unisolate an endpoint that was previously isolated.
- Scan: initial a full scan of an endpoint.

The responder operates on a 'fqdn' or 'ip' case artifact (observable) from TheHive. The value of the FQDN should be the endpoint name as it appears in the Cortex XDR console.

The responder accepts multiple inputs at once if your observable is multi-line value with one entry per line.

7.1.26 PaloAltoNGFW

PaloAltoNGFW_block_external_IP_address

Details

Author	Maxim Konakin, OSCD Initiative
Version	2.0.0
License	AGPL-V3
Website	https://www.paloaltonetworks.com/
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	thehive:alert, thehive:case_artifact, thehive:case

Description

Block external IP address

Configuration

Name	Description
Hostname_PaloAltoNGFW	Hostname PaloAltoNGFW
User_PaloAltoNGFW	User PaloAltoNGFW
Password_PaloAltoNGFW	User PaloAltoNGFW
Security_rule_for_block_external_IP_address	Name external name security rule for IP address
TheHive_instance	URL of the TheHive instance to query
TheHive_API_key	TheHive API key with read access

PaloAltoNGFW_block_external_domain

Details

Author	Maxim Konakin, OSCD Initiative
Version	2.0.0
License	AGPL-V3
Website	https://www.paloaltonetworks.com/
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	thehive:alert, thehive:case_artifact, thehive:case

Description

Block external domain

Configuration

Name	Description
Hostname_PaloAltoNGFW	Hostname PaloAltoNGFW
User_PaloAltoNGFW	User PaloAltoNGFW
Password_PaloAltoNGFW	User PaloAltoNGFW
Security_rule_for_block_external_domain	Name external security rule for domains
TheHive_instance	URL of the TheHive instance to query
TheHive_API_key	TheHive API key with read access

PaloAltoNGFW_block_external_user

Details

Author	Maxim Konakin, OSCD Initiative
Version	1.0.0
License	AGPL-V3
Website	https://www.paloaltonetworks.com/
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
Data Type Supported	thehive:alert, thehive:case_artifact, thehive:case

Description

Block external user

Configuration

Name	Description
Hostname_PaloAltoNGFW	Hostname PaloAltoNGFW
User_PaloAltoNGFW	User PaloAltoNGFW
Password_PaloAltoNGFW	User PaloAltoNGFW
Security_rule_for_block_external_user	Name security rule for external users
TheHive_instance	URL of the TheHive instance to query
TheHive_API_key	TheHive API key with read access

PaloAltoNGFW_block_internal_IP_address

Details

Author	Maxim Konakin, OSCD Initiative
Version	2.0.0
License	AGPL-V3
Website	https://www.paloaltonetworks.com/
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	thehive:alert, thehive:case_artifact, thehive:case

Description

Block internal IP address

Configuration

Name	Description
Hostname_PaloAltoNGFW	Hostname PaloAltoNGFW
User_PaloAltoNGFW	User PaloAltoNGFW
Password_PaloAltoNGFW	User PaloAltoNGFW
Security_rule_for_block_internal_IP_address	Name internal security rule for IP address
TheHive_instance	URL of the TheHive instance to query
TheHive_API_key	TheHive API key with read access

PaloAltoNGFW_block_internal_domain

Details

Author	Maxim Konakin, OSCD Initiative
Version	2.0.0
License	AGPL-V3
Website	https://www.paloaltonetworks.com/
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	thehive:alert, thehive:case_artifact, thehive:case

Description

Block internal domain

Configuration

Name	Description
Hostname_PaloAltoNGFW	Hostname PaloAltoNGFW
User_PaloAltoNGFW	User PaloAltoNGFW
Password_PaloAltoNGFW	User PaloAltoNGFW
Security_rule_for_block_internal_domain	Name internal security rule for domains
TheHive_instance	URL of the TheHive instance to query
TheHive_API_key	TheHive API key with read access

PaloAltoNGFW_block_internal_user

Details

Author	Maxim Konakin, OSCD Initiative
Version	1.0.0
License	AGPL-V3
Website	https://www.paloaltonetworks.com/
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
Data Type Supported	thehive:alert, thehive:case_artifact, thehive:case

Description

Block internal user

Configuration

Name	Description
Hostname_PaloAltoNGFW	Hostname PaloAltoNGFW
User_PaloAltoNGFW	User PaloAltoNGFW
Password_PaloAltoNGFW	User PaloAltoNGFW
Security_rule_for_block_internal_user	Name internal security rule for users
TheHive_instance	URL of the TheHive instance to query
TheHive_API_key	TheHive API key with read access

PaloAltoNGFW_block_port_for_external_communication

Details

Author	Maxim Konakin, OSCD Initiative
Version	2.0.0
License	AGPL-V3
Website	https://www.paloaltonetworks.com/
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	thehive:alert, thehive:case_artifact, thehive:case

Description

Block external port communication

Configuration

Name	Description
Hostname_PaloAltoNGFW	Hostname PaloAltoNGFW
User_PaloAltoNGFW	User PaloAltoNGFW
Password_PaloAltoNGFW	User PaloAltoNGFW
Security_rule_for_block_port_external_communication	Name external security rule for port communications
TheHive_instance	URL of the TheHive instance to query
TheHive_API_key	TheHive API key with read access

PaloAltoNGFW_block_port_for_internal_communication

Details

Author	Maxim Konakin, OSCD Initiative
Version	2.0.0
License	AGPL-V3
Website	https://www.paloaltonetworks.com/
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	thehive:alert, thehive:case_artifact, thehive:case

Description

Block internal port communication

Configuration

Name	Description
Hostname_PaloAltoNGFW	Hostname PaloAltoNGFW
User_PaloAltoNGFW	User PaloAltoNGFW
Password_PaloAltoNGFW	User PaloAltoNGFW
Security_rule_for_block_port_internal_communication	Name internal security rule for port communications
TheHive_instance	URL of the TheHive instance to query
TheHive_API_key	TheHive API key with read access

PaloAltoNGFW_unblock_external_IP_address

Details

Author	Maxim Konakin, OSCD Initiative
Version	1.0.0
License	AGPL-V3
Website	https://www.paloaltonetworks.com/
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
Data Type Supported	thehive:alert, thehive:case_artifact, thehive:case

Description

Unblock external ip

Configuration

Name	Description
Hostname_PaloAltoNGFW	Hostname PaloAltoNGFW
User_PaloAltoNGFW	User PaloAltoNGFW
Password_PaloAltoNGFW	User PaloAltoNGFW
Address_group_for_external_IP_address	Name external Address Group for IP address
TheHive_instance	URL of the TheHive instance to query
TheHive_API_key	TheHive API key with read access

PaloAltoNGFW_unblock_external_domain

Details

Author	Maxim Konakin, OSCD Initiative
Version	1.0.0
License	AGPL-V3
Website	https://www.paloaltonetworks.com/
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	thehive:alert, thehive:case_artifact, thehive:case

Description

Unblock external domain

Configuration

Name	Description
Hostname_PaloAltoNGFW	Hostname PaloAltoNGFW
User_PaloAltoNGFW	User PaloAltoNGFW
Password_PaloAltoNGFW	User PaloAltoNGFW
Address_group_for_unblock_external_domain	Name external Address Group for domains
TheHive_instance	URL of the TheHive instance to query
TheHive_API_key	TheHive API key with read access

PaloAltoNGFW_unblock_external_user

Details

Author	Maxim Konakin, OSCD Initiative
Version	1.0.0
License	AGPL-V3
Website	https://www.paloaltonetworks.com/
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	thehive:alert, thehive:case_artifact, thehive:case

Description

Unblock external user

Configuration

Name	Description
Hostname_PaloAltoNGFW	Hostname PaloAltoNGFW
User_PaloAltoNGFW	User PaloAltoNGFW
Password_PaloAltoNGFW	User PaloAltoNGFW
Security_rule_for_block_external_user	Name security rule for external users
TheHive_instance	URL of the TheHive instance to query
TheHive_API_key	TheHive API key with read access

PaloAltoNGFW_unblock_internal_IP_address

Details

Author	Maxim Konakin, OSCD Initiative
Version	1.0.0
License	AGPL-V3
Website	https://www.paloaltonetworks.com/
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
Data Type Supported	thehive:alert, thehive:case_artifact, thehive:case

Description

Unblock internal ip

Configuration

Name	Description
Hostname_PaloAltoNGFW	Hostname PaloAltoNGFW
User_PaloAltoNGFW	User PaloAltoNGFW
Password_PaloAltoNGFW	User PaloAltoNGFW
Address_group_for_internal_IP_address	Name internal Address Group for IP address
TheHive_instance	URL of the TheHive instance to query
TheHive_API_key	TheHive API key with read access

PaloAltoNGFW_unblock_internal_domain

Details

Author	Maxim Konakin, OSCD Initiative
Version	1.0.0
License	AGPL-V3
Website	https://www.paloaltonetworks.com/
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	thehive:alert, thehive:case_artifact, thehive:case

Description

Unblock internal domain

Configuration

Name	Description
Hostname_PaloAltoNGFW	Hostname PaloAltoNGFW
User_PaloAltoNGFW	User PaloAltoNGFW
Password_PaloAltoNGFW	User PaloAltoNGFW
Address_group_for_unblock_internal_domain	Name internal Address Group for domains
TheHive_instance	URL of the TheHive instance to query
TheHive_API_key	TheHive API key with read access

PaloAltoNGFW_unblock_internal_user

Details

Author	Maxim Konakin, OSCD Initiative
Version	1.0.0
License	AGPL-V3
Website	https://www.paloaltonetworks.com/
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	thehive:alert, thehive:case_artifact, thehive:case

Description

Unblock internal user

Configuration

Name	Description
Hostname_PaloAltoNGFW	Hostname PaloAltoNGFW
User_PaloAltoNGFW	User PaloAltoNGFW
Password_PaloAltoNGFW	User PaloAltoNGFW
Security_rule_for_block_internal_user	Name security rule for internal users
TheHive_instance	URL of the TheHive instance to query
TheHive_API_key	TheHive API key with read access

PaloAltoNGFW_unblock_port_for_external_communication

Details

Author	Maxim Konakin, OSCD Initiative
Version	1.0.0
License	AGPL-V3
Website	https://www.paloaltonetworks.com/
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	thehive:alert, thehive:case_artifact, thehive:case

Description

Unblock external port communication

Configuration

Name	Description
Hostname_PaloAltoNGFW	Hostname PaloAltoNGFW
User_PaloAltoNGFW	User PaloAltoNGFW
Password_PaloAltoNGFW	User PaloAltoNGFW
Service_group_for_external_port_communication	Name external Service Group for port communication
TheHive_instance	URL of the TheHive instance to query
TheHive_API_key	TheHive API key with read access

PaloAltoNGFW_unblock_port_for_internal_communication

Details

Author	Maxim Konakin, OSCD Initiative
Version	1.0.0
License	AGPL-V3
Website	https://www.paloaltonetworks.com/
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	thehive:alert, thehive:case_artifact, thehive:case

Description

Unblock internal port communication

Configuration

Name	Description
Hostname_PaloAltoNGFW	Hostname PaloAltoNGFW
User_PaloAltoNGFW	User PaloAltoNGFW
Password_PaloAltoNGFW	User PaloAltoNGFW
Service_group_for_internal_port_communication	Name internal Service Group for port communication
TheHive_instance	URL of the TheHive instance to query
TheHive_API_key	TheHive API key with read access

Additional details from the README file:

Description of the responder module operation for the Palo Alto NGFW system

This description contains the required actions from the engineer to integrate the responder with the Palo Alto NGFW.

Installation

need install:

1. pip install cortexutils
2. pip install requests
3. pip install pan-os-python
4. pip install thehive4py

ToDo

For responders to work, you need to upload the PaloAltoNGFW folder to the directory where other responders are stored. Further it is necessary:

- Reboot the cortex system;
- To configure the responder, go to the cortex web console, go to the “Organization” tab, select the organization for which the configuration will be performed and go to the “Responders Config” tab and configure the fields for “PaloAltoNGFW_main” in accordance with their values:



07-0-0-Integrations/Responders/PaloAltoNGFW/assets/Responders.jpg

1. Hostname_PaloAltoNGFW - network address of the PaloAltoNGFW system
 2. User_PaloAltoNGFW - user in the PaloAltoNGFW system
 3. Password_PaloAltoNGFW - password for the user in the PaloAltoNGFW system
 4. Securityrule* - the name of the security rule in the PaloAltoNGFW system. The following standard rule names have been established: 4.1 To block/unblock user: 4.1.1 “TheHive Block internal user” 4.1.2 “TheHive Block external user”
- 4.2 To block/unblock network addresses: 4.2.1 “TheHive Block internal IP address” 4.2.2 “TheHive Block external IP address”
- 4.3 To block/unblock FQDN: 4.3.1 “TheHive Block external Domain” 4.3.2 “TheHive Block internal Domain”
- 4.4 To block/unblock ports: 4.4.1 “TheHive Block port for internal communication” 4.4.2 “TheHive Block port for external communication”
- 4.5 TheHive_instance - url address of The Hive system (used only for case and alert types). It is important for each organization to have its own user with the API!
- 4.6 TheHive_API_key - API key to connect to TheHive system Note: the specified safety rules must be created in PaloAltoNGFW, and also placed in the order of their application. Types of data used to work in TheHive system:
1. Network address - ‘ip’
 2. FQDN - ‘hostname’
 3. port-protocol - ‘port-protocol’
 4. Username - ‘username’ Note: types ‘port-protocol’ and ‘username’ need to be created in TheHive system. By default, TheHive does not have these data types in the Observable type, so you must add it in the admin settings.



07-0-0-Integrations/Responders/PaloAltoNGFW/assets/AddObservableType.jpg

7.1.27 QRadarAutoClose

QRadar_Auto_Closing_Offense

Details

Author	Florian Perret
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	thehive:case

Description

Closing the QRadar Offense associated to your case in one clic !

Configuration

Name	Description
QRadar_API_Key	A QRadar API key with sufficient rights to close an offense
QRadar_Url	URL of your QRadar API, must be accessible from Cortex server. eg: myqradar.myorg.com/api/siem/offenses
Cert_Path	If you need a certificate to authenticate to your QRadar API, please provide the path here

Additional details from the README file:

Simple responder to close a QRadar Offense through a simple clic !

If you need to change the customfield which contain the QRadar Offense ID, change the “externalReferences” from QRadarAutoClose.py line 15. Be careful this have to be fulfill with the “Internal Reference” of the customfield, not it’s name !

7.1.28 RT4

RT4-CreateTicket

Details

Author	Michael Davis, REN-ISAC
Version	1.0
License	MIT
Website	https://github.com/TheHive-Project/Cortex-Analyzers/tree/master/responders/RT4
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	thehive:case_artifact, thehive:alert, thehive:case

Description

Cortex Responder to create a ticket in RT4 from TheHive observables or alerts

Configuration

Name	Description
server	RT4 Base URL, e.g., https://rt.domain.local
username	RT4 username for authentication
password	RT4 password for user account
Queue	Default queue in which to create new tickets
Owner	Default owner to assign newly created tickets (optional)
Status	Default ticket status to assign newly created tickets (optional)
cus- tom_field_list	Name:Value of Custom Fields in RT to set on every ticket created (e.g.: 'How Reported:TheHive' sets CF.{How Reported} = TheHive on every new ticket)
tag_to_templat	Mapping table of tags to templates (e.g.: 'phishing:phish_letter' maps anything tagged as 'phishing' to the 'phish_letter' template)
the- hive_cf_rtticke	Name of a case custom field in TheHive in which RT ticket #s will be saved upon successful case-level Responder run (optional)
thehive_url	TheHive Base URL, e.g., https://thehive.domain.local:9000 (optional: only needed to process Cases)
the- hive_token	TheHive API token for authentication (optional: only needed to process Cases)

Additional details from the README file:

Request Tracker 4 Cortex Responder

Summary: Creates RT tickets from TheHive

Applies To: Case Observables (Artifacts), Alerts, Cases

Initial Responder Configuration

The following need to be configured under **Organization** → **Responders** prior to use:

server - **Required** - RT4 base URL, e.g.: <https://rt.domain.local>

username - **Required** - RT4 username for API authentication

password - **Required** - RT4 password for user account above

Queue - **Required** - Default queue in which to create new tickets (can be overridden by custom tag on observables)

Owner - Default owner to assign newly created tickets (Optional - can be overridden by custom tags per observable)

Status - Default status to assign newly created tickets (Optional - can be overridden by custom tags per observable)

custom_field_list - Colon-separated Name:Value pairs of RT custom fields and values to set across all newly-created tickets (Optional - can be overridden by custom tags per observable) - adding a value of `How Reported:TheHive` would set the custom field named `How Reported` to `TheHive` on all newly created tickets

tag_to_template_map - **Required** - Tags to Templates mapping (can be overridden by custom tag on observables). Should be colon-separated tag-to-template values. E.g.

thehive_cf_rtticket - Name of a case custom field in TheHive in which RT ticket #s will be saved upon successful case-level Responder run (Optional - TheHive Custom Field should be of type 'String')

thehive_url - TheHive Base URL, e.g., <https://thehive.domain.local:9000> (Optional - only needed to process Cases)

thehive_token - TheHive API token for authentication (Optional - only needed to process Cases)

```
phishing:phishing_generic
spear_phishing:phishing_spear
```

Any observable with a `phishing` tag would be assigned the template named `phishing_generic`. Any observable tagged `spear_phishing` would have its ticket created with a body from the `phishing_spear` template.

Workflow

1. Set *Initial Responder Configuration*
2. Create *Template(s)*
3. As new observables arrive, appropriately *tag* them
4. Run the RT4-CreateTicket responder
5. When complete, the ticket(s) should be created and the `thehive_cf_rtticket` custom field on TheHive cases (if present) should be populated with the URL to any created ticket

Templates

Inside the `./templates` dir of the RT4 responder, you will need to create the templates for subjects and notification bodies that will be used on ticket creation. For the above example on an observable tagged to use the `phishing_generic` template, there should be a file inside `./templates/` called `phishing_generic.j2` (all templates should end in the `.j2` extension since it uses Jinja2 templating)

The `.j2` files should be formatted like so:

```
{% block Subject %}
[SOC] ** Notification ** Phishing Site Targeting Your Organization
{% endblock %}

{% block Text %}
Greetings,

We have recently discovered a potential phishing site targeting employees at your_
organization:

Domain(s):
{{ indicator_list }}

On behalf of the SOC,

--
soc@org.local
24x7 Watch Desk
https://www.org.local
{% endblock %}
```

The mandatory blocks are Subject and Text inside which are the respective content for the ticket creation. You may reference any variables inside the template file which exist in the observable/artifact/alert/case for population of other data within the ticket notification (in the above case, `indicator_list`). Those variables should be inside double curly-braces as is the format for Jinja. Example data available in the *Observable Object Data* section.

Inside the jinja2 template, all block names are passed at RT ticket variables with their respective block values upon ticket creation. Therefore, any number of blocks corresponding to RT fields can also be assigned to further customize setting ticket variables at the template level.

Example:

```
{% block CF_Classification %}Phishing{% endblock %}
```

Every ticket created from that template will have the RT custom field CF_Classification set to “Phishing” upon ticket creation.

Tags to Modify RT4 Responder Behavior

Set any of the following tags to modify behavior of the created ticket:

`rt4_set_requestor:customer@domain.local` or `contact:customer@domain.local` - **Required** - This is the only tag that must be present. Without one of these, the ticket won't be created.

`rt4_set_cf_Classification:phishing` - sets the CF.{Classification} = 'phishing' in RT ticket

`rt4_set_cc:staff@domain.local` - adds `staff@domain.local` as Cc on ticket

`rt4_set_admincc:emp@domain.local` - sets AdminCc of ticket to `emp@domain.local`

`rt4_set_owner:staff@domain.local` - sets Owner of ticket to `staff@domain.local` (**must match person in RT or ticket creation will fail**)

`rt4_set_queue:Incident Reports` - sets Queue of ticket created to *Incident Reports*

`rt4_set_subject:This is a test` - overrides the Subject line from the template with *This is a test*

`rt4_set_status:Resolved` - creates the ticket and then sets its status to *Resolved* (can also use any other ticket status in your RT instance)

`rt4_set_template:phishing_generic` - overrides any default template from `tag_to_template_map` setting when constructing the body of the notification, in this case instructing the Responder to use the `phishing_generic` template

Ticket customization order

As already alluded to, there are 4 ways to customize ticket creation options:

1. Global level
 - Queue
 - Owner
 - Status
 - Custom Fields
 - Template
2. Template level
 - All of the above except Template, plus:
 - Requestor/Cc/AdminCc
3. Case/Alert level
 - All RT options
4. Case artifact/observable level
 - All RT options

Greater numbered config options take precedence over smaller ones.

Example:

If a `tag_to_template` map at the Org Responder config in Cortex is set to map tags of `phishing` to the `phishing_generic` template, but a `set_rt4_template:phishing_spear` tag on the observable sets a different template, the observable tag takes precedence.

Observable Object Data

Observables are a custom dictionary in which their properties are stored. In addition to the ticket properties passed to RT, each observable is also tagged with its case/artifact info which makes available the following info in each observable:

```
"owner": "michael",
"severity": 2,
"_routing": "AWxyhvveZCX08BqIWSLs",
"flag": false,
"updatedBy": "michael",
"customFields": {
  "RTTicket": {
    "string": "http://192.168.0.2/Ticket/Display.html?id=141, http://192.168.0.2/
↪Ticket/Display.html?id=142, http://192.168.0.2/Ticket/Display.html?id=143"
  }
},
```

(continues on next page)

(continued from previous page)

```

"_type": "case",
"description": "test",
"title": "RT-testing",
"tags": [
  "contact:requestor@domain.tld",
  "rt4:submitted"
],
"createdAt": 1565289544365,
"_parent": null,
"createdBy": "michael",
"caseId": 1,
"tlp": 2,
"metrics": {
  "seen_prior": 1
},
"_id": "AWxyhvveZCX08BqIWSLs",
"id": "AWxyhvveZCX08BqIWSLs",
"_version": 45,
"startDate": 1565289480000,
"pap": 2,
"status": "Open",
"updatedAt": 1570482005825,
"indicator_list": [
  "malicious.baddomain.tld"
]

```

Those properties can all be referenced as variables in the jinja2 template as mentioned in the *Templates* section.

7.1.29 Redmine

Redmine_Issue

Details

Author	Marc-André DOLL
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	thehive:case, thehive:case_task

Description

Create a redmine issue from a case

Configuration

Name	Description
in-stance_name	Name of the Redmine instance
url	URL where to find the Redmine API
username	Username to log into Redmine
password	Password to log into Redmine
project_field	Name of the custom field containing the Redmine project to use when creating the issue
tracker_field	Name of the custom field containing the Redmine tracker to use when creating the issue
as-signee_field	Name of the custom field containing the Redmine assignee to use when creating the issue
reference_field	Name of the case custom field in which to store the opened issue. If not defined, this information will not be stored
opening_status	Status used when opening a Redmine issue (if not defined here, will use the default opening status from the Redmine Workflow)
closing_task	Closing the task after successfully creating the Redmine issue

7.1.30 RiskIQ

RiskIQ_PushArtifactToProject

Details

Author	RiskIQ
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	thehive:case_artifact

Description

Push a case to a RiskIQ Illuminate project.

Configuration

Name	Description
username	API username of the RiskIQ Illuminate or PassiveTotal account (usually an email address)
api_key	API key of the RiskIQ Illuminate or PassiveTotal account
project_visibility	Visibility for new RiskIQ Illuminate projects (analyst, team, or public).
project_prefix	Prefix to add when auto-generating project names from case names.
the-hive_artifact_tag	Tag to apply to artifact in TheHive when it has been pushed to a RiskIQ Illuminate Project (leave blank to skip tagging).
riq_artifact_tag	Tag to apply to artifact in RiskIQ Illuminate when it has been pushed to an Illuminate Project (leave blank to skip tagging).

7.1.31 RunWorkflow

RunWorkflow

Details

Author	EMCA Software
Version	1.1
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	thehive:case, thehive:alert, thehive:case_task

Description

Run Workflow by id

Configuration

Name	Description
url	Webhook URL
api_key	API key for authorization
VerifySSL	Set to false to bypass SSL verification

7.1.32 SEPBlockHash

Symantec Endpoint Protection Block Hash

Details

Author	EMCA Software
Version	0.1
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	thehive:case_artifact

Description

SEP Block Hash

Configuration

Name	Description
base_url	SEP URL
username	API user
password	API user Password
domain	SEP domain

7.1.33 SEPQuarantineHost

Symantec Endpoint Protection Quarantine Host

Details

Author	EMCA Software
Version	0.1
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	thehive:case_artifact

Description

SEP Quarantine Host by Computer ID

Configuration

Name	Description
base_url	SEP URL
username	API user
password	API user Password
domain	SEP domain

7.1.34 SEPUnblockHash

Symantec Endpoint Protection Unblock Hash

Details

Author	EMCA Software
Version	0.1
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	thehive:case_artifact

Description

SEP Unblock Hash

Configuration

Name	Description
base_url	SEP URL
username	API user
password	API user Password
domain	SEP domain

7.1.35 SEPUnquarantineHost

Symantec Endpoint Protection Unquarantine Host

Details

Author	EMCA Software
Version	0.1
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	thehive:case_artifact

Description

SEP Unquarantine Host by Computer ID

Configuration

Name	Description
base_url	SEP URL
username	API user
password	API user Password
domain	SEP domain

7.1.36 SMGBlockDomain

Symantec Messaging Gateway Block Domain

Details

Author	EMCA Software
Version	0.1
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	thehive:case_artifact

Description

Symantec Messaging Gateway Domain Block

Configuration

Name	Description
smg_ip	SMG Server IP
username	Admin User
password	Admin User Password
BAD_DOMAINS_EMAILS_GROUP	BAD DOMAINS EMAILS GROUP Name
BAD_IPs_GROUP	BAD IPs GROUP Name

7.1.37 SMGBlockEmail

Symantec Messaging Gateway Block Email

Details

Author	EMCA Software
Version	0.1
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	thehive:case_artifact

Description

Symantec Messaging Gateway Email Block

Configuration

Name	Description
smg_ip	SMG Server IP
username	Admin User
password	Admin User Password
BAD_DOMAINS_EMAILS_GROUP	BAD DOMAINS EMAILS GROUP Name
BAD_IPs_GROUP	BAD IPs GROUP Name

7.1.38 SMGBlockIP

Symantec Messaging Gateway Block IP

Details

Author	EMCA Software
Version	0.1
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	thehive:case_artifact

Description

Symantec Messaging Gateway IP Block

Configuration

Name	Description
smg_ip	SMG Server IP
username	Admin User
password	Admin User Password
BAD_DOMAINS_EMAILS_GROUP	BAD DOMAINS EMAILS GROUP Name
BAD_IPs_GROUP	BAD IPs GROUP Name

7.1.39 SMGUnblockDomain

Symantec Messaging Gateway Unblock Domain

Details

Author	EMCA Software
Version	0.1
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	thehive:case_artifact

Description

Symantec Messaging Gateway Domain Unblock

Configuration

Name	Description
smg_ip	SMG Server IP
username	Admin User
password	Admin User Password
BAD_DOMAINS_EMAILS_GROUP	BAD DOMAINS EMAILS GROUP Name
BAD_IPs_GROUP	BAD IPs GROUP Name

7.1.40 SMGUnblockEmail

Symantec Messaging Gateway Unblock Email

Details

Author	EMCA Software
Version	0.1
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	thehive:case_artifact

Description

Symantec Messaging Gateway Email Unblock

Configuration

Name	Description
smg_ip	SMG Server IP
username	Admin User
password	Admin User Password
BAD_DOMAINS_EMAILS_GROUP	BAD DOMAINS EMAILS GROUP Name
BAD_IPs_GROUP	BAD IPs GROUP Name

7.1.41 SMGUnblockIP

Symantec Messaging Gateway Unblock IP

Details

Author	EMCA Software
Version	0.1
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	thehive:case_artifact

Description

Symantec Messaging Gateway IP Unblock

Configuration

Name	Description
smg_ip	SMG Server IP
username	Admin User
password	Admin User Password
BAD_DOMAINS_EMAILS_GROUP	BAD DOMAINS EMAILS GROUP Name
BAD_IPs_GROUP	BAD IPs GROUP Name

7.1.42 SendGrid

SendGrid

Details

Author	Equate Technologies
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	thehive:case, thehive:alert

Description

Send an email with information from a TheHive case or alert via SendGrid API over HTTPS

Configuration

Name	Description
from	Email address to use as the From: field
api_key	SendGrid API key

7.1.43 SentinelOne

SentinelOne-Unisolate

Details

Author	EMCA Software
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	thehive:case_artifact

Description

Reconnect a host in SentinelOne

Configuration

Name	Description
s1_console_url	SentinelOne console URL
s1_api_key	SentinelOne API Key
s1_account_id	SentinelOne Account ID
s1_verify_ssl	Verify SSL Certificate

SentinelOne-Scan

Details

Author	EMCA Software
Version	1.0
License	AGPL-V3
Requires Registration	Yes
Requires Subscription	Yes
Free Subscription Available	No
DataType Supported	thehive:case_artifact

Description

Initiate a scan on SentinelOne

Configuration

Name	Description
s1_console_url	S1 console URL
s1_api_key	S1 API key
s1_account_id	Account ID
s1_verify_ssl	Verify SSL

SentinelOne-Isolate

Details

Author	EMCA Software
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	thehive:case_artifact

Description

Isolate a host in SentinelOne

Configuration

Name	Description
s1_console_url	SentinelOne console URL
s1_api_key	SentinelOne API Key
s1_account_id	SentinelOne Account ID
s1_verify_ssl	Verify SSL Certificate

7.1.44 Shuffle

Shuffle

Details

Author	@frikkylikeme
Version	1.0
License	AGPL-V3
Website	https://github.com/frikky/shuffle
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	thehive:case, thehive:alert

Description

Execute a workflow in Shuffle

Configuration

Name	Description
url	The URL to your shuffle instance
api_key	The API key to your Shuffle user
workflow_id	The ID of the workflow to execute

7.1.45 UmbrellaBlacklister

Umbrella_Blacklister

Details

Author	Kyle Parrish
Version	1.1
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	thehive:case_artifact

Description

Add domain to Umbrella blacklist via Enforcement API.

Configuration

Name	Description
integration_url	Custom integration url

7.1.46 Velociraptor

Velociraptor_Flow

Details

Author	Wes Lambert
Version	0.1
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	thehive:case_artifact

Description

Run Velociraptor flow

Configuration

Name	Description
velociraptor_client_config	Path to API client config file
velociraptor_artifact	Artifact to collect
upload_flow_results	Upload the results of a flow as an observable
thehive_url	URL pointing to your TheHive installation, e.g. <code>'http://127.0.0.1:9000'</code>
thehive_apikey	TheHive API key (used to add the downloaded file back to the alert/case)

Additional details from the README file:

Velociraptor

This responder can be used to run a flow for a Velociraptor artifact. This could include gathering data, or performing initial response, as the artifact (or artifact “pack”) could encompass any number of actions. The responder can be run on an observable type of `ip`, `fqdn`, or `other`, and will look for a matching client via the Velociraptor server. If a client match is found for the last seen IP, or the hostname, the responder will kick off the flow, the results will be returned, and the client ID will be added as a tag to the case and the observable.

Requirements

The following options are required in the Velociraptor Responder configuration:

- `velociraptor_client_config`: The path to the Velociraptor API client config. (See the following for generating an API client config: <https://www.velocidex.com/docs/user-interface/api/>, and ensure the appropriate ACLs are granted to the API user).
- `velociraptor_artifact`: The name artifact you which to collect (as you would see it in the Velociraptor GUI).
- `upload_flow_results`: Upload flow results to TheHive case (bool).
- `thehive_url`: URL of your TheHive installation (e.g. `'http://127.0.0.1:9000'`).
- `thehive_apikey`: TheHive API key used to add flow results/file(s) to a case.

7.1.47 VirustotalDownloader

Virustotal_Downloader

Details

Author	Mario Henkel @hariomenkel
Version	0.1
License	AGPL-V3
Requires Registration	Yes
Requires Subscription	Yes
Free Subscription Available	No
DataType Supported	thehive:case_artifact
Service Homepage	Virustotal_Downloader

Description

Download a file from Virustotal by its hash

Configuration

Name	Description
virustotal_apikey	Virustotal API key which should be used to download files
thehive_url	URL pointing to your TheHive installation, e.g. <code>'http://127.0.0.1:9000'</code>
thehive_apikey	TheHive API key which is used to add the downloaded file back to the alert/case

Additional details from the README file:

VirusTotalDownloader

This responder comes in only 1 flavor that lets you download a sample of malware from VirusTotal by submitting a hash.

Requirements

This responder need a valid Premium API key from VirusTotal as the `virustotal_apikey` parameter in the configuration. To add the sample in Observables in TheHive, the responder also requires the URL of TheHive as the `thehive_url` parameter and a valid API key as the `thehive_apikey` parameter.

7.1.48 Wazuh

Wazuh

Details

Author	Wes Lambert
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	thehive:case, thehive:case_artifact

Description

Block an IP on a host via Wazuh agent

Configuration

Name	Description
wazuh_manager	URL for Wazuh Manager
wazuh_user	User for Wazuh Manager
wazuh_password	Password for Wazuh Manager

7.1.49 ZEROFOX_Close_alert

ZEROFOX_Close_alert

Details

Author	TheHive-Project
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	thehive:case

Description

Close alert in Zerofox

Configuration

Name	Description
url	URL for Zerofox API
api	Key API for Zerofox

7.1.50 ZEROFOX_Takedown_request

ZEROFOX_Takedown_request

Details

Author	TheHive-Project
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	thehive:case

Description

Request for a takedown regarding the alert in Zerofox

Configuration

Name	Description
url	URL for Zerofox API
api	Key API for Zerofox

7.2 Analyzers

7.2.1 AbuseIPDB



AbuseIPDB

Details

Author	Matteo Lodi
Version	1.0
License	AGPL-v3
Requires Registration	Yes
Requires Subscription	Yes
Free Subscription Available	Yes
DataType Supported	ip
Service Homepage	AbuseIPDB

Description

Determine whether an IP was reported or not as malicious by AbuseIPDB

Configuration

Name	Description
key	API key for AbuseIPDB
days	Check for IP Reports in the last X days

Additional details from the README file:

AbuseIPDB

[AbuseIPDB](#) is a project dedicated to helping combat the spread of hackers, spammers, and abusive activity on the internet.

The analyzer comes in only one flavor.

Requirements

You need a valid AbuseIPDB API integration subscription to use the analyzer:

- Provide your API key as a value for the `key` parameter.
- Set the `days` parameter to limit temporal range in search

7.2.2 Abuse_Finder

Abuse_Finder

Details

Author	CERT-BDF
Version	3.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	ip, domain, fqdn, url, mail
Service Homepage	Abuse_Finder

Description

Find abuse contacts associated with domain names, URLs, IPs and email addresses.

Configuration

Name	Description
------	-------------

Additional details from the README file:

Abuse_Finder

Use CERT-SG's [Abuse Finder](#) to find abuse contacts associated with domain names, URLs, IPs and email addresses.

The analyzer comes in only one flavor.

No configuration is required. It can be used out of the box.

This Analyzer can only be run as a docker container or as process with Python <= 3.6.

7.2.3 AnyRun

AnyRun_Sandbox_Analysis

Details

Author	Andrea Garavaglia, Davide Arcuri, LDO-CERT
Version	1.0
License	AGPL-V3
Requires Registration	Yes
Requires Subscription	Yes
Free Subscription Available	No
DataType Supported	file, url
Service Homepage	AnyRun_Sandbox_Analysis

Description

Any.Run Sandbox file analysis

Configuration

Name	Description
token	API token
privacy_type	Define the privacy setting (Allowed values: public, bylink, owner)
verify_ssl	Verify SSL certificate

Additional details from the README file:

AnyRun

ANY.RUN is a malware sandbox service in the cloud. By using this analyzer, an analyst can submit a suspicious file or URL to the service for analysis and get a report. The report can contain various information such as:

- Interactive access
- Research threats by filter in public submissions
- File and URL dynamic analysis
- Mitre ATT&CK mapping
- Detailed malware reports

Requirements

You need a valid AnyRun API integration subscription to use the analyzer. Free plan does not provide API access.

- Provide your API token as a value for the `token` parameter.
- Define the privacy setting in `privacy_type` parameter.
- Set `verify_ssl` parameter as false if you connection requires it

7.2.4 Autofocus

Autofocus_GetSampleAnalysis

Details

Author	ANSSI
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	hash

Description

Get full analysis from a sample based on its hash

Configuration

Name	Description
apikey	Autofocus API key

Autofocus_SearchIOC

Details

Author	ANSSI
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	domain, fqdn, user-agent, imphash, ip, mutex, tag, url

Description

Search samples in Autofocus based on a single IOC

Configuration

Name	Description
apikey	Autofocus API key

Autofocus_SearchJSON

Details

Author	ANSSI
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	other

Description

Search samples in Autofocus with a full search query in JSON

Configuration

Name	Description
apikey	Autofocus API key

7.2.5 BackscatterIO

BackscatterIO_Enrichment

Details

Author	brandon@backscatter.io
Version	1.0
License	APLv2
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	ip, network, autonomous-system, port

Description

Enrich values using Backscatter.io data.

Configuration

Name	Description
key	API key for Backscatter.io

BackscatterIO_GetObservations

Details

Author	brandon@backscatter.io
Version	1.0
License	APLv2
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	ip, network, autonomous-system

Description

Determine whether a value has known scanning activity using Backscatter.io data.

Configuration

Name	Description
key	API key for Backscatter.io

7.2.6 BitcoinAbuse

BitcoinAbuse

Details

Author	Peter Juhas
Version	1.0
License	AGPL-V3
Website	https://github.com/pjuhas/Cortex-Analyzers
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	btc_address

Description

Check Bitcoin address against Bitcoin Abuse database

Configuration

Name	Description
key	API key for Bitcoin Abuse

7.2.7 C1fApp

C1fApp

Details

Author	etz69
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	url, domain, fqdn, ip

Description

Query C1fApp OSINT Aggregator for IPs, domains and URLs

Configuration

Name	Description
url	URL of C1fApp service
key	API key

7.2.8 CERTatPassiveDNS

CERTatPassiveDNS

Details

Author	Nils Kuhnert, CERT-Bund
Version	2.0
License	AGPL-V3
Website	https://github.com/BSI-CERT-Bund/cortex-analyzers
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	domain, fqdn, ip

Description

Checks CERT.at Passive DNS for a given domain.

Configuration

Name	Description
limit	Define the maximum number of results per request

7.2.9 CIRCLHashlookup



CIRCLHashlookup

Details

Author	Mikael Keri
Version	1.1
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	Yes
DataType Supported	hash
Service Homepage	CIRCLHashlookup

Description

CIRCL hashlookup uses a public API to lookup hash values against databases of known good files

Configuration

Name	Description
------	-------------

7.2.10 CIRCLPassiveDNS



CIRCLPassiveDNS

Details

Author	Nils Kuhnert, CERT-Bund
Version	2.0
License	AGPL-V3
Website	https://github.com/BSI-CERT-Bund/cortex-analyzers
Requires Registration	Yes
Requires Subscription	Yes
Free Subscription Available	Yes
DataType Supported	domain, url, ip
Service Homepage	CIRCLPassiveDNS

Description

Check CIRCL's Passive DNS for a given domain or URL.

Configuration

Name	Description
user	Username
password	Password

Additional details from the README file:

CIRCLPassiveDNS

Check CIRCL's Passive DNS for a
given domain.

This analyzer comes in only one flavor.

Requirements

Access to CIRCL Passive DNS is only allowed to trusted partners in Luxembourg and abroad. [Contact CIRCL](#) if you would like access. Include your affiliation and the foreseen use of the Passive DNS data.

If the CIRCL positively answers your access request, you'll obtain a username
and password which are needed to make the analyzer work.

supply your username as the value for the `user` parameter and your password as the value for the `password` parameter.

7.2.11 CIRCLPassiveSSL



CIRCLPassiveSSL

Details

Author	Nils Kuhnert, CERT-Bund
Version	2.0
License	AGPL-V3
Website	https://github.com/BSI-CERT-Bund/cortex-analyzers
Requires Registration	Yes
Requires Subscription	Yes
Free Subscription Available	Yes
DataType Supported	ip, certificate_hash, hash
Service Homepage	CIRCLPassiveSSL

Description

Check CIRCL's Passive SSL for a given IP address or a X509 certificate hash.

Configuration

Name	Description
user	Username
password	Password

Additional details from the README file:

CIRCLPassiveSSL

Check [CIRCL's Passive SSL](#) service for a given IP address or certificate hash.

This analyzer comes in only one flavor.

Requirements

Access to CIRCL Passive SSL is allowed to partners including security researchers or incident analysts worldwide. [Contact CIRCL](#) if you would like access.

If the CIRCL positively answers your access request, you'll obtain a username and password which are needed to make the analyzer work.

Supply your username as the value for the user parameter and your password as the value for the password parameter.

7.2.12 CISMCAAP



MCAP

Malicious Code Analysis Platform

CISMCAAP

Details

Author	Joe Lazaro
Version	1.0
License	AGPL-V3
Requires Registration	Yes
Requires Subscription	No
Free Subscription Available	No
DataType Supported	ip, hash, url, domain, fqdn, file
Service Homepage	CISMCAAP

Description

Malicious Code Analysis Platform (MCAP) by the Center for Internet Security (CIS). Submit files for analysis or check feeds for known indicators of compromise for other data types.

Configuration

Name	Description
key	API key
private_samples	Submitted samples will not be shared with other members of the portal
minimum_confidence	Restrict to IOCs with this confidence score or higher.
minimum_severity	Restrict to IOCs with this severity score or higher.
polling_interval	Interval (seconds) between requests for sample status.
max_sample_result_wait	Maximum time to retry requests for sample status.

Additional details from the README file:

The Center for Internet Security, Inc. (CIS®) makes the connected world a safer place for people, businesses, and governments through our core competencies of collaboration and innovation. CIS is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), the trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities, and the Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®), which supports the rapidly changing cybersecurity needs of U.S. elections offices.

Malicious Code Analysis Platform (MCAP) is a no-cost web-based sandbox which enables MS-ISAC and EI-ISAC members to submit suspicious files such as executables, DLLs, documents, quarantine files, and archives for analysis in a controlled and non-public fashion. The platform also enables users to perform threat analysis based on domain, IP address, URL, hashes, and various Indicators of Compromise (IOCs).

This analyzer allows you to submit a variety of observables to MCAP to analyze files or check feeds for known indicators of compromise for other data types.

To read more, visit <https://www.cisecurity.org/ms-isac>

7.2.13 Censys



Censys

Censys

Details

Author	Nils Kuhnert, CERT-Bund
Version	1.0
License	AGPL-V3
Website	https://github.com/BSI-CERT-Bund/censys-analyzer
Requires Registration	Yes
Requires Subscription	Yes
Free Subscription Available	Yes
DataType Supported	ip, hash, domain, other
Service Homepage	Censys

Description

Check IPs, certificate hashes or domains against censys.io.

Configuration

Name	Description
uid	UID for Censys
key	API key

Additional details from the README file:

Censys

[Censys](#) is a platform that helps information security practitioners discover, monitor, and analyze devices that are accessible from the Internet. Regularly probes every public IP address and popular domain names, curate and enrich the resulting data, and make it intelligible through an interactive search engine and API.

Requirements

You need a valid Censys API integration subscription to use the analyzer.

- Provide your API uid as values for the `uid` parameter.
- Provide your API key as values for the `key` parameter.

7.2.14 CheckPhish

CheckPhish

Details

Author	Peter Juhas
Version	1.0
License	AGPL-V3
Website	https://github.com/pjuhas/Cortex-Analyzers
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	string
Service Homepage	CheckPhish

Description

Check url address via CheckPhish using jobID returned from CheckPhish_Submit

Configuration

Name	Description
key	Api key for CheckPhish

CheckPhish_Submit

Details

Author	Peter Juhas
Version	1.0
License	AGPL-V3
Website	https://github.com/pjuhas/Cortex-Analyzers
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	url
Service Homepage	CheckPhish_Submit

Description

Submit url address to CheckPhish

Configuration

Name	Description
key	Api key for CheckPhish

7.2.15 ClamAV

ClamAV_FileInfo

Details

Author	Brian Laskowski
Version	1.1
License	AGPL-V3
Website	https://github.com/Hestat/Cortex-Analyzers
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	file

Description

Use Clamscan with custom rules

Configuration

Name	Description
------	-------------

7.2.16 Crowdsec



Crowdsec_Analyzer

Details

Author	CERT-ARKEA
Version	1.0
License	AGPL-V3
Requires Registration	Yes
Requires Subscription	Yes
Free Subscription Available	Yes
DataType Supported	ip
Service Homepage	Crowdsec_Analyzer

Description

Query Crowdsec API

Configuration

Name	Description
api_key	Crowdsec API key

Additional details from the README file:

CrowdSec

Check [CrowdSec](#) Threat Intelligence about an ip address.

Running the analyzer will expose the result as taxonomies in the short report displayed in the ip observable.



The raw report contains the whole json response from CrowdSec.

e.g.:

```
{
  "ip_range_score": 0,
  "ip": "223.171.256.256",
  "ip_range": "223.171.0.0/16",
  "as_name": "LGTELECOM",
  "as_num": 17853,
  "location": {
    "country": "KR",
    "city": null,

```

(continues on next page)

(continued from previous page)

```

    "latitude": 42,
    "longitude": 42
  },
  "reverse_dns": null,
  "behaviors": [
    {
      "name": "pop3/imap:bruteforce",
      "label": "POP3/IMAP Bruteforce",
      "description": "IP has been reported for performing a POP3/IMAP brute force attack.
→"
    }
  ],
  "history": {
    "first_seen": "2022-09-26T03:45:00+00:00",
    "last_seen": "2022-10-11T08:15:00+00:00",
    "full_age": 16,
    "days_age": 15
  },
  "classifications": {
    "false_positives": [],
    "classifications": []
  },
  "attack_details": [
    {
      "name": "crowdsecurity/postfix-spam",
      "label": "Postfix Bruteforce",
      "description": "Detect spammers/postfix brute force",
      "references": []
    }
  ],
  "target_countries": {
    "DE": 25,
    "FR": 25,
    "PL": 25,
    "SK": 25
  },
  "scores": {
    "overall": {
      "aggressiveness": 0,
      "threat": 4,
      "trust": 0,
      "anomaly": 1,
      "total": 1
    },
    "last_day": {
      "aggressiveness": 0,
      "threat": 0,
      "trust": 0,
      "anomaly": 1,
      "total": 0
    },
    "last_week": {

```

(continues on next page)

(continued from previous page)

```
    "aggressiveness": 0,
    "threat": 4,
    "trust": 0,
    "anomaly": 1,
    "total": 1
  },
  "last_month": {
    "aggressiveness": 0,
    "threat": 4,
    "trust": 0,
    "anomaly": 1,
    "total": 1
  }
},
"references": []
}
```

Requirements

Provide a CrowdSec CTI Api key as a value for the api_key parameter.

7.2.17 Crtsh



Crt_sh_Transparency_Logs

Details

Author	crackytsi
Version	1.0
License	AGPL-V3
Website	https://crt.sh
Requires Registration	Yes
Requires Subscription	Yes
Free Subscription Available	Yes
DataType Supported	domain
Service Homepage	Crt_sh_Transparency_Logs

Description

Query domains against the certificate transparency lists available at crt.sh.

Configuration

Name	Description
------	-------------

Additional details from the README file:

Crtsh

Crtsh is a platform that permits you search for certificates that have been logged by CT.

Requirements

It does not require any requirements.

7.2.18 CuckooSandbox



CuckooSandbox_File_Analysis_Inet

Details

Author	Andrea Garavaglia, LDO-CERT
Version	1.2
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	file
Service Homepage	CuckooSandbox_File_Analysis_Inet

Description

Cuckoo Sandbox file analysis with Internet access.

Configuration

Name	Description
url	URL
token	API token
verifyssl	Verify SSL certificate
cert_path	Path to the CA on the system used to check server certificate

CuckooSandbox_Url_Analysis

Details

Author	Andrea Garavaglia, LDO-CERT
Version	1.2
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
Data Type Supported	url
Service Homepage	CuckooSandbox_Url_Analysis

Description

Cuckoo Sandbox URL analysis.

Configuration

Name	Description
url	URL
token	API token
verifyssl	Verify SSL certificate
cert_path	Path to the CA on the system used to check server certificate

Additional details from the README file:

CuckooSandbox

CuckooSandbox is an advanced, extremely modular, and 100% open source automated malware analysis system with infinite application opportunities.

- Analyze many different malicious files (executables, office documents, pdf files, emails, etc) as well as malicious websites under Windows, Linux, macOS, and Android virtualized environments.
- Trace API calls and general behavior of the file and distill this into high level information and signatures comprehensible by anyone.
- Dump and analyze network traffic, even when encrypted with SSL/TLS. With native network routing support to drop all traffic or route it through InetSIM, a network interface, or a VPN.
- Perform advanced memory analysis of the infected virtualized system through Volatility as well as on a process memory granularity using YARA.

The analyzer comes in two different flavour to analyze url or file with internet access.

Requirements

You need to have your cuckoosandbox deployed in your infrastructure. You can download it and follow installation instructions.

The address of the machine must be set as `url` parameter and relative token as the value for the `token` parameter. Depending on your network configuration you can configure `verifyssl` and `cert_path` accordingly.

7.2.19 CyberChef



CyberChef_FromBase64

Details

Author	Wes Lambert
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	other
Service Homepage	CyberChef_FromBase64

Description

Convert Base64 with CyberChef Server

Configuration

Name	Description
url	CyberChef Server URL

CyberChef_FromCharCode

Details

Author	Wes Lambert
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	other
Service Homepage	CyberChef_FromCharCode

Description

Convert Char Code with CyberChef Server

Configuration

Name	Description
url	CyberChef Server URL

CyberChef_FromHex

Details

Author	Wes Lambert
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	other
Service Homepage	CyberChef_FromHex

Description

Convert Hex with CyberChef Server

Configuration

Name	Description
url	CyberChef Server URL

Additional details from the README file:

Cyberchef

[Cyberchef](#) is a simple, intuitive web app for carrying out all manner of “cyber” operations within a web browser. These operations include simple encoding like XOR or Base64, more complex encryption like AES, DES and Blowfish, creating binary and hexdumps, compression and decompression of data, calculating hashes and checksums, IPv6 and X.509 parsing, changing character encodings, and much more.

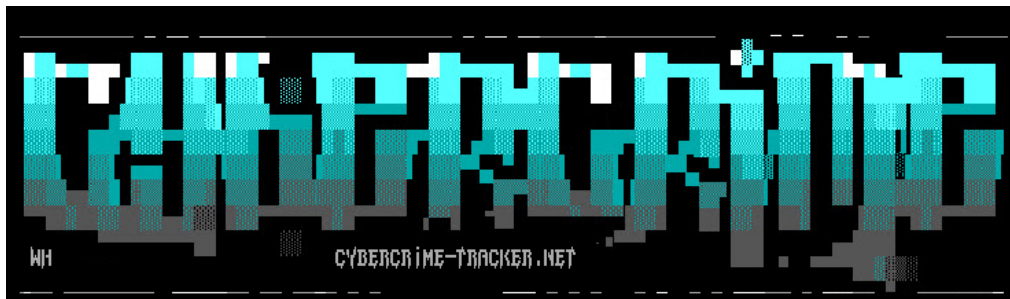
The analyzer comes in three flavours to help you convert from base64, hex or CharCode.

Requirements

You need to deploy [Cyberchef-server](#) on your infrastructure.

The url of the server must be used to configure the `url` parameter.

7.2.20 CyberCrime-Tracker



CyberCrime-Tracker

Details

Author	ph34tur3
Version	1.0
License	AGPL-V3
Website	https://github.com/ph34tur3/Cortex-Analyzers
Requires Registration	Yes
Requires Subscription	Yes
Free Subscription Available	Yes
DataType Supported	domain, fqdn, ip, url, other
Service Homepage	CyberCrime-Tracker

Description

Search cybercrime-tracker.net for C2 servers.

Configuration

Name	Description
------	-------------

Additional details from the README file:

cybercrime-tracker

[cybercrime-tracker](#) site is dedicated to tracking the C&C servers of botnets. This site is used as a source for many IP and domain blacklists.

Requirements

No configuration is required.

7.2.21 Cyberprotect

THREATSCORE 

Cyberprotect_ThreatScore

Details

Author	Rémi Allain, Cyberprotect
Version	3.0
License	AGPL-V3
Website	https://github.com/Cyberprotect/Cortex-Analyzers
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	domain, hash, ip, url, user-agent
Service Homepage	Cyberprotect_ThreatScore

Description

ThreatScore is a cyber threat scoring system provided by Cyberprotect

Configuration

Name	Description
------	-------------

Additional details from the README file:

cyberprotect

[cyberprotect](#) collect more than 500 millions of network events per day and value those data by analyzed them with analysis engines (behavioral analysis, sandboxes, threat feeds, etc.).

Requirements

No configuration is required.

7.2.22 Cylance



Cylance

Details

Author	Mikael Keri
Version	1.0
License	AGPL-V3
Requires Registration	Yes
Requires Subscription	Yes
Free Subscription Available	No
DataType Supported	hash
Service Homepage	Cylance

Description

Search for a specific hash, if there is a match, corresponding client information

Configuration

Name	Description
ten_id	Tenant ID
app_id	App ID
app_secret	App Secret
region	Portal region, : NA, US, APN, JP, APS, AU, EU, GOV, SA, SP

Additional details from the README file:

7.2.23 Cylance hashlookup

Cylance hash lookup enables you to query possible infected clients of yours using a SHA256 hash. The response includes information about the matching sample(s) along with information about affected clients.

7.2.24 FAQ

Sadly, although the response data contains an MD5 hash, the API only allows you to query with a SHA256

7.2.25 DNSDB

DNSDB_DomainName

Details

Author	CERT-BDF
Version	2.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	domain, fqdn

Description

Use DNSDB to fetch historical records for a domain.

Configuration

Name	Description
server	DNSDB server name
key	Key

DNSDB_IPHistory

Details

Author	CERT-BDF
Version	2.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	ip

Description

Use DNSDB to fetch historical records for an IP address.

Configuration

Name	Description
server	DNSDB server name
key	Key

DNSDB_NameHistory

Details

Author	CERT-BDF
Version	2.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	domain, fqdn

Description

Use DNSDB to fetch historical records for a fully-qualified domain name.

Configuration

Name	Description
server	DNSDB server name
key	Key

7.2.26 DNSLookingglass



DNS_Lookingglass

Details

Author	Dennis Perto, Conscia
Version	1.0
License	AGPL-V3
Website	https://github.com/xme/thehive/Cortex-Analyzers
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	domain, fqdn
Service Homepage	DNS_Lookingglass

Description

Query the SANS ISC Global DNS Lookingglass API to check a domain name for resolved IP addresses.

Configuration

Name	Description
------	-------------

Additional details from the README file:

DNS Lookingglass Analyzer

Lookup domain names from different locations using the ISC SANS [DNS Lookingglass](#) API service.

Requirements

There is no requirements to use this analyzer.

7.2.27 DNSSinkhole

DNSSinkhole

Details

Author	Andrea Garavaglia, LDO-CERT
Version	1.0
License	AGPL-V3
Website	https://github.com/LDO-CERT/cortex-analyzer
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	domain

Description

Check if a domain is sinkholed via DNS Sinkhole server

Configuration

Name	Description
ip	Define the DNS Sinkhole Server IP
sink_ip	Define the sinkholed response address IP

7.2.28 DShield



DShield_lookup

Details

Author	Xavier Xavier, SANS ISC
Version	1.0
License	AGPL-V3
Website	https://github.com/xme/thehive/Cortex-Analyzers
Requires Registration	No
Requires Subscription	No
Free Subscription Available	Yes
DataType Supported	ip
Service Homepage	DShield_lookup

Description

Query the SANS ISC DShield API to check for an IP address reputation.

Configuration

Name	Description
------	-------------

Additional details from the README file:

DSHield

[DSHield](#) is a community-based collaborative firewall log correlation system. It receives logs from volunteers worldwide and uses them to analyze attack trends.

The analyzer comes in just one analyzer that returns info of submitted ip.

Requirements

No configuration is required.

7.2.29 Diario



Diario_GetReport

Details

Author	Ignacio Rodriguez Paez
Version	1.0
License	AGPL-V3
Requires Registration	Yes
Requires Subscription	Yes
Free Subscription Available	No
DataType Supported	file, hash
Service Homepage	Diario_GetReport

Description

Get the latest Diario report for a file or hash.

Configuration

Name	Description
client_id	Client id for Diario
secret	Secret for Diario
polling_interval	Define time interval between two requests attempts for the report

Diario_Scan

Details

Author	Ignacio Rodriguez Paez
Version	1.0
License	AGPL-V3
Requires Registration	Yes
Requires Subscription	Yes
Free Subscription Available	No
DataType Supported	file
Service Homepage	Diario_Scan

Description

Use Diario to scan a file, it can be DOC*, XLS*, PPTX or PDF.

Configuration

Name	Description
client_id	Client id for Diario
secret	Secret for Diario
polling_interval	Define time interval between two requests attempts for the report

7.2.30 DomainMailSPFDMARC

DomainMailSPFDMARC_Analyzer

Details

Author	torsolaso
Version	1.1
License	AGPL-V3
Website	https://thehive-project.org
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	domain, fqdn

Description

DomainMailSPFDMARC

Configuration

Name	Description
------	-------------

7.2.31 DomainTools

DomainTools_HostingHistory

Details

Author	ANSSI
Version	2.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	domain

Description

Use DomainTools to get a list of historical registrant, name servers and IP addresses for a domain name.

Configuration

Name	Description
username	DomainTools API credentials
key	DomainTools API credentials

DomainTools_Reputation

Details

Author	CERT-BDF
Version	2.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	domain, fqdn

Description

Use DomainTools to get a reputation score on a domain or fqdn

Configuration

Name	Description
username	DomainTools API credentials
key	DomainTools API credentials

DomainTools_ReverselP

Details

Author	CERT-BDF
Version	2.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	ip, domain, fqdn

Description

Use DomainTools to get a list of domain names sharing the same IP address.

Configuration

Name	Description
username	DomainTools API credentials
key	DomainTools API credentials

DomainTools_ReverseIPWhois

Details

Author	ANSSI
Version	2.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	mail, ip, domain, other

Description

Use DomainTools to get a list of IP addresses which share the same registrant information.

Configuration

Name	Description
username	DomainTools API credentials
key	DomainTools API credentials

DomainTools_ReverseNameServer

Details

Author	CERT-BDF
Version	2.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	domain

Description

Use DomainTools to get a list of domain names that share the same primary or secondary name server.

Configuration

Name	Description
username	DomainTools API credentials
key	DomainTools API credentials

DomainTools_ReverseWhois

Details

Author	CERT-BDF
Version	2.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	mail, ip, domain, other

Description

Use DomainTools to get a list of domain names which share the same registrant information.

Configuration

Name	Description
username	DomainTools API credentials
key	DomainTools API credentials

DomainTools_Risk

Details

Author	CERT-BDF
Version	2.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	domain, fqdn

Description

Use DomainTools to get a risk score and evidence details on a domain or fqdn

Configuration

Name	Description
username	DomainTools API credentials
key	DomainTools API credentials

DomainTools_WhoisHistory

Details

Author	CERT-BDF
Version	2.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	domain

Description

Use DomainTools to get a list of historical Whois records associated with a domain name.

Configuration

Name	Description
username	DomainTools API credentials
key	DomainTools API credentials

DomainTools_WhoisLookup

Details

Author	CERT-BDF
Version	2.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	domain, ip

Description

Use DomainTools to get the ownership record for a domain or an IP address with basic registration details parsed.

Configuration

Name	Description
username	DomainTools API credentials
key	DomainTools API credentials

DomainTools_WhoisLookupUnparsed

Details

Author	CERT-BDF
Version	2.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
Data Type Supported	ip, domain

Description

Use DomainTools to get the ownership record for an IP address or a domain without parsing.

Configuration

Name	Description
username	DomainTools API credentials
key	DomainTools API credentials

7.2.32 DomainToolsIris



DomainToolsIris_Investigate

Details

Author	DomainTools
Version	1.0
License	AGPL-V3
Requires Registration	Yes
Requires Subscription	Yes
Free Subscription Available	No
DataType Supported	domain
Service Homepage	DomainToolsIris_Investigate

Description

Use DomainTools Iris API to investigate a domain.

Configuration

Name	Description
username	DomainTools Iris API credentials
key	DomainTools Iris API credentials
pivot_count_threshold	Pivot count threshold.

DomainToolsIris_Pivot

Details

Author	DomainTools
Version	1.0
License	AGPL-V3
Requires Registration	Yes
Requires Subscription	Yes
Free Subscription Available	No
DataType Supported	hash, ip, mail
Service Homepage	DomainToolsIris_Pivot

Description

Use DomainTools Iris API to pivot on ssl_hash, ip, or email.

Configuration

Name	Description
username	DomainTools Iris API credentials
key	DomainTools Iris API credentials

- DomainToolsIris***Investigate**: Use DomainTools Iris API to investigate a domain.
- DomainToolsIris***Pivot**: Use DomainTools Iris API to pivot on ssl_hash, ip, or email.

Requirements

You need a [valid DomainTools API integration subscription](#) to use the analyzer:

- Provide your username as a value for the `username` parameter and API key as a value for the `key` parameter.
- Set the `pivot_count_threshold` parameter to highlight any item below that value as being of interest in the report's template.

7.2.33 EchoTrail



EchoTrail

Details

Author	Joe Lazaro
Version	1.0
License	AGPL-V3
Requires Registration	Yes
Requires Subscription	No
Free Subscription Available	Yes
DataType Supported	hash, filename
Service Homepage	EchoTrail

Description

EchoTrail Insights takes a Windows filename or hash and provides several unique pieces of analytical context including prevalence & rank scores, process ancestry, behavioral analysis, and security analysis.

Configuration

Name	Description
key	API key

7.2.34 Elasticsearch

Elasticsearch_Analysis

Details

Author	Nick Prokop
Version	1.0
License	MIT
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	url, domain, ip, hash, filename, fqdn

Description

Search for IoCs in Elasticsearch

Configuration

Name	Description
endpoints	Define the Elasticsearch endpoints
keys	Set the Elasticsearch api keys for each endpoint. Note: Use api key or basic auth, but not both.
users	Set the Elasticsearch users for each endpoint. Note: Use api key or basic auth, but not both.
passwords	Set the Elasticsearch passwords for each endpoint. Note: Use api key or basic auth, but not both.
kibana	Define the kibana address
dashboard	Set the kibana dashboard id that will be linked in the report
index	Define the Elasticsearch indices to use
field	Define the fields to query
size	Define the number of hits per index to return
verifyssl	Verify SSL certificate
cert_path	Path to the CA on the system used to check server certificate

7.2.35 EmailRep



EmailRep

Details

Author	Manabu Niseki
Version	1.0
License	MIT
Website	https://github.com/ninoseki/emailrep-analyzer
Requires Registration	No
Requires Subscription	No
Free Subscription Available	Yes
DataType Supported	mail
Service Homepage	EmailRep

Description

emailrep.io lookup.

Configuration

Name	Description
key	Define the API Key

Additional details from the README file:

Emailrep

[DShiEmailrepeld](#) is a system of crawlers, scanners and enrichment services that collects data on email addresses, domains, and internet personas.

EmailRep uses hundreds of data points from social media profiles, professional networking sites, dark web credential leaks, data breaches, phishing kits, phishing emails, spam lists, open mail relays, domain age and reputation, deliverability, and more to predict the risk of an email address.

Requirements

A key can be added to configuration but it's not necessary.

7.2.36 EmergingThreats



EmergingThreats_DomainInfo

Details

Author	Davide Arcuri and Andrea Garavaglia, LDO-CERT
Version	1.0
License	AGPL-V3
Website	https://github.com/dadokkio/Cortex-Analyzers
Requires Registration	Yes
Requires Subscription	Yes
Free Subscription Available	No
DataType Supported	domain, fqdn
Service Homepage	EmergingThreats_DomainInfo

Description

Retrieve ET reputation, related malware, and IDS requests for a given domain.

Configuration

Name	Description
key	API key

EmergingThreats_IPInfo

Details

Author	Davide Arcuri and Andrea Garavaglia, LDO-CERT
Version	1.0
License	AGPL-V3
Website	https://github.com/dadokkio/Cortex-Analyzers
Requires Registration	Yes
Requires Subscription	Yes
Free Subscription Available	No
DataType Supported	ip
Service Homepage	EmergingThreats_IPInfo

Description

Retrieve ET reputation, related malware, and IDS requests for a given IP address.

Configuration

Name	Description
key	API key

EmergingThreats_MalwareInfo

Details

Author	Davide Arcuri and Andrea Garavaglia, LDO-CERT
Version	1.0
License	AGPL-V3
Website	https://github.com/dadokkio/Cortex-Analyzers
Requires Registration	Yes
Requires Subscription	Yes
Free Subscription Available	No
DataType Supported	file, hash
Service Homepage	EmergingThreats_MalwareInfo

Description

Retrieve ET details and info related to a malware hash.

Configuration

Name	Description
key	API key

Additional details from the README file:

EmergingThreats

[EmergingThreats](#) intelligence helps prevent attacks and reduce risk by helping you understand the historical context of where these threats originated, who is behind them, when have they attacked, what methods they used, and what they're after.

The analyzer is available in 3 flavors:

- `EmergingThreats_DomainInfo`: retrieve ET reputation, related malware, and IDS requests for a given domain.
- `EmergingThreats_IPInfo`: retrieve ET reputation, related malware, and IDS requests for a given IP address.
- `EmergingThreats_MalwareInfo`: retrieve ET details and info related to a malware hash.

Requirements

You need a valid EmergingThreats API subscription to use the analyzer:

- Provide your API key as a value for the `key` parameter.

7.2.37 EmlParser



EmlParser

Details

Author	StrangeBee
Version	2.1
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	file
Service Homepage	EmlParser

Description

Parse and visualise EML email message. Submit a .eml formatted file and extract some useful information.

Configuration

Name	Description
email_visu	Enable email visualisation in report. This option requires the program <i>wkhtmltoimage</i> and installation of <i>wkhtmltopdf</i> package on the system. Docker image has this program installed. Refer to the documentation for more information.
wkhtml-toimage_path	Path of wkhtmltoimage program on the system. This program is required to generate visualisation of the message as it seen in mail client program. If using Docker image, use default configuration.

Additional details from the README file:

This Analyzer allows you to view the content of an email without opening it in a dedicated application.

This programs gathers headers, message content, files, gives access to the raw message and extracts following observables:

- email addresses from headers
- IP addresses and hostnames from headers
- URLs found in plain text and html content
- filenames and Files attached

Extracted observables are enriched with tags giving context.

Email visualisation

An option permits to get an overview of the HTML rendered email. The program creates a screenshot of html parts of the message, inline and attachment parts. By default, this option is **not** enabled. To proceed, the Analyzer requires the program *wkhtmltoimage* beeing installed on the system.

When enabled, the Analyzer tries to render the html included in the email. If it fails, a dedicated message is displayed.



Requirements

wkhtmltopdf program is required to enable visualisation. DEB and RPM packages exist. Once installed, in Cortex, configure the Analyzer accordingly :

- set the parameter `email_visualisation` to true.
- If needed, replace the default value of the `wkhtmltoimage` program path in the parameter `wkhtmltoimage_path` (the default value suits the docker image of the Analyzer).

7.2.38 EnrichmentEngine

EnrichmentEngine

Details

Author	EMCA
Version	1.0
License	EMCA SOFTWARE LICENSE
Website	https://git.emca.pl/7.X/enrichment-engine
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	ip, domain, fqdn, hash, url

Description

Use EnrichmentEngine to get scan results for IOCs from various services, e.g. VT, Shodan, Censys, etc.

Configuration

Name	Description
user	User for EnrichmentEngine
password	Password for EnrichmentEngine

7.2.39 FalconSandbox

FalconSandbox

Details

Author	Sebastian Schmerl - Computacenter
Version	1.0
License	AGPL-v3
Requires Registration	Yes
Requires Subscription	Yes
Free Subscription Available	No
DataType Supported	file
Service Homepage	FalconSandbox

Description

Submit observables to the Crowdstrike FalconX Sandbox

Configuration

Name	Description
API_Base_Url	Crowdstrike Api Base Url
Client_ID	Crowdstrike Api ClientID
Client_Secret	Crowdstrike Api Client Secret

7.2.40 FileInfo

FileInfo

Details

Author	TheHive-Project
Version	8.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	file

Description

Parse files in several formats such as OLE and OpenXML to detect VBA macros, extract their source code, generate useful information on PE, PDF files...

Configuration

Name	Description
manalyze_enable	Wether to enable manalyze submodule or not.
manalyze_enable_docker	Use docker to run Manalyze. Can be used only if not using the docker image of FileInfo
manalyze_enable_binary	Use local binary to run Manalyze. Need to compile it before!
manalyze_binary_path	Path to the Manalyze binary that was compiled before. Keep the default value if using the docker image of FileInfo
floss_enable	Enable the use of FireEye FLARE FLOSS
floss_binary_path	Path to the FLOSS binary.
floss_minimal_string_length	Length of strings must be in order to be considered.

7.2.41 FireEyeSight



FireEyeSight

Details

Author	Davide Arcuri and Andrea Garavaglia, LDO-CERT
Version	1.0
License	AGPL-V3
Website	https://github.com/LDO-CERT/Cortex-Analyzers
Requires Registration	Yes
Requires Subscription	Yes
Free Subscription Available	No
DataType Supported	domain, ip, hash, url
Service Homepage	FireEyeSight

Description

Query domains, IPs, hashes and URLs on FireEye's iSIGHT threat intelligence service.

Configuration

Name	Description
key	API key for FireEye iSIGHT.
pwd	Password associated to the API key.

Additional details from the README file:

FireEyeiSight

FireEyeiSight adds context and priority to global threats before, during and after an attack. Data is gleaned from the adversarial underground, virtual network detection sensors and Mandiant IR investigations from the world's largest breaches.

The analyzer comes in only one flavor.

Requirements

You need a valid FireEye iSight subscription to use the analyzer.

- Provide your API key as a value for the **key** parameter.
- Provide your associated password as a value for **pwd** parameter.

7.2.42 FireHOLBlocklists



FireHOLBlocklists

Details

Author	Nils Kuhnert, CERT-Bund
Version	2.0
License	AGPL-V3
Website	https://github.com/BSI-CERT-Bund/cortex-analyzers
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	ip
Service Homepage	FireHOLBlocklists

Description

Check IP addresses against the FireHOL blocklists

Configuration

Name	Description
blocklistpath	Path to blocklists

Additional details from the README file:

FireJOLBlocklists

[FireJOLBlocklists](#) is a composition of other IP lists. The objective is to create a blacklist that can be safe enough to be used on all systems, with a firewall, to block access entirely, from and to its listed IPs.

The analyzer comes in a single flavour that will return if provided ip is in block list and link to its report.

Requirements

You need to clone original repo on the cortex machine [git clone <https://github.com/firehol/blocklist-ipsets>] and update relative path in `blocklistpath` variable.

7.2.43 ForcepointWebsensePing

ForcepointWebsensePing

Details

Author	Andrea Garavaglia, Davide Arcuri - LDO-CERT
Version	1.0
License	AGPL-V3
Requires Registration	Yes
Requires Subscription	Yes
Free Subscription Available	No
DataType Supported	url, ip, domain, fqdn
Service Homepage	ForcepointWebsensePing

Description

Use ForcepointWebsensePing to determine which category a certain URL is assigned to.

Configuration

Name	Description
hostname	Forcepoint remote Filtering Service
timeout	WebsensePing timeout-secs
path	WebsensePing path
malicious_categories	List of Forcepoint categories to be considered as malicious
suspicious_categories	List of Forcepoint categories you would consider as suspicious
safe_categories	List of Forcepoint categories you would consider as safe

Requirements

You need a [valid Forcepoint license](#) to use the analyzer:

- Install WebsensePing on instance where you will run this analyzer
- Provide hostname of remote Filtering Service as a value for the `hostname` parameter and timeout as a value for the `timeout` parameter.

7.2.44 Fortiguard



Fortiguard_URLCategory

Details

Author	Eric Capuano
Version	2.1
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	domain, url, fqdn
Service Homepage	Fortiguard_URLCategory

Description

Check the Fortiguard category of a URL, FQDN or a domain. Check the full available list at <https://fortiguard.com/webfilter/categories>

Configuration

Name	Description
malicious_categories	List of FortiGuard categories to be considered as malicious
suspicious_categories	List of FortiGuard categories to be considered as suspicious

Additional details from the README file:

Fortiguard

[Fortiguard](#) is a web filtering service commonly used in organizations.

The analyzer comes in a single flavour that will return websense categorization for provided url or domain.

Requirements

The analyzer returns just their categorization, you can customize which category must be considered suspicious or malicious adding them to `suspicious_categories` or `malicious_categories` variables.

7.2.45 GRR

GRR

Details

Author	pettai@sunet.se , SUNET
Version	0.1
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	ip, fqdn

Description

Search GRR for the host agent.

Configuration

Name	Description
url	URL of the GRR API.
username	API user to use
password	API password to the API user

7.2.46 GoogleDNS

GoogleDNS_resolve

Details

Author	CERT-LaPoste
Version	1.0.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	domain, ip, fqdn

Description

Request Google DNS over HTTPS service

Configuration

Name	Description
------	-------------

7.2.47 GoogleSafebrowsing

GoogleSafebrowsing

Details

Author	Nils Kuhnert, CERT-Bund
Version	2.0
License	AGPL-V3
Website	https://github.com/BSI-CERT-Bund/cortex-analyzers
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	url, domain

Description

Use Google Safebrowsing to check URLs and domain names.

Configuration

Name	Description
client_id	Client identifier
key	API key

7.2.48 GoogleVisionAPI

GoogleVisionAPI_WebDetection

Details

Author	CERT-LaPoste
Version	1.0.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	file, url

Description

Find look alike image via Google Cloud Vision API using the Web_Detection service

Configuration

Name	Description
api_key	API key for this service
max_result	Maximum number of url to fetch

7.2.49 GreyNoise



GreyNoise

Details

Author	Nclose
Version	3.1
License	APLv2
Requires Registration	Yes
Requires Subscription	Yes
Free Subscription Available	Yes
DataType Supported	ip
Service Homepage	GreyNoise

Description

Determine whether an IP has known scanning activity using GreyNoise.

Configuration

Name	Description
key	API key for GreyNoise
api_type	API Type to Match Key, either 'enterprise' or 'community'

Additional details from the README file:

GreyNoise

GreyNoise collect and analyze untargeted, widespread, and opportunistic scan and attack activity that reaches every server directly connected to the Internet. Mass scanners (such as Shodan and Censys), search engines, bots, worms, and crawlers generate logs and events omnidirectionally on every IP address in the IPv4 space. GreyNoise gives you the ability to filter this useless noise out.

The analyzer comes in a single flavour, but supports both the GreyNoise Paid and Community APIs, that will return GreyNoise additional information categorization for provided ip.

Requirements

You need a valid GreyNoise API integration subscription or Community account to use the analyzer.

- Provide your API key as values for the `key` parameter.
- Provide your API key type as “enterprise” (the default) or “community” for the `api_type` parameter

7.2.50 HIBP

HIBP_Query

Details

Author	Matt Erasmus, Jonas Hergenbahn
Version	2.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	mail

Description

Query haveibeenpwned.com for a compromised email address

Configuration

Name	Description
unverified	Include unverified breaches
truncate	Truncated response means only the name of data breaches
api_key	Api key for hibp
retries	Retries to request api while getting status code 429

7.2.51 Hashdd

hashdd

Hashdd_Detail

Details

Author	iosonogio, dadokkio
Version	2.0
License	AGPLv3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	Yes
DataType Supported	hash
Service Homepage	Hashdd_Detail

Description

Determine whether a hash is good or bad; if good then list what it is.

Configuration

Name	Description
api_key	API key for hashdd

Hashdd_Status

Details

Author	iosonogio, dadokkio
Version	2.0
License	AGPLv3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	hash

Description

Determine whether a hash is good or bad.

Configuration

Name	Description
api_key	API key for hashdd

Additional details from the README file:

Hashdd

Hashdd search engine for file hashes which automatically queries 3rd party services like VirusTotal and enriches the information provided based on the 3rd party data.

The analyzer includes two flavors: Status and Detail. The first one is used to query hashdd without an API key for the threat level only. The latter produces additional meta information about the sample, but requires an API key.

Requirements

A valid Hashdd API is necessary just for detail flavour, for status can still be added.

- Provide your API key as values for the key parameter.

7.2.52 Hippocampe

Hipposcore

Details

Author	CERT-BDF
Version	2.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	ip, domain, fqdn, url

Description

Get the Hippocampe Score report associated with an IP address, a domain or a URL.

Configuration

Name	Description
url	URL of the service

HippoMore

Details

Author	CERT-BDF
Version	2.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	ip, domain, fqdn, url

Description

Get the Hippocampe detailed report for an IP address, a domain or a URL.

Configuration

Name	Description
url	URL of the service

7.2.53 Hunterio



Hunterio_DomainSearch

Details

Author	Rémi Allain, Cyberprotect
Version	1.0
License	AGPL-V3
Website	https://github.com/Cyberprotect/Cortex-Analyzers
Requires Registration	Yes
Requires Subscription	Yes
Free Subscription Available	Yes
DataType Supported	domain, fqdn
Service Homepage	Hunterio_DomainSearch

Description

hunter.io is a service to find email addresses from a domain.

Configuration

Name	Description
key	api key of hunter.io

7.2.54 HybridAnalysis

HybridAnalysis_GetReport

Details

Author	Daniil Yugoslavskiy, Tieto
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	hash, file, filename

Description

Fetch Hybrid Analysis reports associated with hashes and filenames.

Configuration

Name	Description
secret	HybridAnalysis secret
key	API key

7.2.55 IBMXForce

IBMXForce_Lookup

Details

Author	Davide Arcuri and Andrea Garavaglia, LDO-CERT
Version	1.0
License	AGPL-V3
Website	https://github.com/LDO-CERT/Cortex-Analyzers
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
Data Type Supported	domain, ip, hash, url

Description

Query domains, IPs, hashes and URLs against IBM X-Force threat intelligence sharing platform.

Configuration

Name	Description
url	X-Force API URL
key	X-Force API Key
pwd	X-Force API Password
verify	Enable/Disable certificate verification

7.2.56 IP-API

IP-API

Details

Author	Peter Juhas
Version	1.0
License	AGPL-V3
Website	https://github.com/pjuhas/Cortex-Analyzers
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
Data Type Supported	ip, domain

Description

Check IP address or domain using ip-api.com

Configuration

Name	Description
------	-------------

7.2.57 IPVoid

IPVoid

Details

Author	Joel Snape @ Nettitude
Version	1.0
License	AGPL-v3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	ip

Description

Determine whether an IP is present on any of the feeds consumed by IPVoid

Configuration

Name	Description
key	API key for IPVoid

7.2.58 IPinfo

IPinfo_Details

Details

Author	Manabu Niseki
Version	1.0
License	MIT
Website	https://github.com/ninoseki/ipinfo-analyzers
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	ip

Description

IPinfo details lookup.

Configuration

Name	Description
api_key	Define the API key to use to connect the service

IPinfo_Hosted_Domains

Details

Author	Manabu Niseki
Version	1.0
License	MIT
Website	https://github.com/ninoseki/ipinfo-analyzers
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	ip

Description

IPinfo hosted domains lookup.

Configuration

Name	Description
api_key	Define the API key to use to connect the service

7.2.59 IVRE



IVRE

Details

Author	Pierre Lalet
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	autonomous-system, certificate_hash, domain, fqdn, ip, network, port, user-agent
Service Homepage	IVRE

Description

Fetch details from an IVRE instance.

Configuration

Name	Description
use_data	Use data from the data purpose (MaxMind)
use_passive	Use data from the passive purpose
use_scans	Use data from the scans (nmap) purpose
db_url	The URL of the IVRE database (e.g., mongodb://host/ivre or http://host/cgi); defaults to using IVRE's configuration
db_url_data	The URL of the IVRE database for the data purpose (e.g., maxmind:///usr/share/ivre/geoip or http://host/cgi); defaults to using IVRE's configuration
db_url_pass	The URL of the IVRE database for the passive purpose (e.g., mongodb://host/ivre or http://host/cgi); defaults to using IVRE's configuration
db_url_scan	The URL of the IVRE database for the scans (nmap) purpose (e.g., mongodb://host/ivre or http://host/cgi); defaults to using IVRE's configuration

Additional details from the README file:

IVRE

Get intelligence from an [IVRE](#) instance.

Requirements

You need an access to an IVRE instance. Unlike most analyzers, IVRE does not exist as a public service but is an open-source tool: you need to install and run your own instance. The repository is [on GitHub](#).

To learn more about IVRE (and its “purposes”), you can read the documentation, particularly about [the principles](#), and some [use cases](#).

Supply the following parameters to the analyzer in order to use it:

- `db_url` (string): the IVRE instance database URL (format: same as IVRE’s configuration; default: use IVRE’s configuration)
- `db_url_data` (string): the IVRE instance database URL for the data purpose (idem)
- `db_url_passive` (string): the IVRE instance database URL for the passive purpose (idem)
- `db_url_scans` (string): the IVRE instance database URL for the scans purpose (idem)
- `use_data` (boolean): should the analyzer use the data purpose?
- `use_passive` (boolean): should the analyzer use the passive purpose?
- `use_scans` (boolean): should the analyzer use the scans purpose?

7.2.60 Inoitsu



Inoitsu

Details

Author	Abdelkader Ben Ali
Version	1.0
License	MIT
Requires Registration	No
Requires Subscription	No
Free Subscription Available	Yes
DataType Supported	mail
Service Homepage	Inoitsu

Description

Query Inoitsu for a compromised email address.

Configuration

Name	Description
------	-------------

Additional details from the README file:

7.2.61 Inoitsu-analyzer

This analyzer helps you investigate suspicious emails received from known or unknown senders to ensure that their email addresses aren't compromised.

No API key required.

If the email is compromised then it returns:

- Total breaches
- Most recent breach
- Breached data
- Critical data
- Exposure rating: The comparative data exposure and risk rating assigned to this email address.

You need first to enable the analyzer.

Organization: **DWR**

Users

Analizers Config

Analizers

Responders Config

Responders

Available analyzers (165)

Refresh analyzers

Q Inoitsu

Analyzer	Max TLP	Max PAP	Rate Limit	Cache
Inoitsu_1_0 Version: 1.0 Author: Abdelkader Ben Ali License: MIT Type: Process Inoitsu lookup.				<div>+ Enable</div>

Navigate to Analyzers then run Inoitsu analyzer.

Test Inoitsu analyzer on a compromised email address.

Test Inoitsu analyzer on an uncompromised email address.

Job details

Inoitsu_1_0

Artifact

[MAIL] al[REDACTED].[REDACTED]@su[REDACTED].[REDACTED].tn

Date

a minute ago

TLP

TLP:AMBER

PAP

PAP:AMBER

Status

Success

Report summary

InoitsuCompromised="False"

Job report

Report

```
{
  "summary": {
    "taxonomies": [
      {
        "level": "safe",
        "namespace": "Inoitsu",
        "predicate": "Compromised",
        "value": "False"
      }
    ]
  },
  "full": {
    "Email": "al[REDACTED].[REDACTED]@su[REDACTED].[REDACTED].tn",
    "Leaked": false
  },
  "success": true,
  "artifacts": [],
  "operations": []
}
```

[Back to list](#)

In the observables section add emails to test.

Then select the emails that you want to analyze, select Inoitsu and click on Run selected analyzers.

☒ Inoitsu_1_0

Run selected analyzers

Cancel

Observable List (2 of 2)

<input checked="" type="checkbox"/>	Type	Value/Filename	Date Added	Actions
<input checked="" type="checkbox"/>	mail	al[REDACTED].[REDACTED]@su[REDACTED].[REDACTED].tn email No reports available	09/10/20 12:34	
<input checked="" type="checkbox"/>	mail	jon[REDACTED]@gmail[REDACTED].com email No reports available	09/10/20 12:33	

Observable List (2 of 2)

<input type="checkbox"/>	Type	Value/Filename	Date Added	Actions
<input type="checkbox"/>	mail	al[REDACTED].[REDACTED]@su[REDACTED].[REDACTED].tn email Inoitsu:Compromised="False"	09/10/20 12:34	
<input type="checkbox"/>	mail	jon[REDACTED]@gmail[REDACTED].com email Inoitsu:Compromised="True"	09/10/20 12:33	

To view the report of the compromised email, click on Inoitsu:Compromised="True"

Report of Inoitsu_1_0 analysis

Inoitsu lookup (j[redacted]@gmail.com)

Compromised: true

Total breaches: 95

Most recent breach: 2020-08-19

Breached data: Ages,Auth tokens,Avatars,Bios,Browser user agent details,Buying preferences,Charitable donations,Credit status information,Dates of birth,Deceased statuses,Device information,Email addresses,Employers,Ethnicities,Family structure,Financial investments,Genders,Geographic locations,Government issued IDs,Home ownership statuses,IP addresses,Income levels,Job titles,Marital statuses,Names,Nationalities,Net worths,Occupations,Partial credit card data>Password strengths,Passwords,Phone numbers,Physical addresses,Political donations,Profile photos,Purchases,Salutations,Social media profiles,Spoken languages,User website URLs,Usernames,Website activity

Critical data: Government issued IDs,Passwords,Profile photos,Usernames

Exposure rating: 6/10

To view the report of the uncompromised email, click on Inoitsu:Compromised="False"

Report of Inoitsu_1_0 analysis

Inoitsu lookup (a[redacted]@s[redacted].tn)

Compromised: false

7.2.62 IntezerCommunity



IntezerCommunity

Details

Author	Matteo Lodi
Version	1.0
License	AGPL-v3
Requires Registration	Yes
Requires Subscription	Yes
Free Subscription Available	Yes
DataType Supported	file
Service Homepage	IntezerCommunity

Description

Analyze a possible malicious file with Intezer Analyzer

Configuration

Name	Description
key	API key for Intezer

Additional details from the README file:

Intezer

Intezer is a subscription-based SaaS product that provides rapid malware detection and analysis.

The analyzer comes in a single flavour that permits user to upload files and detect code reuse in trusted and malicious software, and obtain new insights and information about malware families and threat actors.

Requirements

You need a valid Intezer Community API integration subscription to use the analyzer.

- Provide your API key as values for the key parameter.

7.2.63 Investigate

Investigate_Categorization

Details

Author	Cisco Umbrella Research @opendns
Version	1.0
License	AGPL-V3
Website	https://github.com/TheHive-Project/Cortex-Analyzers/Investigate
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	domain, fqdn

Description

Retrieve Investigate categorization and security features for a domain.

Configuration

Name	Description
key	Define the Investigate API Key

Investigate_Sample

Details

Author	Cisco Umbrella Research @opendns
Version	1.0
License	AGPL-V3
Website	https://github.com/TheHive-Project/Cortex-Analyzers/Investigate
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	hash

Description

Retrieve sample data from Investigate for a hash. (Sample data provided by ThreatGrid)

Configuration

Name	Description
key	Define the Investigate API Key

7.2.64 JoeSandbox

JoeSandbox_File_Analysis_Inet

Details

Author	CERT-BDF
Version	3.0
License	AGPL-V3
Requires Registration	Yes
Requires Subscription	Yes
Free Subscription Available	No
DataType Supported	file

Description

Joe Sandbox file analysis with Internet access.

Configuration

Name	Description
url	URL of JoeSandbox service
key	API key
analysistimeout	Analysis timeout (seconds)
networktimeout	Network timeout (second)
HTML_report	Download HTML report
images	Allow images in the report
observables	Creat observables form report

JoeSandbox_File_Analysis_Noinet

Details

Author	CERT-BDF
Version	3.0
License	AGPL-V3
Requires Registration	Yes
Requires Subscription	Yes
Free Subscription Available	No
DataType Supported	file

Description

Joe Sandbox file analysis without Internet access.

Configuration

Name	Description
url	URL of JoeSandbox service
key	API key
analysistimeout	Analysis timeout (seconds)
networktimeout	Network timeout (second)
HTML_report	Download HTML report
images	Allow images in the report
observables	Creat observables form report

JoeSandbox_Url_Analysis

Details

Author	CERT-BDF
Version	2.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	url

Description

Joe Sandbox URL analysis.

Configuration

Name	Description
url	URL of JoeSandbox service
key	API key
analysistimeout	Analysis timeout (seconds)
networktimeout	Network timeout (second)

Additional details from the README file:

Joe SandBox

With the version 3.0 this analyzer allow you to have:

- the HTML report as an observable
- the screenshot from Joe Sandbox in the analysis report
- IP and URL as observable

This analyzer has 3 flavors:

- URL analysis
- File analysis inet
- File analysis noinet

7.2.65 KasperskyTIP

KasperskyThreatIntelligencePortal

Details

Author	Peter Juhas
Version	1.0
License	AGPL-V3
Website	https://github.com/pjuhas/Cortex-Analyzers
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	ip, domain, hash

Description

Analyze IP address, domain or hash via Kaspersky Threat Intelligence Portal

Configuration

Name	Description
key	API key for Kaspersky Threat Intelligence Portal

7.2.66 LastInfoSec



LastInfoSec

Details

Author	LastInfoSec
Version	1.0
License	AGPL-3.0
Requires Registration	Yes
Requires Subscription	Yes
Free Subscription Available	No
DataType Supported	hash, domain
Service Homepage	LastInfoSec

Description

Get LastInfoSec Report

Configuration

Name	Description
apiKey	LastInfoSec Api Key

7.2.67 LdapQuery

Ldap_Query

Details

Author	Florian Perret @cyber_pescadito
Version	2.0
License	AGPL-V3
Website	https://github.com/cyberpescadito/Cortex-Analyzers/tree/master/analyzers/LdapQuery
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
Data Type Supported	username, mail

Description

Query your LDAP server to harvest informations about an user of your organization

Configuration

Name	Description
LDAP_address	Should contain the protocol. Eg: ldaps://myldap.myorg.com
LDAP_port	Should contain the ldap port. Eg: 389 or 636
LDAP_username	Username of the account that will be used to bind to LDAP server. The Account should have permissions to read ldap objects and attributes.
LDAP_password	Password of the account used to bind to LDAP server.
base_DN	The base DN to use in your LDAP. Eg: dc=myorg,dc=com
uid_search_field	Specify here the field to use when searching by username. Eg: uid or sAMAccountName
attributes	Specify here the attributes you want to harvest. Eg: mail

7.2.68 MISP



MISP

Details

Author	Nils Kuhnert, CERT-Bund
Version	2.1
License	AGPL-V3
Website	https://github.com/BSI-CERT-Bund/cortex-analyzers
Requires Registration	No
Requires Subscription	No
Free Subscription Available	Yes
DataType Supported	domain, ip, url, fqdn, uri_path, user-agent, hash, mail, mail_subject, registry, regexp, other, filename
Service Homepage	MISP

Description

Query multiple MISP instances for events containing an observable.

Configuration

Name	Description
name	Name of MISP servers
url	URL of MISP servers
key	API key for each server
cert_check	Verify server certificate
cert_path	Path to the CA on the system used to check server certificate

Additional details from the README file:

MISP

MISP A threat intelligence platform for gathering, sharing, storing and correlating Indicators of Compromise of targeted attacks, threat intelligence, financial fraud information, vulnerability information or even counter-terrorism information.

The analyzer comes in a single flavour that will return MISP additional information for provided observable.

Requirements

You need a valid MISP API integration to use the analyzer.

- Provide your API key as values for the key parameter.

7.2.69 MISPPWarningLists



MISPPWarningLists

Details

Author	Nils Kuhnert, CERT-Bund
Version	2.0
License	AGPL-V3
Website	https://github.com/BSI-CERT-Bund/misp-warninglists-analyzer
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	ip, hash, domain, fqdn, url
Service Homepage	MISPPWarningLists

Description

Check IoCs/Observables against MISP Warninglists to filter false positives.

Configuration

Name	Description
path	path to Warninglists folder
conn	sqlalchemy connection string

Additional details from the README file:

MISPWarningLists

`MISPWarningLists` are lists of well-known indicators that can be associated to potential false positives, errors or mistakes.

The analyzer comes in a single flavour that will check observables against MISP Warninglists to filter false positives.

Requirements

Option 1 low performances:

- Clone the `MISPWarningLists` GitHub repository.
- In the analyzer parameters configure the path of WarningLists folder.

Option 2 high performances:

- Clone the `MISPWarningLists` GitHub repository.
- Install `PostgreSQL` database.
- Set `conn_string` and `warninglists_path` located inside script `warninglists_create_db.py` and run it in order to parse all `MISPWarningLists` and insert into `PostgreSQL`.
- In the analyzer parameters configure the `conn` to DB (for example: `postgresql+psycopg2://user:password@localhost:5432/warninglists'`).

7.2.70 Malpedia

Malpedia

Details

Author	Davide Arcuri and Andrea Garavaglia, LDO-CERT
Version	1.0
License	AGPL-V3
Website	https://github.com/LDO-CERT/cortex-analyzers
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
Data Type Supported	file

Description

Check files against Malpedia YARA rules.

Configuration

Name	Description
path	Rulepath
username	Username
password	Password

7.2.71 Maltiverse



Maltiverse_Report

Details

Author	ottimo
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	hash, domain, ip, url
Service Homepage	Maltiverse_Report

Description

Get the latest Maltiverse report for an hash, domain or an IP address.

Configuration

Name	Description
polling_interval	Define time interval between two requests attempts for the report
api_key	Auth token to use when requesting data to Maltiverse

Additional details from the README file:

Maltiverse

This analyzer lets you query the free [Maltiverse](#) Threat Intelligence platform for enrichment information about a particular hash, domain, ip or url.

The analyzer comes in a single flavour that will return Maltiverse additional information categorization for provided ip.

Requirements

You can specify time interval between two requests attempts for the report with the `polling_interval` parameter.

7.2.72 MalwareBazaar



MalwareBazaar

Details

Author	Andrea Garavaglia, Davide Arcuri - LDO-CERT
Version	1.0
License	AGPL-V3
Requires Registration	Yes
Requires Subscription	Yes
Free Subscription Available	Yes
DataType Supported	hash
Service Homepage	MalwareBazaar

Description

Search hashes on MalwareBazaar.

Configuration

Name	Description
api_key	MalwareBazaar api key

Additional details from the README file:

MalwareBazaar

[MalwareBazaar](#) is a project operated by abuse.ch. The purpose of the project is to collect and share malware samples, helping IT-security researchers and threat analysts protecting their constituency and customers from cyber threats.

The analyzer comes in a single flavour that takes as input an hash and enrich it with additional intelligence .

Requirements

You need a valid MalwareBazaar API subscription to use the analyzer.

- Provide your API key as values for the key parameter.

7.2.73 MalwareClustering

MalwareClustering_Search

Details

Author	LDO-CERT
Version	1.0
License	AGPL-V3
Website	https://github.com/LDO-CERT/Cortex-Analyzers
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	file, hash

Description

Uses ApiVectors to find similarities between malware samples.

Configuration

Name	Description
n4j_host	Neo4j server host
n4j_port	Neo4j server port
n4j_user	Neo4j server user
n4j_pwd	Neo4j server password
threshold	ApiScout correlation threshold

Additional details from the README file:

7.2.74 Prerequisites:

Required:

- [neo4j db instance](https://neo4j.com/download/)
- pip3 install -r requirements

Optional:

- bulk **import known** malware samples **in** db from:
 - [cloned malpedia repo](https://malpedia.caad.fkie.fraunhofer.de/)
 - folder **with** some malicious sample **with** optional json malpedia like definition

```
from malwareclustering_api import Api
test = Api(host='127.0.0.1', port=7474, user='neo4j', password='password', threshold=40,
↪ folder_path='/home/user/malware_samples')
test.process()
```

7.2.75 Malwares



Malwares_GetReport

Details

Author	LDO-CERT
Version	1.0
License	AGPL-V3
Requires Registration	Yes
Requires Subscription	Yes
Free Subscription Available	Yes
DataType Supported	file, hash, domain, ip
Service Homepage	Malwares_GetReport

Description

Get the latest Malwares report for a file, hash, domain or an IP address.

Configuration

Name	Description
key	Malwares.com API Key

Malwares_Scan

Details

Author	LDO-CERT
Version	1.0
License	AGPL-V3
Requires Registration	Yes
Requires Subscription	Yes
Free Subscription Available	Yes
DataType Supported	file, url
Service Homepage	Malwares_Scan

Description

Use Malwares' API to scan a file or URL.

Configuration

Name	Description
key	Malwares.com API Key

Additional details from the README file:

Malwares

Malwares is a web service to collect, analyze and detect various malicious codes or malwares such as Trojans, Viruses, Worms so that customers or end-users can make proper security policies to take countermeasures against security threats.

The analyzer comes in a two flavour that permit you to query different data types (file, hash, domain, ip) or submit new sample for analysis (file, hash).

Requirements

You need a valid Malware API subscription to use the analyzer.

- Provide your API key as values for the **key** parameter.

7.2.76 MaxMind

MaxMind_GeoIP

Details

Author	CERT-BDF
Version	4.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	ip

Description

Use MaxMind to geolocate an IP address.

Configuration

Name	Description
------	-------------

7.2.77 MetaDefender

MetaDefenderCloud_GetReport

Details

Author	Davide Arcuri and Andrea Garavaglia, LDO-CERT
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	hash

Description

Get the latest MetaDefender Cloud report for hash.

Configuration

Name	Description
key	API key for MetaDefender
url	url address for MetaDefender server

MetaDefenderCloud_Reputation

Details

Author	Davide Arcuri and Andrea Garavaglia, LDO-CERT
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	ip, url, domain

Description

Get the latest MetaDefender Cloud reputation report .

Configuration

Name	Description
key	API key for MetaDefender
url	url address for MetaDefender server

MetaDefenderCloud_Scan

Details

Author	Davide Arcuri and Andrea Garavaglia, LDO-CERT
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	file

Description

Scan a file with MetaDefender Cloud

Configuration

Name	Description
key	API key for MetaDefender
url	url address for MetaDefender server
polling	Define time interval between two requests attempts for the report

MetaDefenderCore_GetReport

Details

Author	Davide Arcuri and Andrea Garavaglia, LDO-CERT
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	hash

Description

Get the latest MetaDefender Core report for hash.

Configuration

Name	Description
key	API key for MetaDefender
url	url address for MetaDefender server

MetaDefenderCore_Scan

Details

Author	Davide Arcuri and Andrea Garavaglia, LDO-CERT
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	file

Description

Scan a file with MetaDefender Core

Configuration

Name	Description
key	API key for MetaDefender
url	url address for MetaDefender server
polling	Define time interval between two requests attempts for the report

7.2.78 MnemonicPDNS

Mnemonic_pDNS_Closed

Details

Author	Michael Stensrud, Nordic Financial CERT
Version	3.0
License	AGPL-V3
Website	https://passivedns.mnemonic.no/search
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	ip, domain

Description

Query IP addresses and domains against Mnemonic pDNS restricted service.

Configuration

Name	Description
key	Define the API Key

Mnemonic_pDNS_Public

Details

Author	Michael Stensrud, Nordic Financial CERT
Version	3.0
License	AGPL-V3
Website	https://passivedns.mnemonic.no/search
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	ip, domain

Description

Query IP addresses and domains against Mnemonic pDNS public service.

Configuration

Name	Description
------	-------------

7.2.79 MsgParser

Msg_Parser

Details

Author	CERT-BDF
Version	3.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	file

Description

Parse Outlook MSG files and extract the main artifacts.

Configuration

Name	Description
------	-------------

7.2.80 NERD



NERD

Details

Author	Vaclav Bartos, CESNET
Version	1.0
License	AGPL-V3
Requires Registration	Yes
Requires Subscription	No
Free Subscription Available	Yes
DataType Supported	ip
Service Homepage	NERD

Description

Get Reputation score and other basic information from Network Entity Reputation Database (NERD)

Configuration

Name	Description
key	API key
url	Base URL of the NERD instance

Additional details from the README file:

Nerd

Project [Nerd](#) aims to build an extensive reputation database of known sources of cyber threats. That is, a list of known malicious IP addresses or other network entities (e.g. ASNs or domain names) together with all security-relevant information about each of them.

The analyzer comes in a single flavour that will return additional information categorization for provided ip.

Requirements

You need a valid Nerd API integration subscription to use the analyzer.

- Provide your API key as values for the `key` parameter.
- Default url of NERD instance is provided for `url` parameter but you could override it.

7.2.81 NSRL

NSRL

Details

Author	Andrea Garavaglia, Davide Arcuri - LDO-CERT
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	hash, filename

Description

Query NSRL

Configuration

Name	Description
conn	sqlalchemy connection string
grep_path	path of grep
nsrl_folder	path of NSRL folder

7.2.82 Nessus

Nessus

Details

Author	Guillaume Rousse
Version	2.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	ip, fqdn

Description

Use Nessus Professional to scan hosts.

Configuration

Name	Description
url	Define the URL to the Nessus service
login	Define the login to Nessus
password	Define the password to the Nessus account
policy	Define the policy used to run scans
ca_bundle	Define the path to the Nessus CA
allowed_network	Define networks allowed to be scanned

7.2.83 OTXQuery

OTXQuery

Details

Author	Eric Capuano
Version	2.0
License	AGPL-V3
Requires Registration	Yes
Requires Subscription	Yes
Free Subscription Available	Yes
DataType Supported	url, domain, file, hash, ip
Service Homepage	OTXQuery

Description

Query AlienVault OTX for IPs, domains, URLs, or file hashes.

Configuration

Name	Description
key	Define the API key to use to connect the service

Additional details from the README file:

OXT Alienvault

[OXT Alienvault](#) is the world's first and largest truly open threat intelligence community. OTX provides access to a global community of threat researchers and security professionals, with more than 100,000 participants in 140 countries, who contribute over 19 million threat indicators daily. OTX allows anyone in the security community to actively discuss, research, validate, and share the latest threat data, trends, and techniques, thereby helping one another strengthen cyber defenses and raise awareness of emerging threats on a global level.

Requirements

You need a valid OXT Alienvault API subscription to use the analyzer.

- Provide your API key as values for the `key` parameter.

7.2.84 Onyphe



Onyphe_Summary

Details

Author	Pierre Baudry, Adrien Barchapt, Andrea Garavaglia, Davide Arcuri
Version	1.0
License	AGPL-V3
Requires Registration	Yes
Requires Subscription	Yes
Free Subscription Available	Yes
DataType Supported	ip, domain, fqdn
Service Homepage	Onyphe_Summary

Description

Retrieve summary information Onyphe has for given ip, domain or fqdn.

Configuration

Name	Description
key	Define the API key to use to connect the service
verbose_taxonomies	Set true if you want detailed taxonomies for port, subnet, geoloc, domain

7.2.85 OpenCTI



O P E N C T I

OpenCTI_SearchExactObservable

Details

Author	ANSSI
Version	2.0
License	AGPL-V3
Website	https://github.com/TheHive-Project/Cortex-Analyzers/
Requires Registration	Yes
Requires Subscription	No
Free Subscription Available	No
DataType Supported	domain, ip, url, fqdn, uri_path, user-agent, hash, mail, mail_subject, registry, regexp, other, filename
Service Homepage	OpenCTI_SearchExactObservable

Description

Query multiple OpenCTI instances for a specific observable.

Configuration

Name	Description
name	Name of OpenCTI servers
url	URL of OpenCTI servers
key	API key for each server
cert_check	Verify server certificate

OpenCTI_SearchObservables

Details

Author	ANSSI
Version	2.0
License	AGPL-V3
Website	https://github.com/TheHive-Project/Cortex-Analyzers/
Requires Registration	Yes
Requires Subscription	No
Free Subscription Available	No
DataType Supported	domain, ip, url, fqdn, uri_path, user-agent, hash, mail, mail_subject, registry, regexp, other, filename
Service Homepage	OpenCTI_SearchObservables

Description

Query multiple OpenCTI instances for a list of observables matching a pattern.

Configuration

Name	Description
name	Name of OpenCTI servers
url	URL of OpenCTI servers
key	API key for each server
cert_check	Verify server certificate

Additional details from the README file:

OpenCTI is an open cyber threat intelligence platform which aims at providing a powerful knowledge management database with an enforced schema especially tailored for cyber threat intelligence and cyber operations and based on STIX 2.

The analyzer comes in only one flavor to look for an observable in the platform. The analyzer comes in two flavors to search for an observable in the platform:

- OpenCTI***SearchExactObservable**: returns an exact match only
- OpenCTI***SearchObservables**: returns all observables containing the input data

Requirements

The OpenCTI analyzer requires you to have access to one or several OpenCTI instances. You can also deploy your own instance. instances in version 4. You can also deploy your own instance.

Three parameters are required for each instance to make the analyzer work:

- url : URL of the instance, e.g. "<https://demo.opencti.io>"

7.2.86 PaloAltoWildFire



PaloAltoWildFire

Details

Author	Ignacio Rodriguez Paez, Joe Lazaro
Version	1.0
License	AGPL-V3
Requires Registration	Yes
Requires Subscription	Yes
Free Subscription Available	No
DataType Supported	file, url, hash
Service Homepage	PaloAltoWildFire

Description

Run Palo Alto WildFire analysis on a file, hash, or URL

Configuration

Name	Description
api_host	You can send requests to the WildFire global cloud (U.S., default option) or to the WildFire regional clouds that Palo Alto Networks owns and maintains. See the WildFire Public Cloud documentation for a list of valid servers.
key	API key for WildFire
polling_i	Define time interval between two requests attempts for the report

Additional details from the README file:

WildFire® is the industry’s largest, most integrated cloud malware protection engine that utilizes patented machine learning models for real-time detection of previously unseen, targeted malware and advanced persistent threats, keeping your organization protected.

When you submit observables to WildFire, they are analyzed in a sandboxed environment using multiple techniques:

- Dynamic analysis observes the files as they execute
- Machine learning extracts unique features from each file
- Static analysis provides instant identification of malware variants
- Uses a custom hypervisor to prevent malware evasion techniques

This analyzer supports “file”, “url”, and “hash” observables to be submitted to WildFire and produces a nicely formatted report in TheHive with all the pertinent information.

Product website: <https://www.paloaltonetworks.com/network-security/wildfire>

7.2.87 PassiveTotal

PassiveTotal_Components

Details

Author	Brandon Dixon (9bplus)
Version	2.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	domain, fqdn, ip

Description

PassiveTotal Components Lookup.

Configuration

Name	Description
username	Define the username of the account used to connect the service
key	Define the API key to use to connect the service

PassiveTotal_Enrichment

Details

Author	CERT-BDF
Version	2.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	domain, fqdn, ip

Description

PassiveTotal Enrichment Lookup.

Configuration

Name	Description
username	Define the username of the account used to connect the service
key	Define the API key to use to connect the service

PassiveTotal_Host_Pairs

Details

Author	Brandon Dixon (9bplus)
Version	2.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	domain, fqdn, ip

Description

PassiveTotal Host Pairs Lookup.

Configuration

Name	Description
username	Define the username of the account used to connect the service
key	Define the API key to use to connect the service

PassiveTotal_Malware

Details

Author	CERT-BDF
Version	2.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	domain, fqdn, ip

Description

PassiveTotal Malware Lookup.

Configuration

Name	Description
username	Define the username of the account used to connect the service
key	Define the API key to use to connect the service

PassiveTotal_Osint

Details

Author	CERT-BDF
Version	2.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	domain, fqdn, ip

Description

PassiveTotal OSINT Lookup.

Configuration

Name	Description
username	Define the username of the account used to connect the service
key	Define the API key to use to connect the service

PassiveTotal_Passive_Dns

Details

Author	CERT-BDF
Version	2.1
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	domain, fqdn, ip

Description

PassiveTotal Passive DNS Lookup.

Configuration

Name	Description
username	Define the username of the account used to connect the service
key	Define the API key to use to connect the service

PassiveTotal_Ssl_Certificate_Details

Details

Author	CERT-BDF
Version	2.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	hash, ip

Description

PassiveTotal SSL Certificate Details Lookup.

Configuration

Name	Description
username	Define the username of the account used to connect the service
key	Define the API key to use to connect the service

PassiveTotal_Ssl_Certificate_History

Details

Author	CERT-BDF
Version	2.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	hash, ip

Description

PassiveTotal SSL Certificate History Lookup.

Configuration

Name	Description
username	Define the username of the account used to connect the service
key	Define the API key to use to connect the service

PassiveTotal_Trackers

Details

Author	Brandon Dixon (9bplus)
Version	2.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	domain, fqdn, ip

Description

PassiveTotal Trackers Lookup.

Configuration

Name	Description
username	Define the username of the account used to connect the service
key	Define the API key to use to connect the service

PassiveTotal_Unique_Resolutions

Details

Author	CERT-BDF
Version	2.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	domain, fqdn, ip

Description

PassiveTotal Unique Resolutions Lookup.

Configuration

Name	Description
username	Define the username of the account used to connect the service
key	Define the API key to use to connect the service

PassiveTotal_Whois_Details

Details

Author	CERT-BDF
Version	2.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	domain, fqdn, ip

Description

PassiveTotal Whois Details Lookup.

Configuration

Name	Description
username	Define the username of the account used to connect the service
key	Define the API key to use to connect the service

7.2.88 Patrowl



Patrowl_GetReport

Details

Author	Nicolas Mattiocco
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	fqdn, domain, ip
Service Homepage	Patrowl_GetReport

Description

Get the current Patrowl report for a fdqn, a domain or an IP address.

Configuration

Name	Description
url	Define the PatrOwl url
api_key	Define the PatrOwl API Key

Additional details from the README file:

Patrowl

Get the current [Patrowl](#) report for a fdqn, a domain or an IP address.

The analyzer comes in only one flavor called **Patrowl_GetReport**.

Requirements

You need a running [Patrowl](#) instance or to have access to one to use the analyzer. Supply the following parameters to the analyzer in order to use it:

- url: The PatrowlManager service URL
- api_key: A valid API Key of a Patrowl user

7.2.89 PayloadSecurity

PayloadSecurity_File_Analysis

Details

Author	Emmanuel Torquato
Version	1.0
License	AGPL-V3
Website	https://github.com/notset/Cortex-Analyzers
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	file

Description

PayloadSecurity Sandbox File Analysis

Configuration

Name	Description
url	Define the url of the service
key	Define the API key used to connect the service
secret	Define the secret used to connect the service
environmentId	Define the environment Id used by the service
timeout	Define the timeout of requests to the service
verifyssl	Verify SSL certificate

PayloadSecurity_Url_Analysis

Details

Author	Emmanuel Torquato
Version	1.0
License	AGPL-V3
Website	https://github.com/notset/Cortex-Analyzers
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	url

Description

PayloadSecurity Sandbox Url Analysis

Configuration

Name	Description
url	Define the url of the service
key	Define the API key used to connect the service
secret	Define the secret used to connect the service
environmentId	Define the environment Id used by the service
timeout	Define the timeout of requests to the service
verifyssl	Verify SSL certificate

7.2.90 PhishTank



PhishTank_CheckURL

Details

Author	Eric Capuano
Version	2.1
License	AGPL-V3
Requires Registration	Yes
Requires Subscription	Yes
Free Subscription Available	Yes
DataType Supported	url
Service Homepage	PhishTank_CheckURL

Description

Use PhishTank to check if a URL is a verified phishing site.

Configuration

Name	Description
key	Define the API Key

Additional details from the README file:

PhishTank

[PhishTank](#) is a free community site where anyone can submit, verify, track and share phishing data.

The analyzer comes in a single flavour that returns the availability of submitted url in PhishTank database.

Requirements

You need a valid PhishTank API subscription to use the analyzer.

- Provide your API key as values for the `key` parameter.

7.2.91 PhishingInitiative



PhishingInitiative_Lookup

Details

Author	CERT-BDF
Version	2.0
License	AGPL-V3
Requires Registration	Yes
Requires Subscription	Yes
Free Subscription Available	Yes
DataType Supported	url
Service Homepage	PhishingInitiative_Lookup

Description

Use Phishing Initiative to check if a URL is a verified phishing site.

Configuration

Name	Description
key	Define the API Key

PhishingInitiative_Scan

Details

Author	Remi Pointel
Version	1.0
License	AGPL-V3
Requires Registration	Yes
Requires Subscription	Yes
Free Subscription Available	No
DataType Supported	url
Service Homepage	PhishingInitiative_Scan

Description

Use Phishing Initiative to scan a URL.

Configuration

Name	Description
key	Define the API Key

Additional details from the README file:

Phishing-Initiative

[Phishing-Initiative](#) enables any Internet user to help fight against phishing attacks. When reporting us the address of a suspected phishing website, we'll analyze it and have it blocked in the participating Web browsers.

The analyzer comes in two flavours: lookup and scan. The first search in the database and can be used with basic API access while the second one requires higher profile role.

Requirements

You need a valid Phishing-Initiative API integration subscription to use the analyzer.

- Provide your API key as values for the `key` parameter.

7.2.92 ProofPoint

ProofPoint_Lookup

Details

Author	Emmanuel Torquato
Version	1.0
License	AGPL-V3
Website	https://github.com/CERT-BDF/Cortex-Analyzers
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	url, file, hash

Description

Check URL, file, SHA256 against ProofPoint forensics

Configuration

Name	Description
url	URL of the Proofpoint API, the default should be okay.
apikey	API key to use
secret	Secret to the API key
verifyssl	Verify server's SSL certificate

7.2.93 Pulsedive

Pulsedive_GetIndicator

Details

Author	Nils Kuhnert
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	url, domain, ip, hash

Description

Search Pulsedive.com for a giver domain name, hash, ip or url

Configuration

Name	Description
key	Define the API Key

7.2.94 RecordedFuture

RecordedFuture_risk

Details

Author	KAPSCH-CDC
Version	1.0
License	AGPL-V3
Website	https://github.com/kapschcdc/Cortex-Analyzers
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	domain, ip, hash

Description

Get the latest risk data from RecordedFuture for a hash, domain or an IP address.

Configuration

Name	Description
key	API key for RecordedFuture

7.2.95 RiskIQ

RiskIQ_Articles

Details

Author	RiskIQ
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	domain, fqdn, ip

Description

RiskIQ: OSINT articles that reference an indicator.

Configuration

Name	Description
username	API username of the RiskIQ Illuminate or PassiveTotal account (usually an email address)
api_key	API key of the RiskIQ Illuminate or PassiveTotal account
days_back	Number of days back to search for date-bounded historical queries

RiskIQ_Artifacts

Details

Author	RiskIQ
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	domain, fqdn, ip

Description

RiskIQ: Illuminate / PassiveTotal project artifacts that match an indicator.

Configuration

Name	Description
username	API username of the RiskIQ Illuminate or PassiveTotal account (usually an email address)
api_key	API key of the RiskIQ Illuminate or PassiveTotal account
days_back	Number of days back to search for date-bounded historical queries

RiskIQ_Certificates

Details

Author	RiskIQ
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	domain, fqdn, ip

Description

RiskIQ: SSL/TLS certificates associated with an indicator.

Configuration

Name	Description
username	API username of the RiskIQ Illuminate or PassiveTotal account (usually an email address)
api_key	API key of the RiskIQ Illuminate or PassiveTotal account
days_back	Number of days back to search for date-bounded historical queries

RiskIQ_Components

Details

Author	RiskIQ
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	domain, fqdn, ip

Description

RiskIQ: web components observed during crawls on a hostname.

Configuration

Name	Description
username	API username of the RiskIQ Illuminate or PassiveTotal account (usually an email address)
api_key	API key of the RiskIQ Illuminate or PassiveTotal account
days_back	Number of days back to search for date-bounded historical queries

RiskIQ_Cookies

Details

Author	RiskIQ
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	domain, fqdn, ip

Description

RiskIQ: cookies observed during crawls on a hostname.

Configuration

Name	Description
username	API username of the RiskIQ Illuminate or PassiveTotal account (usually an email address)
api_key	API key of the RiskIQ Illuminate or PassiveTotal account
days_back	Number of days back to search for date-bounded historical queries

RiskIQ_HostpairChildren

Details

Author	RiskIQ
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	domain, fqdn, ip

Description

RiskIQ: hosts with a child web component relationship to an IOC.

Configuration

Name	Description
username	API username of the RiskIQ Illuminate or PassiveTotal account (usually an email address)
api_key	API key of the RiskIQ Illuminate or PassiveTotal account
days_back	Number of days back to search for date-bounded historical queries

RiskIQ_HostpairParents

Details

Author	RiskIQ
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	domain, fqdn, ip

Description

RiskIQ: hosts with a parent web component relationship to an IOC.

Configuration

Name	Description
username	API username of the RiskIQ Illuminate or PassiveTotal account (usually an email address)
api_key	API key of the RiskIQ Illuminate or PassiveTotal account
days_back	Number of days back to search for date-bounded historical queries

RiskIQ_Malware

Details

Author	RiskIQ
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	domain, fqdn, ip

Description

RiskIQ: malware hashes from various sources associated with an IOC.

Configuration

Name	Description
username	API username of the RiskIQ Illuminate or PassiveTotal account (usually an email address)
api_key	API key of the RiskIQ Illuminate or PassiveTotal account
days_back	Number of days back to search for date-bounded historical queries

RiskIQ_Projects

Details

Author	RiskIQ
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	domain, fqdn, ip

Description

RiskIQ: Illuminate / PassiveTotal projects that contain an artifact which matches an IOC.

Configuration

Name	Description
username	API username of the RiskIQ Illuminate or PassiveTotal account (usually an email address)
api_key	API key of the RiskIQ Illuminate or PassiveTotal account
days_back	Number of days back to search for date-bounded historical queries

RiskIQ_Reputation

Details

Author	RiskIQ
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	domain, fqdn, ip

Description

RiskIQ Illuminate Reputation Score for an indicator.

Configuration

Name	Description
username	API username of the RiskIQ Illuminate or PassiveTotal account (usually an email address)
api_key	API key of the RiskIQ Illuminate or PassiveTotal account
days_back	Number of days back to search for date-bounded historical queries

RiskIQ_Resolutions

Details

Author	RiskIQ
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	domain, fqdn, ip

Description

RiskIQ: PDNS resolutions for an IOC.

Configuration

Name	Description
username	API username of the RiskIQ Illuminate or PassiveTotal account (usually an email address)
api_key	API key of the RiskIQ Illuminate or PassiveTotal account
days_back	Number of days back to search for date-bounded historical queries

RiskIQ_Services

Details

Author	RiskIQ
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	ip

Description

RiskIQ: services observed on an IP address.

Configuration

Name	Description
username	API username of the RiskIQ Illuminate or PassiveTotal account (usually an email address)
api_key	API key of the RiskIQ Illuminate or PassiveTotal account
days_back	Number of days back to search for date-bounded historical queries

RiskIQ_Subdomains

Details

Author	RiskIQ
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	fqdn, domain

Description

RiskIQ: subdomains observed historically in pDNS records.

Configuration

Name	Description
username	API username of the RiskIQ Illuminate or PassiveTotal account (usually an email address)
api_key	API key of the RiskIQ Illuminate or PassiveTotal account
days_back	Number of days back to search for date-bounded historical queries

RiskIQ_Summary

Details

Author	RiskIQ
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	domain, fqdn, ip

Description

RiskIQ Illuminate and PassiveTotal datasets with records for an indicator.

Configuration

Name	Description
username	API username of the RiskIQ Illuminate or PassiveTotal account (usually an email address)
api_key	API key of the RiskIQ Illuminate or PassiveTotal account
days_back	Number of days back to search for date-bounded historical queries

RiskIQ_Trackers

Details

Author	RiskIQ
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	domain, fqdn, ip

Description

RiskIQ: trackers observed during a crawl on a host.

Configuration

Name	Description
username	API username of the RiskIQ Illuminate or PassiveTotal account (usually an email address)
api_key	API key of the RiskIQ Illuminate or PassiveTotal account
days_back	Number of days back to search for date-bounded historical queries

RiskIQ_Whois

Details

Author	RiskIQ
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	domain, fqdn, ip

Description

RiskIQ Whois lookup for an indicator.

Configuration

Name	Description
username	API username of the RiskIQ Illuminate or PassiveTotal account (usually an email address)
api_key	API key of the RiskIQ Illuminate or PassiveTotal account
days_back	Number of days back to search for date-bounded historical queries

7.2.96 Robtex

Robtex_Forward_PDNS_Query

Details

Author	Nils Kuhnert
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	domain, fqdn

Description

Check domains and FQDNs using the Robtex passive DNS API.

Configuration

Name	Description
------	-------------

Robtex_IP_Query

Details

Author	Nils Kuhnert
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	ip

Description

Check IPs using the Robtex IP API.

Configuration

Name	Description
------	-------------

Robtex_Reverse_PDNS_Query

Details

Author	Nils Kuhnert
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	ip

Description

Check IPs using the Robtex reverse passive DNS API.

Configuration

Name	Description
------	-------------

7.2.97 SEKOIAIntelligenceCenter

SEKŌIA.IO

SEKOIAIntelligenceCenter_Context

Details

Author	SEKOIA
Version	1.0
License	AGPL-V3
Requires Registration	Yes
Requires Subscription	Yes
Free Subscription Available	No
DataType Supported	domain, fqdn, url, hash, ip
Service Homepage	SEKOIAIntelligenceCenter_Context

Description

Query the Intelligence Center to retrieve the context of an observable

Configuration

Name	Description
api_key	Intelligence center API key
url	Intelligence center URL

SEKOIAIntelligenceCenter_Indicators

Details

Author	SEKOIA
Version	1.0
License	AGPL-V3
Requires Registration	Yes
Requires Subscription	Yes
Free Subscription Available	No
DataType Supported	domain, fqdn, url, hash, ip
Service Homepage	SEKOIAIntelligenceCenter_Indicators

Description

Query the Intelligence Center to retrieve indicators

Configuration

Name	Description
api_key	Intelligence center API key
url	Intelligence center URL

SEKOIAIntelligenceCenter_Observables

Details

Author	SEKOIA
Version	1.0
License	AGPL-V3
Requires Registration	Yes
Requires Subscription	Yes
Free Subscription Available	No
DataType Supported	domain, fqdn, url, hash, ip
Service Homepage	SEKOIAIntelligenceCenter_Observables

Description

Query the Intelligence Center to retrieve known observables

Configuration

Name	Description
api_key	Intelligence center API key
url	Intelligence center URL

- SEKOIAIntelligenceCenter***Indicators**: Find indicators matching the observable provided.
- SEKOIAIntelligenceCenter***Context**: Get indicators and their context for the observable provided.
- SEKOIAIntelligenceCenter***Observables**: Query the Intelligence Center to retrieve known observables.

Requirements

You need an active [SEKOIA.IO Intelligence Center](#) subscription to use the analyzer:

- Provide your API key as a value for the `api_key` parameter.

To get any help don't hesitate to contact support@sekoia.io.

7.2.98 SecurityTrails

SecurityTrails_Passive_DNS

Details

Author	Manabu Niseki, @ninoseki
Version	1.0
License	MIT
Website	https://github.com/ninoseki/cortex-securitytrails
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	ip

Description

SecurityTrails Passive DNS Lookup.

Configuration

Name	Description
api_key	Define the API key to use to connect the service

SecurityTrails_Whois

Details

Author	Manabu Niseki, @ninoseki
Version	1.0
License	MIT
Website	https://github.com/ninoseki/cortex-securitytrails
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	domain

Description

SecurityTrails Whois Lookup.

Configuration

Name	Description
api_key	Define the API key to use to connect the service

7.2.99 SentinelOne

SentinelOne_DeepVisibility_DNSQuery

Details

Author	Joe Vasquez
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	url, domain, fqdn

Description

Query Sentinel One Deep Visibility API v2.1 for hosts that have requested DNS lookups for a domain/URL/FQDN.

Configuration

Name	Description
s1_console_url	Console URL
s1_api_key	API Key, don't forget this will expire!
s1_account_id	Account ID
hours_ago	Number of hours ago for the fromDate of the query. ToDate will be now. Default is 12.

7.2.100 Shodan

Shodan_DNSResolve

Details

Author	ANSSI
Version	1.0
License	AGPL-V3
Website	https://github.com/TheHive-Project/Cortex-Analyzers/Shodan
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	domain, fqdn

Description

Retrieve domain resolutions on Shodan.

Configuration

Name	Description
key	Define the API Key

Shodan_Host

Details

Author	Sebastien Larinier @Sebdraven
Version	1.0
License	AGPL-V3
Website	https://github.com/TheHive-Project/Cortex-Analyzers/Shodan
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	ip

Description

Retrieve key Shodan information on an IP address.

Configuration

Name	Description
key	Define the API Key

Shodan_Host_History

Details

Author	ANSSI
Version	1.0
License	AGPL-V3
Website	https://github.com/TheHive-Project/Cortex-Analyzers/Shodan
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	ip

Description

Retrieve Shodan history scan results for an IP address.

Configuration

Name	Description
key	Define the API Key

Shodan_InfoDomain

Details

Author	ANSSI
Version	1.0
License	AGPL-V3
Website	https://github.com/TheHive-Project/Cortex-Analyzers/Shodan
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	domain, fqdn

Description

Retrieve key Shodan information on a domain.

Configuration

Name	Description
key	Define the API Key

Shodan_ReverseDNS

Details

Author	ANSSI
Version	1.0
License	AGPL-V3
Website	https://github.com/TheHive-Project/Cortex-Analyzers/Shodan
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	ip

Description

Retrieve ip reverse DNS resolutions on Shodan.

Configuration

Name	Description
key	Define the API Key

Shodan_Search

Details

Author	Sebastien Larinier @Sebdraven
Version	2.0
License	AGPL-V3
Website	https://github.com/TheHive-Project/Cortex-Analyzers/Shodan
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	other

Description

Search query on Shodan

Configuration

Name	Description
key	Define the API Key

7.2.101 SinkDB

SinkDB

Details

Author	Mark Kikta, RedLegg Cybersecurity Solutions
Version	1.1
License	AGPL-V3
Website	https://github.com/RedLegg/sinkdb-analyzer
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	ip, domain, fqdn, mail

Description

Check if ip is sinkholed via the new sinkdb.abuse.ch HTTPS API. Original analyzer can be found at <https://github.com/BSI-CERT-Bund/sinkdb-analyzer>

Configuration

Name	Description
key	Define the HTTPS API Key

7.2.102 SoltraEdge

SoltraEdge

Details

Author	Michael Stensrud, Nordic Financial CERT
Version	1.0
License	AGPL-V3
Website	http://soltra.com/en/
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	domain, ip, url, fqdn, uri_path, user-agent, hash, mail, mail_subject, registry, regexp, other, filename

Description

Query against Soltra Edge.

Configuration

Name	Description
token	Define the Token Key
username	Define the Username
base_url	Base API URL for Soltra Edge Server. (Example: https://test.soltra.com/api/stix)
verify_ssl	Verify server certificate

7.2.103 SophosIntelix

SophosIntelix_GetReport

Details

Author	SOL
Version	0.3
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	hash, domain, fqdn, url

Description

Fast and easy way to find out if the file is known Good, PUA (Potentially Unwanted Application), or, Malware. For more information or to sign up for SophosLabs Intelix (with a free tier) see <https://www.sophos.com/en-us/labs/intelix.aspx>

Configuration

Name	Description
clientID	Client ID for Sophos Labs Intelix
clientSecret	Client Secret for Sophos Labs Intelix
polling_interval	Define time interval between two requests attempts for the report

SophosIntelix_Submit_Dynamic

Details

Author	SOL
Version	0.1
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	file

Description

Detonate your suspicious file in SophosLabs Sandbox and find what behaviours the file has. For more information or to sign up for SophosLabs Intelix (with a free tier) see <https://www.sophos.com/en-us/labs/intelix.aspx>

Configuration

Name	Description
clientID	Client ID for Sophos Labs Intelix
clientSecret	Client Secret for Sophos Labs Intelix
polling_interval	Define time interval between two requests attempts for the report

SophosIntelix_Submit_Static

Details

Author	SOL
Version	0.1
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	file

Description

Use SophosLabs machine learning to understand the characteristics of your suspicious file allowing you to see if the file is similar to known malware. For more information or to sign up for SophosLabs Intelix (with a free tier) see <https://www.sophos.com/en-us/labs/intelix.aspx>

Configuration

Name	Description
clientID	Client ID for Sophos Labs Intelix
clientSecret	Client Secret for Sophos Labs Intelix
polling_interval	Define time interval between two requests attempts for the report

7.2.104 SpamAssassin



Apache SpamAssassin

SpamAssassin

Details

Author	Davide Arcuri - LDO-CERT
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	file
Service Homepage	SpamAssassin

Description

Get spam score from local SpamAssassin instance

Configuration

Name	Description
url	SpamAssassin url
port	SpamAssassin port
spam_score	Minimum score to consider mail as spam
timeout	Timeout for socket operations in seconds

7.2.105 SpamhausDBL

SpamhausDBL

Details

Author	Wes Lambert
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	domain, fqdn

Description

Perform domain lookup to Spamhaus DBL

Configuration

Name	Description
------	-------------

7.2.106 Splunk



Splunk_Search_Domain_FQDN

Details

Author	Unit777, LetMeR00t
Version	3.0
License	AGPL-V3
Website	https://www.splunk.com
Requires Registration	No
Requires Subscription	No
Free Subscription Available	Yes
DataType Supported	domain, fqdn

Description

Execute a savedsearch on a Splunk instance with a domain or a FQDN as argument

Configuration

Name	Description
host	Splunk API host or IP
port	Splunk API port
port_gui	Splunk GUI port
username	User account used for searches
password	User password of the previous mentioned account
application	Splunk application in which the saved searches are stored
owner	Username that corresponds to the owner of the saved searches
saved_searches	Name of the saved searches to use
earliest_time	If not empty, this will set the earliest time of the searches
latest_time	If not empty, this will set the latest time of the searches
max_count	Maximum number of results to return for a search

Splunk_Search_File_Filename

Details

Author	Unit777, LetMeR00t
Version	3.0
License	AGPL-V3
Website	https://www.splunk.com
Requires Registration	No
Requires Subscription	No
Free Subscription Available	Yes
DataType Supported	file, filename

Description

Execute a savedsearch on a Splunk instance with a file/filename as argument

Configuration

Name	Description
host	Splunk API host or IP
port	Splunk API port
port_gui	Splunk GUI port
username	User account used for searches
password	User password of the previous mentioned account
application	Splunk application in which the saved searches are stored
owner	Username that corresponds to the owner of the saved searches
saved_searches	Name of the saved searches to use
earliest_time	If not empty, this will set the earliest time of the searches
latest_time	If not empty, this will set the latest time of the searches
max_count	Maximum number of results to return for a search

Splunk_Search_Hash

Details

Author	Unit777, LetMeR00t
Version	3.0
License	AGPL-V3
Website	https://www.splunk.com
Requires Registration	No
Requires Subscription	No
Free Subscription Available	Yes
DataType Supported	hash

Description

Execute a savedsearch on a Splunk instance with a hash as argument

Configuration

Name	Description
host	Splunk API host or IP
port	Splunk API port
port_gui	Splunk GUI port
username	User account used for searches
password	User password of the previous mentioned account
application	Splunk application in which the saved searches are stored
owner	Username that corresponds to the owner of the saved searches
saved_searches	Name of the saved searches to use
earliest_time	If not empty, this will set the earliest time of the searches
latest_time	If not empty, this will set the latest time of the searches
max_count	Maximum number of results to return for a search

Splunk_Search_IP

Details

Author	Unit777, LetMeR00t
Version	3.0
License	AGPL-V3
Website	https://www.splunk.com
Requires Registration	No
Requires Subscription	No
Free Subscription Available	Yes
DataType Supported	ip

Description

Execute a savedsearch on a Splunk instance with an IP as argument

Configuration

Name	Description
host	Splunk API host or IP
port	Splunk API port
port_gui	Splunk GUI port
username	User account used for searches
password	User password of the previous mentioned account
application	Splunk application in which the saved searches are stored
owner	Username that corresponds to the owner of the saved searches
saved_searches	Name of the saved searches to use
earliest_time	If not empty, this will set the earliest time of the searches
latest_time	If not empty, this will set the latest time of the searches
max_count	Maximum number of results to return for a search

Splunk_Search_Mail_Email

Details

Author	Unit777, LetMeR00t
Version	3.0
License	AGPL-V3
Website	https://www.splunk.com
Requires Registration	No
Requires Subscription	No
Free Subscription Available	Yes
DataType Supported	mail, email

Description

Execute a savedsearch on a Splunk instance with a mail/email as argument

Configuration

Name	Description
host	Splunk API host or IP
port	Splunk API port
port_gui	Splunk GUI port
username	User account used for searches
password	User password of the previous mentioned account
application	Splunk application in which the saved searches are stored
owner	Username that corresponds to the owner of the saved searches
saved_searches	Name of the saved searches to use
earliest_time	If not empty, this will set the earliest time of the searches
latest_time	If not empty, this will set the latest time of the searches
max_count	Maximum number of results to return for a search

Splunk_Search_Mail_Subject

Details

Author	Unit777, LetMeR00t
Version	3.0
License	AGPL-V3
Website	https://www.splunk.com
Requires Registration	No
Requires Subscription	No
Free Subscription Available	Yes
DataType Supported	mail_subject

Description

Execute a savedsearch on a Splunk instance with a mail subject as argument

Configuration

Name	Description
host	Splunk API host or IP
port	Splunk API port
port_gui	Splunk GUI port
username	User account used for searches
password	User password of the previous mentionned account
application	Splunk application in which the saved searches are stored
owner	Username that corresponds to the owner of the saved searches
saved_searches	Name of the saved searches to use
earliest_time	If not empty, this will set the earliest time of the searches
latest_time	If not empty, this will set the latest time of the searches
max_count	Maximum number of results to return for a search

Splunk_Search_Other

Details

Author	Unit777, LetMeR00t
Version	3.0
License	AGPL-V3
Website	https://www.splunk.com
Requires Registration	No
Requires Subscription	No
Free Subscription Available	Yes
DataType Supported	other

Description

Execute a savedsearch on a Splunk instance with an unidentified data as argument

Configuration

Name	Description
host	Splunk API host or IP
port	Splunk API port
port_gui	Splunk GUI port
username	User account used for searches
password	User password of the previous mentioned account
application	Splunk application in which the saved searches are stored
owner	Username that corresponds to the owner of the saved searches
saved_searches	Name of the saved searches to use
earliest_time	If not empty, this will set the earliest time of the searches
latest_time	If not empty, this will set the latest time of the searches
max_count	Maximum number of results to return for a search

Splunk_Search_Registry

Details

Author	Unit777, LetMeR00t
Version	3.0
License	AGPL-V3
Website	https://www.splunk.com
Requires Registration	No
Requires Subscription	No
Free Subscription Available	Yes
DataType Supported	registry

Description

Execute a savedsearch on a Splunk instance with a registry data as argument

Configuration

Name	Description
host	Splunk API host or IP
port	Splunk API port
port_gui	Splunk GUI port
username	User account used for searches
password	User password of the previous mentioned account
application	Splunk application in which the saved searches are stored
owner	Username that corresponds to the owner of the saved searches
saved_searches	Name of the saved searches to use
earliest_time	If not empty, this will set the earliest time of the searches
latest_time	If not empty, this will set the latest time of the searches
max_count	Maximum number of results to return for a search

Splunk_Search_URL_URI_Path

Details

Author	Unit777, LetMeR00t
Version	3.0
License	AGPL-V3
Website	https://www.splunk.com
Requires Registration	No
Requires Subscription	No
Free Subscription Available	Yes
DataType Supported	url, uri_path

Description

Execute a savedsearch on a Splunk instance with an URL or a URI path as argument

Configuration

Name	Description
host	Splunk API host or IP
port	Splunk API port
port_gui	Splunk GUI port
username	User account used for searches
password	User password of the previous mentioned account
application	Splunk application in which the saved searches are stored
owner	Username that corresponds to the owner of the saved searches
saved_searches	Name of the saved searches to use
earliest_time	If not empty, this will set the earliest time of the searches
latest_time	If not empty, this will set the latest time of the searches
max_count	Maximum number of results to return for a search

Splunk_Search_User

Details

Author	LetMeR00t
Version	3.0
License	AGPL-V3
Website	https://www.splunk.com
Requires Registration	No
Requires Subscription	No
Free Subscription Available	Yes
DataType Supported	other

Description

Execute a savedsearch on a Splunk instance with a user ID as argument

Configuration

Name	Description
host	Splunk API host or IP
port	Splunk API port
port_gui	Splunk GUI port
username	User account used for searches
password	User password of the previous mentioned account
application	Splunk application in which the saved searches are stored
owner	Username that corresponds to the owner of the saved searches
saved_searches	Name of the saved searches to use
earliest_time	If not empty, this will set the earliest time of the searches
latest_time	If not empty, this will set the latest time of the searches
max_count	Maximum number of results to return for a search

Splunk_Search_User_Agent

Details

Author	Unit777, LetMeR00t
Version	3.0
License	AGPL-V3
Website	https://www.splunk.com
Requires Registration	No
Requires Subscription	No
Free Subscription Available	Yes
DataType Supported	user-agent

Description

Execute a savedsearch on a Splunk instance with a user agent as argument

Configuration

Name	Description
host	Splunk API host or IP
port	Splunk API port
port_gui	Splunk GUI port
username	User account used for searches
password	User password of the previous mentioned account
application	Splunk application in which the saved searches are stored
owner	Username that corresponds to the owner of the saved searches
saved_searches	Name of the saved searches to use
earliest_time	If not empty, this will set the earliest time of the searches
latest_time	If not empty, this will set the latest time of the searches
max_count	Maximum number of results to return for a search

Additional details from the README file:

This analyzer allows you to execute a list of searches in Splunk by passing the element you are looking for as a parameter

This analyzer comes in 10 flavors:

- **SplunkSearchDomain_FQDN**: Dispatch a list of saved searches on a given domain/fqdn
- **SplunkSearchFile_Filename**: Dispatch a list of saved searches on a given file/filename
- **SplunkSearchHash**: Dispatch a list of saved searches on a given hash
- **SplunkSearchIP**: Dispatch a list of saved searches on a given IP (IPv4 only)
- **SplunkSearchMail_Email**: Dispatch a list of saved searches on a given mail/email
- **SplunkSearchMail_Subject**: Dispatch a list of saved searches on a given mail_subject
- **SplunkSearchOther**: Dispatch a list of saved searches on a given data (any type)
- **SplunkSearchRegistry**: Dispatch a list of saved searches on a given registry
- **SplunkSearchURL_URI_Path**: Dispatch a list of saved searches on a given url/uri_path
- **SplunkSearchUser_Agent**: Dispatch a list of saved searches on a given user_agent
- **SplunkSearchUser**: Dispatch a list of saved searches on a given user id (variable name is 'other')

Requirements

You need to have access to a Splunk instance with a dedicated account. For any saved search you want to use, you have to group them in the same Application and with the same owner. When you configure an analyzer, it will ask you these information:

- **host**: This is the domain name or the IP of your Splunk instance.
- **port**: This is the port to reach to access Splunk (API) (Splunk default to 8089).
- **port_gui**: This is the port to reach to access Splunk (HTTP) (Splunk default to 8000).
- **username** (optional): If your Splunk instance has authentication, you need an account to access to it (and to the indexes you want to search). Please avoid to use admin.
- **password** (optional): If your Splunk instance has authentication, this is the password of the previous account. Please avoid to use admin and respect password complexity. No token access is supported.
- **application**: This is the application in which all the saved searches are stored on your Splunk instance.
- **owner**: This is the owner of all the saved searches, it must be the same for all of them. This can be different from the username mentioned above but you will need shared rights.
- **savedsearches**: A list of all saved searches you want to execute. You just have to put the name of the saved searches here. **Each saved search will be executed/dispatch in parallel (and so they will become jobs) but the Cortex job will finish once all Splunk jobs are done.**
- **earliest_time**: If not empty, this parameter will specify the earliest time to use for all searches. If empty, the earliest time set in the saved search will be used by Splunk
- **latest_time**: If not empty, this parameter will specify the latest time to use for all searches. If empty, the latest time set in the saved search will be used by Splunk
- **max_count**: This parameter is set to 1,000 by default. It's the number of results to recover from the job. A limit is set to avoid any trouble in TheHive/Cortex on the GUI. If value is set to 0, then all available results are returned.

How to recover arguments in Splunk ?

All arguments can be retrieve using “\$args.DATATYPE\$”. As an example is better than a long speech, here it is:

Imagine that you have a search with this query:

```
index=myindex_internet sourcetype=mysourcetype url=$args.url$*
| stats count by user, url, src_ip
```

This query will recover the data using \$args.url\$.

So, you can recover your data using :

- \$args.type\$: This parameter indicates the type of data (if you need so)
- \$args.domain\$: This parameter contains the data for an analysis over a domain
- \$args.fqdn\$: This parameter contains the data for an analysis over a fqdn
- \$args.file\$: This parameter contains the data for an analysis over a file
- \$args.filename\$: This parameter contains the data for an analysis over a filename
- \$args.hash\$: This parameter contains the data for an analysis over a hash
- \$args.ip\$: This parameter contains the data for an analysis over a ip

- `$args.mail$`: This parameter contains the data for an analysis over a mail
- `$args.email$`: This parameter contains the data for an analysis over a email
- `$args.mail_subject$`: This parameter contains the data for an analysis over a email_subject
- `$args.other$`: This parameter contains the data for an analysis over a other
- `$args.registry$`: This parameter contains the data for an analysis over a registry
- `$args.url$`: This parameter contains the data for an analysis over a url
- `$args.uri_path$`: This parameter contains the data for an analysis over a uri_path
- `$args.user-agent$`: This parameter contains the data for an analysis over a user-agent

Taxonomies

They are 5 taxonomies available on this analyzer:

- **Splunk:Results**: Indicates the total number of results found by all the saved searches
- **Splunk:Info** (optional): Indicates the total number of results which have a field “level” set to “info”
- **Splunk:Safe** (optional): Indicates the total number of results which have a field “level” set to “safe”
- **Splunk:Suspicious** (optional): Indicates the total number of results which have a field “level” set to “suspicious”
- **Splunk:Malicious** (optional): Indicates the total number of results which have a field “level” set to “malicious”

As mentionned above, your saved searches can return a field named “level” which will be interpreted by Cortex/TheHive as a taxonomy and will create reports accordingly to the value (info,safe,suspicious or malicious)

7.2.107 StamusNetworks

StamusNetworks_HostID

Details

Author	Stamus Networks
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	ip

Description

Get information from your Scirius Security Platform for an IP address.

Configuration

Name	Description
url	Base URL of Scirius Security Platform
key	API key for Scirius Security Platform
ssl_verify	Verify TLS certificate when connection to Scirius Security Platform
tenant	Tenant value for organization in Scirius Security Platform

7.2.108 StaxxSearch

StaxxSearch

Details

Author	Robert Nixon
Version	1.0
License	AGPL-V3
Website	https://github.com/robertnixon2003/Cortex-Analyzers
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	domain, fqdn, ip, url, hash, mail

Description

Fetch observable details from an Anomali STAXX instance.

Configuration

Name	Description
auth_url	Define the URL of the auth endpoint
query_url	Define the URL of the intelligence endpoint
username	STAXX User Name
password	STAXX Password
cert_check	Verify server certificate
cert_path	Path to the CA on the system used to check the server certificate

7.2.109 StopForumSpam

StopForumSpam

Details

Author	Marc-Andre Doll, STARC by EXAPROBE
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	ip, mail

Description

Query <http://www.stopforumspam.com> to check if an IP or email address is a known spammer.

Configuration

Name	Description
suspicious_confidence_level	Confidence threshold above which the artifact should be marked as suspicious
malicious_confidence_level	Confidence threshold above which the artifact should be marked as malicious

7.2.110 TalosReputation

TalosReputation

Details

Author	Gabriel Antonio da Silva
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	ip

Description

Get the Talos IP reputation

Configuration

Name	Description
------	-------------

7.2.111 TeamCymruMHR

TeamCymruMHR

Details

Author	Wes Lambert
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	hash

Description

Submit hash to Team Cymru's Malware Hash Registry

Configuration

Name	Description
------	-------------

7.2.112 ThreatGrid

ThreatGrid

Details

Author	Cisco Security
Version	1.0
License	MIT
Website	https://github.com/CiscoSecurity
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	file, url, hash

Description

Threat Grid Sandbox

Configuration

Name	Description
tg_host	Threat Grid Host
api_key	Threat Grid API Key

7.2.113 ThreatMiner

ThreatMiner

Details

Author	Peter Juhas
Version	1.0
License	AGPL-V3
Website	https://github.com/pjuhas/Cortex-Analyzers
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	ip, domain

Description

WHOIS queries from threatminer.org

Configuration

Name	Description
------	-------------

7.2.114 ThreatResponse

ThreatResponse

Details

Author	Cisco Security
Version	1.0
License	MIT
Website	https://github.com/CiscoSecurity
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	domain, filename, fqdn, hash, ip, url

Description

Threat Response

Configuration

Name	Description
region	Threat Response Region (us, eu, or apjc). Will default to 'us' region if left blank
client_id	Threat Response Client ID
client_password	Threat Response API Client Password
extract_amp_targets	Would you like to extract AMP connector GUIDs as artifacts?

7.2.115 Threatcrowd

Threatcrowd

Details

Author	Rémi Allain, Cyberprotect
Version	1.0
License	AGPL-V3
Website	https://github.com/Cyberprotect/Cortex-Analyzers
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	mail, ip, domain, fqdn

Description

Look up domains, mail and IP addresses on ThreatCrowd.

Configuration

Name	Description
------	-------------

7.2.116 Thunderstorm



THOR_Thunderstorm_ScanSample

Details

Author	Florian Roth
Version	0.3.1
License	AGPL-V3
Website	https://github.com/NextronSystems/Cortex-Analyzers
Requires Registration	Yes
Requires Subscription	Yes
Free Subscription Available	No
DataType Supported	file
Service Homepage	THOR_Thunderstorm_ScanSample

Description

Submits sample to an on-premise THOR Thunderstorm web service and processes the scan result

Configuration

Name	Description
thunderstorm_server	Thunderstorm Server
thunderstorm_port	Thunderstorm Port
thunderstorm_source	Source System
thunderstorm_ssl	Use an SSL encrypted HTTP connection
thunderstorm_ssl_verify	Verify the SSL certificate of the remote service

Additional details from the README file:

Thunderstorm

The Thunderstorm analyzer submits a file sample to a local or public THOR Thunderstorm service and processes the scan result

Requirements

- [ThunderstormAPI](#)

Scope

THOR [Thunderstorm](#) is a web service version of the well-known scanner THOR. THOR focuses on APTs, hacking activity, traces of hacking activity and file anomalies like obfuscation techniques, suspicious PE packers or PE header anomalies.

Matches

The reports contain useful meta data and a list of matching rules. Each rule links to a related public report or states that the rules was based on internal research.

The reports include a total score and sub scores defined in the matching YARA rules.

The score and level indicate the criticality of the finding.

Access to Thunderstorm

THOR Thunderstorm is a high-speed, multi-threaded, caching scan service that is licensed and installed on-premise on the Linux system of your choice. Nextron systems offers access to test systems with the FQDN [thunderstorm.nextron-systems.com](#) on request.

7.2.117 TorBlutmagie

TorBlutmagie

Details

Author	Marc-André DOLL, STARC by EXAPROBE
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	ip, domain, fqdn

Description

Query http://torstatus.blutmagie.de/query_export.php/Tor_query_EXPORT.csv for TOR exit nodes IP addresses or names.

Configuration

Name	Description
cache.duration	Define the cache duration
cache.root	Define the path to the stored data

7.2.118 TorProject

TorProject

Details

Author	Marc-André DOLL, STARC by EXAPROBE
Version	1.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	ip

Description

Query <https://check.torproject.org/exit-addresses> for TOR exit nodes IP addresses.

Configuration

Name	Description
ttl	Define the TTL
cache.duration	Define the cache duration
cache.root	Define the path to the stored data

7.2.119 Triage



Triage

Details

Author	Mikael Keri
Version	1.0
License	AGPL-V3
Requires Registration	Yes
Requires Subscription	Yes
Free Subscription Available	No
DataType Supported	ip, url, file
Service Homepage	Triage

Description

Submit artifacts to the Triage sandbox service. This analyzer requires a paid subscription

Configuration

Name	Description
api_key	API key
timeout	Sandbox run timeout in seconds (default: 200)
zip_pw	Zip archive password

Additional details from the README file:

7.2.120 Triage Sandbox analyzer

Triage Sandbox is a commercial malware sandbox that let's you run malware in a safe way.

You can read more about the underlying solutions at: <https://hatching.io/>

Thus this analyzer requires you to have a commercial license.

7.2.121 FAQ

7.2.122 URLhaus

URLhaus

Details

Author	ninoseki, Nils Kuhnert
Version	2.0
License	MIT
Website	https://github.com/ninoseki/cortex_URLhaus_analyzer
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	domain, fqdn, url, hash, ip

Description

Search domains, IPs, URLs or hashes on URLhaus.

Configuration

Name	Description
------	-------------

7.2.123 Umbrella

Umbrella_Report

Details

Author	Kyle Parrish
Version	1.0
License	AGPL-V3
Website	https://github.com/arnydo/thehive/Cortex-Analyzers
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	domain, fqdn

Description

Query the Umbrella Reporting API for recent DNS queries and their status.

Configuration

Name	Description
api_key	Api Key provided by Umbrella Admin Console.
api_secret	Api Secret provided by Umbrella Admin Console.
organization_id	Organization ID provided by Umbrella Admin Console.
query_limit	Maximum number of results to return.

7.2.124 UnshortenLink

UnshortenLink

Details

Author	Remi Pointel, CERT-BDF
Version	1.2
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	url

Description

Use UnshortenLink to reveal the real URL.

Configuration

Name	Description
------	-------------

7.2.125 Urlscan.io

Urlscan.io_Scan

Details

Author	ninoseki, Kyle Parrish (@arnydo)
Version	0.1.0
License	MIT
Website	https://github.com/arnydo/Cortex-Analyzers
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	url, domain, fqdn

Description

Scan URLs on urlscan.io

Configuration

Name	Description
key	API key for Urlscan.io

Urlscan.io_Search

Details

Author	ninoseki, Kyle Parrish (@arnydo)
Version	0.1.1
License	MIT
Website	https://github.com/arnydo/Cortex-Analyzers
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	ip, domain, hash, fqdn, url

Description

Search IPs, domains, hashes or URLs on urlscan.io

Configuration

Name	Description
------	-------------

7.2.126 VMRay

VMRay

Details

Author	Nils Kuhnert, CERT-Bund
Version	4.1
License	AGPL-V3
Website	https://github.com/BSI-CERT-Bund/cortex-analyzers
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	hash, file, url

Description

VMRay Sandbox file and URL analysis.

Configuration

Name	Description
url	Define the URL of the service
key	Define the API key
certverify	Verify certificates
certpath	Path to certificate file, in case of self-signed etc.
verdict_only	If set to true, only the verdict (or the score for VMRay versions < 4.0) will be added as labels.
query_retry	The amount of seconds to wait before trying to fetch the results.
recursive_sample	The maximum amount of recursive samples which will be analyzed. 0 disables recursion.
reanalyze	If set to true, known samples will be re-analyzed on submission. This is enabled by default.
shareable	If set to true, the hash of the sample will be shared with VirusTotal if the TLP level is white or green.
archive_password	The password that will be used to extract archives.
archive_compound	If set to true, files inside archives are treated as a single, compound sample. Otherwise, each file is treated as its own sample.
max_jobs	Limits the amount of jobs that can be created by jobrules for a submission.
enable_reputation	If set to true, reputation lookups will be performed for submitted samples and analysis artifacts (file hash and URL lookups) by the VMRay cloud reputation service and additional third party services. The user analyzer setting is used as default value for this parameter.
enable_whois	If set to true, domains seen during analyses are queried with external WHOIS service. The user analyzer setting is used as default value for this parameter.
analyzer_mode	Specifies which types of analyzers will be used for analyzing this sample. Supported strings are 'reputation', 'reputation_static', 'reputation_static_dynamic', 'static_dynamic', and 'static'. The user analyzer setting is used as default value for this parameter.
known_malicious	If set to true, triage will be used to pre-filter known malicious samples by results of reputation lookup (if allowed) and static analysis. The user analyzer setting is used as default value for this parameter.
known_benign	If set to true, triage will be used to pre-filter known benign samples by results of reputation lookup (if allowed) and static analysis. The user analyzer setting is used as default value for this parameter.
tags	Tags to attach to the sample.
timeout	Analysis timeout in seconds.
net_scheme	Name of the network schema.

7.2.127 Valhalla



Valhalla_GetRuleMatches

Details

Author	Florian Roth
Version	0.3.1
License	AGPL-V3
Website	https://github.com/NexttronSystems/Cortex-Analyzers
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	hash
Service Homepage	Valhalla_GetRuleMatches

Description

Gets matching YARA rules for a given sample SHA256 hash

Configuration

Name	Description
key	API key for Valhalla

Additional details from the README file:

Valhalla

The Valhalla analyzer queries the Valhalla YARA rule databased and retrieves the matching YARA rules.

Requirements

- [ValhallaAPI](#)

Scope

The result contains all matching YARA rules including

- Nextron's rules in the [public rule repository](#)
- Nextron's rules sold in the form of the [YARA rule feed](#)

The result does not contain matches with YARA rules

- submitted by 3rd parties into the [public rule repository](#) due to legal restrictions
- rules that are tagged as confidential and can therefore only be used in Nextron's scanner [THOR](#)
- rules that require external variables and can therefore only be used in Nextron's scanner [THOR](#)

The database contains YARA rule matches on samples submitted to Virustotal and Nextron's internal sample matching, which accounts for less than 1% of the matches within that database. The database does not contain information on samples that have not been transmitted to Virustotal.

Matches

The matches in the long report link to rule info pages that contain more information, like other matching samples, a report or public source in which the sample from which that rule was derived has been mentioned.

They also include the Antivirus detection rate at the moment of the first submission to Virustotal, which gives a good indication of the overall coverage.

7.2.128 Verifalia

Verifalia

Details

Author	Peter Juhas
Version	1.0
License	AGPL-V3
Website	https://github.com/pjuhas/Cortex-Analyzers
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	mail

Description

Analyze e-mail address via Verifalia

Configuration

Name	Description
login	Username for Verifalia
password	Password for Verifalia

7.2.129 VirusTotal



VirusTotal_DownloadSample

Details

Author	LDO-CERT
Version	3.1
License	AGPL-V3
Requires Registration	Yes
Requires Subscription	Yes
Free Subscription Available	No
DataType Supported	hash
Service Homepage	VirusTotal_DownloadSample

Description

Use VirusTotal to download the original file for an hash.

Configuration

Name	Description
key	API private key for Virustotal

VirusTotal_GetReport

Details

Author	CERT-BDF, StrangeBee
Version	3.1
License	AGPL-V3
Requires Registration	Yes
Requires Subscription	No
Free Subscription Available	No
DataType Supported	file, hash, domain, fqdn, ip, url
Service Homepage	VirusTotal_GetReport

Description

Get the latest VirusTotal report for a file, hash, domain or an IP address.

Configuration

Name	Description
key	API key for Virustotal
polling_interval	Define time interval between two requests attempts for the report
rescan_hash_older_than_days	Rescan hash observable if report is older than selected days
highlighted_antivirus	Add taxonomy if selected AV don't recognize observable
download_sample	Download automatically sample as observable when looking for hash
down-load_sample_if_highlighted	Download automatically sample as observable if highlighted antivirus didn't recognize

VirusTotal_Rescan

Details

Author	CERT-LDO
Version	3.1
License	AGPL-V3
Requires Registration	Yes
Requires Subscription	Yes
Free Subscription Available	No
DataType Supported	hash
Service Homepage	VirusTotal_Rescan

Description

Use VirusTotal to run new analysis on hash.

Configuration

Name	Description
key	API key for Virustotal
polling_interval	Define time interval between two requests attempts for the report
highlighted_antivirus	Add taxonomy if selected AV don't recognize observable
download_sample	Download automatically sample as observable when looking for hash
down-load_sample_if_highlighted	Download automatically sample as observable if highlighted antivirus didn't recognize

VirusTotal_Scan

Details

Author	CERT-BDF, StrangeBee
Version	3.1
License	AGPL-V3
Requires Registration	Yes
Requires Subscription	No
Free Subscription Available	No
DataType Supported	file, url
Service Homepage	VirusTotal_Scan

Description

Use VirusTotal to scan a file or URL.

Configuration

Name	Description
key	API key for Virustotal
polling_interval	Define time interval between two requests attempts for the report
highlighted_antivirus	Add taxonomy if selected AV don't recognize observable

Additional details from the README file:

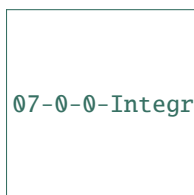
This analyzer let you run Virustotal services on several datatypes:

- *file*
- *hash*
- *domain*
- *fqdn*
- *ip*
- *url*

The program uses [VirusTotal API v3](#).

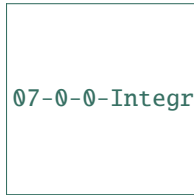
Major improvements have been added with `_VirusTotal_GetReport_` flavor. Now, with the classical scan results, the report can display:

- A Summary: with qualitative information about the detection



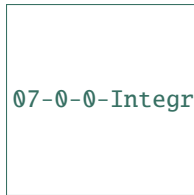
07-0-0-Integrations/Analyzers/VirusTotal/assets/virustotal-summary-report.png

- Crowdsourced YARA results with known Yara rules to detect the threat



07-0-0-Integrations/Analyzers/VirusTotal/assets/virustotal-yara.png

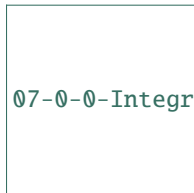
- Contacted IP addresses, domains and URLs if any
- Crowdsourced IDS results with known IDS rules to detect the threat
- Sandbox verdict if any



07-0-0-Integrations/Analyzers/VirusTotal/assets/virustotal-ids-sandbox-urls.png

Extracted Observables

Moreover, these domains, IP addresses, URLs as well as detection YARA and IDS rules reported are added to the extracted Observables, ready to be imported and actioned in TheHive.



07-0-0-Integrations/Analyzers/VirusTotal/assets/virustotal-extracted-observables.png

7.2.130 Virusshare



Virusshare

Details

Author	Nils Kuhnert, CERT-Bund
Version	2.0
License	AGPL-V3
Website	https://github.com/BSI-CERT-Bund/cortex-analyzers
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	hash, file
Service Homepage	Virusshare

Description

Search for MD5 hashes in Virusshare.com hash list

Configuration

Name	Description
path	Define the path to the stored data

Additional details from the README file:

VirusShare

[VirusShare](#) is a repository of malware samples to provide security researchers, incident responders, forensic analysts, and the morbidly curious access to samples of live malicious code.

The analyzer enables local searching for md5 hashes in Virusshare.com hash list.

Requirements

- Download the [VirusShare](#) hashlists. For convenience the `getHashes.sh` script is provided
- In the analyzer parameters configure the path of downloaded hashlists folder.

7.2.131 Vulners



Vulners_CVE

Details

Author	Dmitry Uchakin, Vulners team
Version	1.0
License	AGPL-V3
Requires Registration	Yes
Requires Subscription	Yes
Free Subscription Available	Yes
DataType Supported	cve
Service Homepage	Vulners_CVE

Description

Get information about CVE from powerful Vulners database.

Configuration

Name	Description
key	API key for Vulners

Vulners_IOC

Details

Author	Dmitry Uchakin, Vulners team
Version	1.0
License	AGPL-V3
Requires Registration	Yes
Requires Subscription	Yes
Free Subscription Available	Yes
DataType Supported	url, domain, ip
Service Homepage	Vulners_IOC

Description

Get information from the RST Threat Feed, which integrated with Vulners, for a domain, url or an IP address.

Configuration

Name	Description
key	API key for Vulners

Additional details from the README file:

Vulners-analyzer

This analyzer consists of 2 parts.

1. **Vulners_IOC**: As a result of collaboration between Vulners and RST Threat Feed, the idea was to send IOC analysis results through theHive analyzer: blog post
2. **Vulners_CVE**: Vulners have a strong vulnerability database. This data is useful if: “if the case (incident) is related to the exploitation of a vulnerability, then the analyst (manually / automatically) can add it to observables and quickly get all the basic information on it in order to continue analyzing the case.”

Vulners API key required.

Setting up analyzer

- copy the folders “Vulners” analyzer & “Vulners” into your Cortex analyzer path
- install necessary python modules from the requirements.txt (**pip install -r requirements.txt**)
- restart Cortex to initialize the new Responder “**systemctl restart cortex**”

Get your Vulners api key: .. image:: assets/vulners_api.png

target
assets/vulners_api.png
alt
Vulners API

Add your Vulners API in Cortex settings: .. image:: assets/Cortex_settings.PNG

target
assets/Cortex_settings.PNG
alt
API key in Cortex

Add Observable type in TheHive

By default theHive does not have a “cve” type to be observables, so we have to add it to Administrator Settings:



Run the Analyzer in TheHive

Network IOCs:

Short template:



Long template:



```
07-0-0-Integrations/Analyzers/Vulners/assets/ioc_long_template.png
```



```
07-0-0-Integrations/Analyzers/Vulners/assets/ioc_with_malware_family.PNG
```

Vulnerabilities:

Short template:



```
07-0-0-Integrations/Analyzers/Vulners/assets/cve_short_template.png
```

Long template:

7.2.132 WOT**WOT_Lookup****Details**

Author	Andrea Garavaglia, Davide Arcuri, LDO-CERT
Version	2.0
License	AGPL-V3
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	domain, fqdn

Description

Use Web of Trust to check a domain's reputation.

Configuration

Name	Description
user	Define the API user
key	Define the API key

7.2.133 Yara

Yara

Details

Author	Nils Kuhnert, CERT-Bund
Version	2.0
License	AGPL-V3
Website	https://github.com/BSI-CERT-Bund/cortex-analyzers
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	file

Description

Check files against YARA rules.

Configuration

Name	Description
rules	Define the path rules folder

7.2.134 Yeti

Yeti

Details

Author	CERT-BDF
Version	1.0
License	AGPL-V3
Website	https://github.com/CERT/cortex-analyzers
Requires Registration	No
Requires Subscription	No
Free Subscription Available	No
DataType Supported	domain, fqdn, ip, url, hash

Description

Fetch observable details from a YETI instance.

Configuration

Name	Description
url	Define the URL of the service
api_key	Define the api key of the service
verify_ssl	Verify SSL certificate

7.2.135 Zscaler



Zscaler

Details

Author	Simon Lavigne, Mikael Keri
Version	1.3
License	AGPL-V3
Requires Registration	Yes
Requires Subscription	Yes
Free Subscription Available	No
DataType Supported	ip, domain, url, fqdn
Service Homepage	Zscaler

Description

Check Zscaler category for a domain, fqdn, IP address or FQDN. This analyzer requires a paid subscription to Zscaler ZIA

Configuration

Name	Description
username	Zscaler username
password	Zscaler password
api_key	API key
base_uri	The base URL of your Zscaler subscription
malicious_categories	List of Zscaler categories to be considered as malicious
suspicious_categories	List of Zscaler categories to be considered as suspicious

Additional details from the README file:

Zscaler

General requirements

You will need to have an active Zscaler ZIA subscription to be able to utilize this analyzer.

Credit

Full credit should go to Simon Lavigne for creating this analyzer in the first place.

7.3 How to Write and Submit an Analyzer

7.3.1 Writing an Analyzer

An analyzer is a program that takes an observable and configuration information as **raw input**, analyze the observable and produces a result as **raw output**. It is made of at least 2 types of files:

- The program itself
- One or several service interaction files or flavors
- A Python requirements file, which is only necessary if the analyzer is written in Python.

The Program

The first type of files an analyzer is made of is the core program that performs actions. It can be written in any programming language that is supported by Linux.

While many analyzers are written in Python (*.py files), you can write yours in Ruby, Perl or even Scala. However, the very handy `Cortexutils` library *described below* is in Python. It greatly facilitates analyzer development and it also provides some methods to quickly format the output to make it compliant with the JSON schema expected by [EnergySOAR](#).

Service Interaction Files (Flavors)

An analyzer must have at least one service interaction file. Such files contain key configuration information such as the analyzer's author information, the datatypes (IP, URL, hash, domain...) the analyzer accepts as input, the TLP and PAP ([Permissible Actions Protocol](#)) above which it will refuse to execute to protect against data leakage and to enforce sane OPSEC practices and so on.

An analyzer can have two or more service interaction files to allow it to perform different actions. We speak then of flavors. For example, a sandbox analyzer can analyze a file with or without an Internet connection. Another example could be an analyzer that can either send a file to VirusTotal for analysis or get the last report using its hash.

Python Requirements

If the analyzer is written in Python, a `requirements.txt` must be provided with the list of all the dependencies.

Example: VirusTotal Analyzer Files

Below is a directory listing of the files corresponding to the VirusTotal analyzer. You can see that the analyzer has two flavors: **GetReport** and **Scan**.

```
analyzers/VirusTotal
|-- VirusTotal_GetReport.json
|-- VirusTotal_Scan.json
|-- requirements.txt
|-- virustotal.py
`-- virustotal_api.py
```

Input

The input of an analyzer is a JSON structure with different pieces of information. For example, to use the VirusTotal analyzer's **GetReport** flavor in order to obtain the latest available report for hash d41d8cd98f00b204e9800998ecf8427e, you must submit input such as:

```
{
  "data": "d41d8cd98f00b204e9800998ecf8427e",
  "dataType": "hash",
  "tlp": 0,
  "config": {
    "key": "1234567890abcdef",
    "max_tlp": 3,
    "check_tlp": true,
    "service": "GetReport"
    [..]
  },
  "proxy": {
    "http": "http://myproxy:8080",
    "https": "https://myproxy:8080"
  }
}
```

data, dataType and tlp are the observable-related information generated by TheHive or any other program that is calling Cortex. config is the analyzer's specific configuration provided by an orgAdmin users when the analyzer is enabled in the Cortex UI.

Let's take the **GetReport** flavor of the VirusTotal analyzer as an example again.

Example: VirusTotal Get Report's Input

```
{
  "data": "d41d8cd98f00b204e9800998ecf8427e",
  "dataType": "hash",
  "tlp": 0,
  [..]
}
```

Example: Service Interaction File for VirusTotal GetReport

The <== sign and anything after it are comments that do no appear in the original file.

```
{
  "name": "VirusTotal_GetReport",
  "version": "3.0",
  "author": "CERT-BDF",
  "url": "https://github.com/TheHive-Project/Cortex-Analyzers",
  "license": "AGPL-V3",
  "description": "Get the latest VirusTotal report for a file, hash, domain or an IP ↵
↵address.",
  "dataTypeList": ["file", "hash", "domain", "ip"],
```

(continues on next page)

(continued from previous page)

```

"command": "VirusTotal/virustotal.py", <== Program to run when invoking the analyzer
"baseConfig": "VirusTotal", <== name of base config in Cortex analyzer config page
"config": {
  "service": "get"
},
"configurationItems": [ <== list of configuration items the analyzer needs to operate.
↳(api key etc.)
  {
    "name": "key",
    "description": "API key for Virustotal",
    "type": "string", <== defines what kind of data type the configuration item is.
↳(string, number)
    "multi": false, <== setting multi to true allows to pass a list of items (e.g.
↳MISP analyzer)
    "required": true
  },
  {
    "name": "polling_interval",
    "description": "Define time interval between two requests attempts for the report",
    "type": "number",
    "multi": false,
    "required": false,
    "defaultValue": 60
  }
]
}

```

Service Interaction Configuration Items

name

Name of the specific service (or flavor) of the analyzer.

If your analyzer has only one service interaction (i.e. performs only one action), it is the name of the analyzer's directory.

If your analyzer performs several actions (i.e. comes in several flavors), you have to give a specific and meaningful name to each flavor.

Each flavor's name appear in TheHive's analyzer list and in MISP when you use Cortex for attribute enrichment.

version

The version of the analyzer.

You **must** increase major version numbers when new features are added, modifications are made to take into account API changes, report output is modified or when report templates (more on this later) are updated.

You must increase minor version numbers when bugs are fixed.

The version number is also used in the folder name of the associated report templates ; e.g. *VirusTotal_GetReport* and 3.0 on the JSON file should correspond a folder named *VirusTotal_GetReport_3_0* for report templates. Report templates are used by TheHive to display the analyzer's JSON output in an analyst-friendly fashion.

author

You must provide your full name and/or your organization/team name when submitting an analyzer. Pseudos are not accepted. If you'd rather remain anonymous, please contact us at support@thehive-project.org prior to submitting your analyzer.

url

The URL where the analyzer is stored. This should ideally be <https://github.com/TheHive-Project/Cortex-Analyzers>

license

The license of the code. Ideally, we recommend using the AGPL-v3 license.

Make sure your code's license is compatible with the license(s) of the various components and libraries you use if applicable.

description

Description of the analyzer. Please be concise and clear. The description is shown in the Cortex UI, TheHive and MISP.

dataTypeList

The list of TheHive datatypes supported by the analyzer. Currently TheHive accepts the following datatypes:

- domain
- file
- filename
- fqdn
- hash
- ip
- mail
- mail_subject
- other
- regexp
- registry
- uri_path
- url
- user-agent

If you need additional datatypes for your analyzer, please let us know at support@thehive-project.org.

baseConfig

Name used to group configuration items common to several analyzer. This prevent the user to enter the same API key for all analyzer flavors. The Cortex analyzer config page group configuration items by their `baseConfig`.

config

Configuration dedicated to the analyzer's flavor. This is where we typically specify the TLP level of observables allowed to be analyzed with the `check_tlp` and `max_tlp` parameters. For example, if `max_tlp` is set to 2 (TLP:AMBER), TLP:RED observables cannot be analyzed.

max_tlp

The TLP level above which the analyzer must not be executed.

TLP	max_tlp value
Unknown	-1
WHITE	0
GREEN	1
AMBER	2
RED	3

check_tlp

This is a boolean parameter. When `true`, `max_tlp` is checked. And if the input's TLP is above `max_tlp`, the analyzer is not executed.

For consistency reasons, we do recommend setting both `check_tlp` and `max_tlp` even if `check_tlp` is set to `false`.

max_pap

The PAP level above which the analyzer must not be executed.

TLP	max_tlp value
Unknown	-1
WHITE	0
GREEN	1
AMBER	2
RED	3

check_pap

This is a boolean parameter. When `true`, `max_pap` is checked. And if the input's PAP is above `max_pap`, the analyzer is not executed.

For consistency reasons, we do recommend setting both `check_pap` and `max_pap` even if `check_pap` is set to `false`.

command

The command used to run the analyzer. That's typically the full, absolute path to the main program file.

configurationItems

The list of configurationItems is necessary in order to be able to set all configuration variables for analyzers directly in the Cortex 2 user interface. As in the VirusTotal example above can be seen, every item is a json object that defines:

- name (string)
- description (string)
- type (string)
- multi (boolean)
- required (boolean)
- defaultValue (according to type, optional)

The `multi` parameter allows to pass a list as configuration variable instead of a single string or number. This is used e.g. in the MISP analyzer that queries multiple servers in one run and needs different parameters for that.

Output

The output of an analyzer depends on the success or failure of its execution.

If the analyzer **fails** to execute:

```
{
  "success": false,
  "errorMessage": ".."
}
```

- When `success` is set to `false`, it indicates that something went wrong during the execution.
- `errorMessage` is free text - typically the error output message.

If the analyzer **succeeds** (i.e. it runs without any error):

```
{
  "success": true,
  "artifacts": [...],
  "summary": {
    "taxonomies": [...]
  },
  "full": {...}
}
```

- When `success` is set to `true`, it indicates that the analyzer ran successfully.
- `artifacts` is a list of indicators extracted from the produced report.
- `full` is the full report of the analyzer. It is free form, as long as it is JSON formatted.
- `summary` is used in TheHive for short reports displayed in the observable list and in the detailed page of each observable. It contains a list of taxonomies.

– taxonomies:

```
"taxonomies": [
  {
    "namespace": "NAME",
    "predicate": "PREDICATE",
    "value": "\"VALUE\"",
    "level": "info"
  }
]
```

- `namespace` and `predicate` are free values but they should be as concise as possible. For example, the VirusTotal analyzer uses *VT* as a namespace and *Score* as a predicate.
- `level` intends to convey the maliciousness of the result: :
 - * `info` : the analyzer produced an information, and the short report is shown in blue color in TheHive.
 - * `safe` : the analyzer did not find anything suspicious or the analyzed observable is safe according to the analyzer. TheHive displays the short report in green color.
 - * `suspicious` : the analyzer found that the observable is either suspicious or warrants further investigation. The short report has an orange color in TheHive.
 - * `malicious` : the analyzer found that the observable is malicious. The short report is red colored in TheHive.

The Cortexutils Python Library

So far, all the published analyzers have been written in Python. We released a special Python library called `cortexutils` to help developers easily write their programs. Note though that Python is not mandatory for analyzer coding and any language that runs on Linux can be used, though you won't have the benefits of the CortexUtils library.

Cortexutils can be used with Python 2 and 3. To install it :

```
pip install cortexutils
```

or

```
pip3 install cortexutils
```


Report Templates

When using TheHive, analysts can submit an observable for analysis to one or several Cortex instances by a click of a button. Once finished, Cortex returns the result to TheHive. The TheHive displays that result using HTML templates for short and long reports.

Cortex Result in TheHive

TheHive receives the Cortex result which is simply the JSON formatted analyzer output described above:

- The `summary` section is read to display short reports in the observables list and in the detailed observable page. This is stored in a **dict** object named `content` within TheHive.
- The `full` section is read to display long reports when clicking the short report in the observable list or when accessing a detailed observable page. In TheHive application, it is stored in a **dict** object named `content`.

Displayed Information

When No Template is Imported

In the event that the analyzer report templates are not imported in TheHive (only administrators can do such an operation via the *Admin > Report Templates* menu):

- In the observable list, TheHive is able to display the analyzer `summary` results using a builtin style sheet associated with the previously described taxonomy.
- In the detailed observable page:
 - the `full` result is displayed in raw format (the JSON output from Cortex)
 - the `summary` result is **not displayed**.

When Templates are Imported

If templates are imported into TheHive:

- Short reports are displayed in the observable list and in the detailed observable page.



VT:Score="14/56"

- Long reports are displayed when clicking on the short reports or in the detailed observable page.

Report for VirusTotal_GetReport_2_0 analysis of Mon, May 22nd, 2017 14:15 +02:00 [Show Raw Report](#)

Summary

Score 45/61

Last analysis date 2017-05-22 12:05:02

Virus Total [View Full Report](#)

Scans

Scanner	Detected	Result	Details	Update	Version
Bkav	✓			20170522	1.3.0.8876
MicroWorld-eScan	✗	Gen:Variant.Razy.175324		20170522	12.0.250.0
nProtect	✓			20170522	2017-05-22.02
CMC	✓			20170521	1.1.0.977
CAT-QuickHeal	✓			20170522	14.00
McAfee	✗	RDN/Generic.hra		20170522	6.0.6.653
Malwarebytes	✓			20170522	2.1.1.1115
VIPRE	✗	Trojan.Win32.Generic!BT		20170522	58266

Writing Templates

To display results nicely in TheHive, write two HTML templates:

- One for short reports
- One for long reports

When TheHive users import them in the application, they will be definitely more efficient at reading the analyzer reports and do their job accordingly.

If the analyzer is made of different flavors (i.e. has different service interaction files with a json extension), you should provide two HTML templates (short and long reports) for each flavor.

For example, the VirusTotal analyzer comes in two flavors hence it has 4 HTML templates:

```
thehive-templates/VirusTotal_GetReport_3_0
|-- long.html
`-- short.html
thehive-templates/VirusTotal_Scan_3_0
|-- long.html
`-- short.html
```

The folder's name is the concatenation of the name and the version values found in the service interaction files.

TheHive uses Bootstrap and AngularJS so you can leverage them in your templates.

Short Report Templates (short.html)

The short report uses taxonomies and is built into the analyzers by the `summary()` function. Report templates read it as shown in the example below:

```
<span class="label" ng-repeat="t in content.taxonomies"
  ng-class="{ 'info': 'label-info', 'safe': 'label-success',
    'suspicious': 'label-warning',
    'malicious': 'label-danger' }[t.level]">
  {{t.namespace}}:{{t.predicate}}={{t.value}}
</span>
```

If you want to change or add the information displayed in the short report in the detailed observable page, you have to update the `summary()` function in the analyzer's program and edit `short.html` as well. Basically, copy the code in your `short.html` template and it will do the job.

Long Report Templates (long.html)

Long report templates are more or less free form as long as it reads the content of the relevant section in the Cortex result (full). Feel free to check what has already been written for existing analyzers to write yours.

A good start can be:

```
<!-- Success -->
<div class="panel panel-danger" ng-if="success">
  <div class="panel-heading">
    ANALYZERNAME Report
  </div>
  <div class="panel-body">
    [...]                               <= code here
  </div>
</div>

<!-- General error -->
<div class="panel panel-danger" ng-if="!success">
  <div class="panel-heading">
    <strong>{{(artifact.data || artifact.attachment.name) | fang}}</strong>
  </div>
  <div class="panel-body">
    <dl class="dl-horizontal" ng-if="content.errorMessage">
      <dt><i class="fa fa-warning"></i> ANALYZERNAME: </dt>
      <dd class="wrap">{{content.errorMessage}}</dd>
    </dl>
  </div>
</div>
```

7.3.2 Submitting an Analyzer

Review your Service Interaction File(s)

Review your service interaction files. For example, let's check the VirusTotal JSON analyzer configuration file(s):

```
{
  "name": "VirusTotal_GetReport",
  "version": "3.0",
  "author": "CERT-BDF",
  "url": "https://github.com/TheHive-Project/Cortex-Analyzers",
  "license": "AGPL-V3",
  "description": "Get the latest VirusTotal report for a file, hash, domain or an IP_
↪address",
  "dataTypeList": ["file", "hash", "domain", "ip"],
  "baseConfig": "VirusTotal",
  "config": {
    "check_tlp": true,
    "max_tlp": 3,
    "service": "get"
  },
  "command": "VirusTotal/virustotal.py"
}
```

Ensure that all information is correct and particularly the `author` and `license` parameters.

Provide the List of Requirements

If your analyzer is written in Python, make sure to complete the `requirements.txt` file with the list of all the external libraries that are needed to run the analyzer correctly.

Check the Taxonomy

We chose to use a formatted summary report to match a taxonomy as described above. If you want your analyzer reports in the observable lists, ensure that your summary matches this format. If your analyzer is written in Python and you are using our `cortexutils` library, you can use the `summary()` and `build_taxonomy()` functions.

Provide Global Configuration Parameters

When submitting your analyzer, please provide the necessary global configuration in `/etc/cortex/application.conf` if needed. You can provide this information in a `README` file.

Verify Execution

Use these three simple checks before submitting your analyzer:

- Ensure it works with the expected configuration, TLP or dataType.
- Ensure it works with missing configuration, dataType or TLP: your analyzer must generate an explicit error message.
- Ensure the long report template handles error messages correctly.

7.4 Creating Your First Node

Today, you will learn how to create your first node for n8n.

7.4.1 Prerequisites

You have knowledge of:

- JavaScript/TypeScript
- REST APIs
- Expressions in n8n

Install the following tools:

- Git: You can find instructions on how to install Git [here](#).
- Node.js and npm: You can find instructions on how to install both using nvm (Node Version Manager) [here](#). The current minimum version is 16. In case you already have Node.js and npm installed, you can check the current version with the following command:

```
node -v
npm -v
```

Note: Use node version 16.x and npm version 6.x. If using npm version 7+, you must enable legacy peer dependencies by setting: `npm config set legacy-peer-deps true`.

- Lerna: You can install lerna globally with the following command:

```
npm install --global lerna@5.1.6
```

7.4.2 Selecting the Node

The first thing that we have to do is pick the service we want to create the node for. We will use SendGrid [here](#) as an example.

For the sake of brevity, we will only showcase how to add the functionality to create a contact. Since n8n's repository already has a SendGrid node, we will name this node FriendGrid to avoid conflicts.

7.4.3 Cloning the Repository

In Energy SOAR repository [download](#) n8n development package by running the following command in your terminal (don't forget to replace <USERNAME> and <PASSWORD> with your repository credentials):

n8n is built from five main packages:

- cli
- core
- editor-ui
- nodes-base
- nodes-energy

All these packages are under the `/packages` folder in the main n8n folder. We will be working in the `nodes-energy` folder as it contains custom Energy SOAR nodes. Specifically, `/packages/nodes-energy/nodes`, `packages/nodes-energy/credentials`, and `packages/nodes-energy/package.json`.

The folder `nodes` contains all the nodes in n8n. The folder `credentials` contains all the credentials that the different nodes use. Each node can define multiple credentials. For example, OAuth2 or API Key. Each credential requires different parameters that the user will have to input. The credentials data that the user provides is stored in an encrypted format in n8n's database. The file `package.json` contains all the npm packages that the nodes use. It also contains all the nodes and credentials that are loaded when n8n is started.

7.4.4 Creating the Node

1. Go to `packages/nodes-energy/nodes`.
2. Create a folder called `FriendGrid` (the folder names are PascalCase).
3. Within the `FriendGrid` folder, create a file called `FriendGrid.node.ts` (`YourNodeName.node.ts`).
4. Download and add the `FriendGrid` icon [here](#) to the folder. Name it `friendGrid.svg`.
5. The icon property has to be either a 60x60 pixels PNG or an SVG and must exist in the node's folder.
6. An SVG is preferable. In case you have to use a PNG, make sure that it is compressed. A good tool for that is [tinypng](#).
7. A good place to find company icons is [gilbarbara/logos](#).
8. Paste the following code in the `FriendGrid.node.ts` file.

```
import {
  IExecuteFunctions,
} from 'n8n-core';

import {
  IDataObject,
  INodeExecutionData,
  INodeType,
  INodeTypeDescription,
} from 'n8n-workflow';

import {
  OptionsWithUri,
} from 'request';
```

(continues on next page)

(continued from previous page)

```

export class FriendGrid implements INodeType {
  description: INodeTypeDescription = {
    displayName: 'FriendGrid',
    name: 'friendGrid',
    icon: 'file:friendGrid.svg',
    group: ['transform'],
    version: 1,
    description: 'Consume FriendGrid API',
    defaults: {
      name: 'FriendGrid',
      color: '#1A82e2',
    },
    inputs: ['main'],
    outputs: ['main'],
    credentials: [
      // Node credentials which the user gets displayed and
      // can change on the node.
    ],
    properties: [
      // Node properties which the user gets displayed and
      // can change on the node.
    ],
  };

  async execute(this: IExecuteFunctions): Promise<INodeExecutionData[][]> {
    return [[]];
  }
}

```

Your directory structure should now look like the following:

```

FriendGrid
- FriendGrid.node.ts
- friendGrid.svg

```

7.4.5 Adding the Node to Editor UI

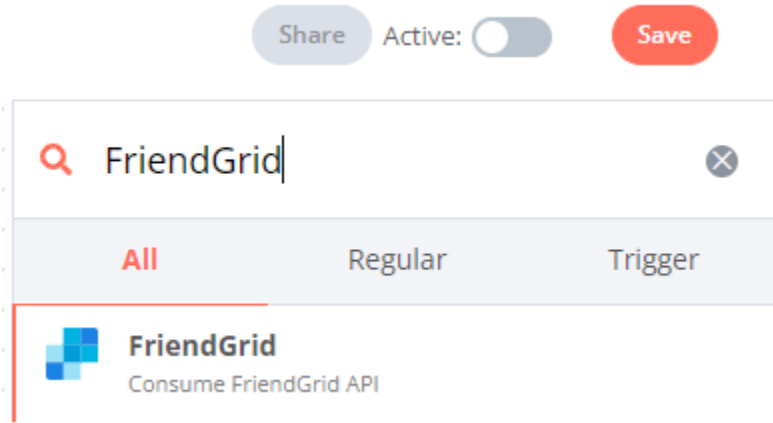
n8n uses the properties set in the property description to render the node in the Editor UI. These properties are display-Name, name, color, icon, description, and subtitle.

Let's see how the node looks in the UI by following these steps:

1. Go to `/packages/nodes-energy/package.json`.
2. Paste `"dist/nodes/FriendGrid/FriendGrid.node.js"`, in the nodes array to register the node (in alphabetical order).
3. Go to the project's main folder (n8n) in the terminal and run the following commands (it can take a few minutes):
 - The first command installs all dependencies of all the modules and links them together.
 - The second command builds all the code.
 - The third command starts n8n in development mode.

```
lerna bootstrap --hoist
npm run build
export N8N_CUSTOM_EXTENSIONS="/packages/nodes-energy"; npm run dev
```

4. Open your browser and go to `localhost:5678` and you should be able to see the Editor UI.
5. Open the Create Node menu, type FriendGrid, and click on it to add the node to the Editor UI.



Notes

- On startup, n8n will load all the nodes and credentials (more about credentials later) that are registered in `/packages/nodes-energy/package.json`.
- The property `description.name` uses camelCase.
- The property `description.color` is the company branding's hexadecimal color. This is usually available on the company's website under style guide. In case the website does not include this information, there are other websites that help you get a company's branding colors. For example, brandpalettes.com.

7.4.6 Creating the UI for the Node

Double-clicking on the FriendGrid node will open the Node Editor View. It will be empty since we haven't added any UI components yet. Luckily, n8n provides predefined JSON-based UI components that we can use to ask the user for different types of data.

SendGrid's docs [here](#) mention that to create a contact, we need to provide the following pieces of information:

- email - Required
- first_name - Optional
- last_name - Optional

There are more parameters that can be provided to create a contact in FriendGrid, but we will use only these three in this tutorial.

7.4.7 Resources and Operations

Now, n8n requires a couple of parameters as well:

- resource - Required
- operation - Required

You can get the node to work without these two parameters, but these should be added for the sake of consistency with the other nodes. Resources and Operations help in organizing all the functionalities of a node. These ensure that all the functionalities of a node remain easily discoverable as the node grows.

The resource value is always singular and its value is the name of the API resource that we want to use. Since we are working with contacts, the resource value would be `contact`. The operation value is always singular as well and it is the name of the operation to perform over the resource. Since we are creating contacts, the operation value would be `create`. You might say that you can “Add a contact” and you are right, but we try to use the same operations (`create`, `delete`, `get`, `getAll` and `update`) across all the nodes.

7.4.8 Adding required fields

Let’s make the Node Editor View ask for these parameters:

Add the following under `description.properties` in `packages/nodes-energy/nodes/FriendGrid/FriendGrid.node.ts`.

```
{
  displayName: 'Resource',
  name: 'resource',
  type: 'options',
  options: [
    {
      name: 'Contact',
      value: 'contact',
    },
  ],
  default: 'contact',
  required: true,
  description: 'Resource to consume',
},
{
  displayName: 'Operation',
  name: 'operation',
  type: 'options',
  displayOptions: {
    show: {
      resource: [
        'contact',
      ],
    },
  },
  options: [
    {
      name: 'Create',
      value: 'create',
      description: 'Create a contact',
    },
  ],
}
```

(continues on next page)

(continued from previous page)

```

    },
  ],
  default: 'create',
  description: 'The operation to perform.',
},
{
  displayName: 'Email',
  name: 'email',
  type: 'string',
  required: true,
  displayOptions: {
    show: {
      operation: [
        'create',
      ],
      resource: [
        'contact',
      ],
    },
  },
  default: '',
  description: 'Primary email for the contact',
},
},

```

Stop the current n8n process by pressing `ctrl + c` in the terminal in which you are running n8n. Run again, by entering the following in the terminal.

```
export N8N_CUSTOM_EXTENSIONS="/packages/nodes-energy"; npm run dev
```

Go to `localhost:5678` (opens new window), refresh the page, and open the node again. The node should now look like in the following image.

FriendGrid's required fields

7.4.9 Adding optional fields

We have given the node the possibility to ask for all the required parameters needed to create a contact. But, what about the optional parameters?

We can add them below the email parameter and set `required: false`. However, if we had more than two optional parameters, and most APIs do, the UI would become overwhelming for the users. To avoid this, we use a UI element named collection (usually called 'Additional Fields') to group all the optional parameters together.

Add the following below the email field in `packages/nodes-energy/nodes/FriendGrid/FriendGrid.node.ts`.

```
{
  displayName: 'Additional Fields',
  name: 'additionalFields',
  type: 'collection',
  placeholder: 'Add Field',
  default: {},
  displayOptions: {
    show: {
      resource: [
        'contact',
      ],
      operation: [
        'create',
      ],
    },
  },
  options: [
    {
      displayName: 'First Name',
      name: 'firstName',
      type: 'string',
      default: '',
    },
    {
      displayName: 'Last Name',
      name: 'lastName',
      type: 'string',
      default: '',
    },
  ],
},
```

Stop the current `n8n` process by pressing `ctrl + c` in the terminal in which you are running `n8n`. Run again, by entering the following in the terminal.

```
export N8N_CUSTOM_EXTENSIONS="/packages/nodes-energy"; npm run dev
```

Go to `localhost:5678` (opens new window), refresh the page, and open the node again. The node should now look like in the following image.

FriendGrid's all fields

Now all our optional fields are presented in the UI and can be set individually depending on the user's use-case.

7.4.10 Creating the UI for credentials

Most REST APIs use some sort of authentication mechanism. FriendGrid's REST API uses API Keys. The API Key informs them about who is making the request to their system and gives you access to all the functionality that the API provides. Given all the things it can do, this has to be treated as a sensitive piece of information and should be kept private.

n8n gives you the ability to ask for sensitive information using credentials. In the credentials, you can use all the generally available UI elements. Additionally, the data that is stored using the credentials would be encrypted before being saved to the database. In order to do that, n8n uses an encryption key.

With that in mind, let's create the UI to ask for the user's FriendGrid API Key. The process of creating and registering credentials is similar to that of creating and registering the node:

Go to `packages/nodes-energy/credentials`. Within the `credentials` folder, create a file named `FriendGridApi.credentials.ts`. Paste the following code.

```
import {
  ICredentialType,
  NodePropertyTypes,
} from 'n8n-workflow';

export class FriendGridApi implements ICredentialType {
  name = 'friendGridApi';
  displayName = 'FriendGrid API';
  documentationUrl = 'friendGrid';
  properties = [
    {
      displayName: 'API Key',
      name: 'apiKey',
      type: 'string' as NodePropertyTypes,
      default: '',
    },
  ],
};
```

Go to `/packages/nodes-energy/package.json`. Paste `"dist/credentials/FriendGridApi.credentials.js"`, in the `credentials` array to register the credentials (in an alphabetical order). Got to `packages/nodes-energy/nodes/FriendGrid/FriendGrid.node.ts`. Associate the credentials with the node by adding the following to `description.credentials`.

```
{
  name: 'friendGridApi',
  required: true,
},
```

Stop the current n8n process by pressing `ctrl + c` in the terminal in which you are running n8n. Run again, by entering the following in the terminal.

```
export N8N_CUSTOM_EXTENSIONS="/packages/nodes-energy"; npm run dev
```

When you go to the Node Editor view, you should see the following. FriendGrid's create credentials

7.4.11 FriendGrid's credentials

7.4.12 Mapping the UI fields to the API

With the UI that we added, we now have all the data that we need to make a request to the FriendGrid API and create contacts.

This is where the execute method comes into play. Every time the node is executed, this method will be run. Within this method, we can have access to the input items and to the parameters that the user set in the UI, including the credentials. To map the fields to the API, perform the following steps:

Go to package/nodes-energy/nodes/FriendGrid.node.ts. Replace the current execute method with the following code.

```
async execute(this: IExecuteFunctions): Promise<INodeExecutionData[][]> {
  let responseData;
  const resource = this.getNodeParameter('resource', 0) as string;
  const operation = this.getNodeParameter('operation', 0) as string;
  // Get credentials the user provided for this node
  const credentials = await this.getCredentials('friendGridApi') as IDataObject;

  if (resource === 'contact') {
    if (operation === 'create') {
      // get email input
      const email = this.getNodeParameter('email', 0) as string;
      // get additional fields input
      const additionalFields = this.getNodeParameter('additionalFields', 0) as
↪ IDataObject;
      const data: IDataObject = {
        email,
      };

      Object.assign(data, additionalFields);

      // Make http request according to API reference
      const options: OptionsWithUri = {
        headers: {
          'Accept': 'application/json',
          'Authorization': `Bearer ${credentials.apiKey}`,
        },
        method: 'PUT',
        body: {
          contacts: [
            data,
          ],
        },
        uri: `https://api.sendgrid.com/v3/marketing/contacts`,
        json: true,
      };

      responseData = await this.helpers.request(options);
    }
  }
}
```

(continues on next page)

(continued from previous page)

```
// Map data to n8n data
return [this.helpers.returnJsonArray(responseData)];
}
```

Stop the current n8n process by pressing `ctrl + c` in the terminal in which you are running n8n. Run again, by entering the following in the terminal.

```
export N8N_CUSTOM_EXTENSIONS="/packages/nodes-energy"; npm run dev
```

Enter the credentials (FriendGrid API Key), contact parameters, and execute the node. Instructions to find the FriendGrid API Key can be found [here](#). If everything went well, you should see the following.

7.4.13 Creating a contact in FriendGrid with n8n

Now we can successfully create contacts in FriendGrid from n8n.

7.4.14 Processing multiples items

In real life, you'll probably have a workflow with more than one node. Our current implementation does not play well with the other nodes. If the data is coming into our FriendGrid node from another node, and that outputs, for example, two contacts, our node will process just the first contact. We want our node to process as many items as it receives.

This is when the `this.getInputData()` function comes into play. Let's update our node so that it can process multiple items.

In the Editor UI, create a new workflow. Add a Function node and connect it to the Start node. Open the function node and replace the existing code with the following.

```
return [
  {
    json: {
      name: 'ricardo@n8n.io'
    }
  },
  {
    json: {
      name: 'hello@n8n.io'
    }
  },
]
```

Execute the Function node. We're using the function node for testing, but you can think of it as any node that is returning "two people" (or more). These two people need to be added to FriendGrid as contacts. Output of the Function node

Add a FriendGrid node to the workflow and connect it to the Function node. Add an expression in the Email field of the FriendGrid node and reference the name property that the Function node outputs. Using expressions in the FriendGrid node

Replace the existing execute method with the following:

```
async execute(this: IExecuteFunctions): Promise<INodeExecutionData[][]> {
  const items = this.getInputData();
  let responseData;
```

(continues on next page)

(continued from previous page)

```

const returnData = [];
const resource = this.getNodeParameter('resource', 0) as string;
const operation = this.getNodeParameter('operation', 0) as string;
// Get credentials the user provided for this node
const credentials = await this.getCredentials('friendGridApi') as IDataObject;

for (let i = 0; i < items.length; i++) {
  if (resource === 'contact') {
    if (operation === 'create') {
      // get email input
      const email = this.getNodeParameter('email', i) as string;
      // get additional fields input
      const additionalFields = this.getNodeParameter('additionalFields', i) as
↪ IDataObject;

      const data: IDataObject = {
        email,
      };

      Object.assign(data, additionalFields);

      // Make http request according to API reference
      const options: OptionsWithUri = {
        headers: {
          'Accept': 'application/json',
          'Authorization': `Bearer ${credentials.apiKey}`,
        },
        method: 'PUT',
        body: {
          contacts: [
            data,
          ],
        },
        uri: `https://api.sendgrid.com/v3/marketing/contacts`,
        json: true,
      };

      responseData = await this.helpers.request(options);
      returnData.push(responseData);
    }
  }
}
// Map data to n8n data structure
return [this.helpers.returnJsonArray(returnData)];
}

```

Execute the workflow. If you open the FriendGrid node, you should see the following.

7.4.15 Output of the FriendGrid node

As showcased above, both the items were processed. That's how all nodes in n8n work (with a few exceptions). They will automatically iterate over all the items and process them.

Let's go over the final version of the execute method. We are getting the items returned by the `this.getInputData()` function and iterating over all of them. Additionally, while doing so, we use the item index to get the correct parameter value using the function `this.getNodeParameters()`. For example, with the following input:

```
[
  {
    json: {
      name: 'ricardo@n8n.io'
    }
  },
  {
    json: {
      name: 'hello@n8n.io'
    }
  },
]
```

The `this.getNodeParameters(ParameterName, index)` function outputs the following:

Index	Parameter Name	Output
0	email	ricardo@n8n.io
1	email	hello@n8n.io

We used the `this.helpers.request(options)` method to make the HTTP Request that creates the contact in FriendGrid. The FriendGrid endpoint returns something like this:

```
{
  "job_id": "b82aca74-3640-4097-85ec-7801d833c2cb"
}
```

We then used the `this.helpers.returnJsonArray()` method to map the API's output data to n8n's data structure. The node then ends up returning the data like the following:

```
[
  {
    "json":{
      "job_id": "b82aca74-3640-4097-85ec-7801d833c2cb"
    }
  }
]
```


7.4.16 Summary

In this tutorial, we implemented the “Create a Contact” functionality of the FriendGrid API. First of all, we made the node show up in the Editor UI and in the Create Node menu with FriendGrid’s branding. Then, we added the fields necessary to create a contact in FriendGrid. We also added the credentials so that the API Key could be stored safely. Finally, we mapped all the parameters to the FriendGrid API.

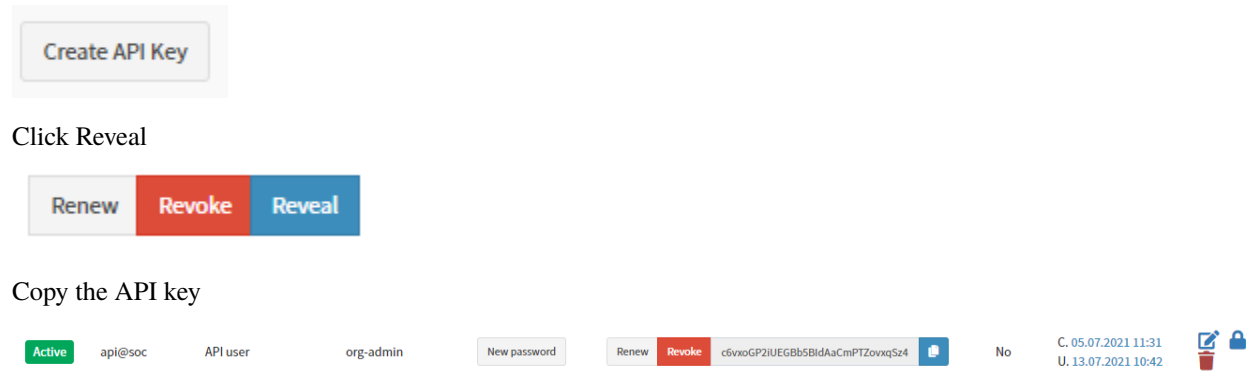
This is just the tip of the iceberg. We built a regular node that consumes a REST API, but a regular node can do everything that can be done with Node.js. Aside from regular nodes you can also build Trigger nodes.

7.5 Energy Logserver SIEM

This integration send alerts from Energy Logserver SIEM to Energy SOAR.

7.5.1 Create API key

Create new (non-admin) user and generate API key.



The screenshot shows the 'Create API Key' button in the top left. Below it, the 'Click Reveal' button is shown. The main part of the screenshot displays the API key details for a user named 'api@soc' (API user, org-admin). The API key is 'c6vnoGP2iUEGBb5BldAaCmPTZovxqSz4'. The key is active and has a 'New password' button next to it. The 'Renew' and 'Revoke' buttons are also visible. The 'Reveal' button is highlighted in blue. The API key is displayed in a red box. The 'No' button is also visible. The 'C. 05.07.2021 11:31' and 'U. 13.07.2021 10:42' timestamps are shown. The 'API user' and 'org-admin' roles are listed. The 'New password' button is next to the API key. The 'Renew' and 'Revoke' buttons are also visible. The 'Reveal' button is highlighted in blue. The API key is displayed in a red box. The 'No' button is also visible. The 'C. 05.07.2021 11:31' and 'U. 13.07.2021 10:42' timestamps are shown.

7.5.2 Edit Alert

Add configuration in the Alert service config.

```
# vi /opt/alert/config.yaml
```

```
hive_connection:
  hive_host: https://<Energy_SOAR_IP>/base
  hive_apikey: <api_key>
```

Restart the Alert service

```
# systemctl restart alert
```

7.5.3 Alert rule configuration

Configure details in the alert rule configuration

```
alert: hivealerter
hive_alert_config_type: classic
hive_alert_config:
  type: "AUDIT"
  source: "SIEM"
  severity: 2
  tags: ["ELS","audit"]
  tlp: 3
  status: "New"
  follow: True
hive_observable_data_mapping:
- ip: "{match[src_ip]}"
  message: "Source IP address"
  tags: ["src: SIEM"]
- domain: "{match[username]}"
  message: "Audit username"
  tags: ["src: SIEM"]
```

7.5.4 Custom message

By default Energy Logserver SIEM send a json with all alert fields. You can customize your message using markdown.

For example:

```
alert_text: "## Summary\r\n\r\n\r\n\r\n| | |\r\n|---|---|\r\n| IP | {} |\r\n| Rule | {} |\r\n\r\n\r\nLog: `{}`\r\nFull log: \r\n```\r\n{}\r\n```\r\n"\r\n\r\nalert_text_args:
- data.srcip
- rule.description
- full_log
- previous_output
```

Preview:

Summary

IP	20.114.64.94
Rule	Multiple web server 400 error codes from same source ip.

Log: 20.114.64.94 - - [07/Mar/2022:23:54:56 +0100] "GET /new-index.php HTTP/1.1" 404 34123 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.102 Safari/537.36" **0.637459** Full log:

```
20.114.64.94 - - [07/Mar/2022:23:54:54 +0100] "GET /b.php HTTP/1.1" 404 34123 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.102 Safari/537.36" **0.646807**
20.114.64.94 - - [07/Mar/2022:23:54:54 +0100] "GET /v.php HTTP/1.1" 404 34123 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.102 Safari/537.36" **0.669269**
20.114.64.94 - - [07/Mar/2022:23:54:55 +0100] "GET /n.php HTTP/1.1" 404 34121 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.102 Safari/537.36" **0.643011**
20.114.64.94 - - [07/Mar/2022:23:54:53 +0100] "GET /c.php HTTP/1.1" 404 34123 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.102 Safari/537.36" **0.658560**
20.114.64.94 - - [07/Mar/2022:23:54:52 +0100] "GET /x.php HTTP/1.1" 404 34122 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.102 Safari/537.36" **0.685517**
20.114.64.94 - - [07/Mar/2022:23:54:51 +0100] "GET /w.php HTTP/1.1" 404 34123 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.102 Safari/537.36" **0.678701**
20.114.64.94 - - [07/Mar/2022:23:54:50 +0100] "GET /m.php HTTP/1.1" 404 34123 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.102 Safari/537.36" **0.667202**
20.114.64.94 - - [07/Mar/2022:23:54:49 +0100] "GET /l.php HTTP/1.1" 404 34123 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.102 Safari/537.36" **0.665535**
20.114.64.94 - - [07/Mar/2022:23:54:49 +0100] "GET /k.php HTTP/1.1" 404 34123 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.102 Safari/537.36" **0.668652**
20.114.64.94 - - [07/Mar/2022:23:54:48 +0100] "GET /j.php HTTP/1.1" 404 34123 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.102 Safari/537.36" **0.667557**
20.114.64.94 - - [07/Mar/2022:23:54:47 +0100] "GET /h.php HTTP/1.1" 404 34123 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.102 Safari/537.36" **0.663914**
```

7.6 Microsoft Exchange

7.6.1 Installation

Download the Exchange integration.

```
# curl -u'license user:license pwd' \  
-O https://repo.energysoar.com/add-ons/synapse.tar.gz
```

Unpack and install the dependencies.

```
# tar -zxvf synapse.tar.gz -C /opt  
# dnf install -y python3-devel gcc  
# /usr/bin/python3 -m pip install -r /opt/synapse/requirements.txt
```

Install the system service.

```
# cp "/opt/synapse/synapse@.service" /usr/lib/systemd/system/
```

Info: The service allows you to run multiple instances. Create a synapse user.

```
# adduser -r -s /bin/nologin -d /opt/synapse --system synapse
```

Change permissions.

```
# chown -R synapse: /opt/synapse
```

7.6.2 Instance configuration

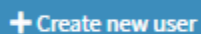
```
# mv /opt/synapse/conf/synapse.conf \  
/opt/synapse/conf/synapse.conf.example  
  
# cp /opt/synapse/conf/synapse.conf.example \  
/opt/synapse/conf/exchange.conf
```

Enter the file `/opt/synapse/conf/exchange.conf` and make the following changes.

Set the API key and user in TheHive section.


```
user:  
api_key:
```

To do this, create a new technical account. Log in as an admin or soc-admin to the Energy SOAR system. In the case of an admin, click on the organization in which you want to create the user. Then create a new local user.

A blue rectangular button with a white plus icon and the text "Create new user".

```
Login: synapse@energysoar.local  
Full name: Synapse  
Profile: analyst
```

If the user already exists, you can create an API key by clicking on the following button.

A rectangular button with a light gray border and a light gray background, containing the text "Create API Key" in a dark gray font.

Then to copy the key, you need to open it by clicking the Reveal button.

A rectangular button with a solid blue background and white text that reads "Reveal".

In the EWS section, provide data for the technical account from which we will read emails.

```
username:  
password:  
auth_type:NTLM  
smtp_address:  
folder_name:Inbox
```

Inbox is the main folder to which all emails are usually sent. If the integration is to read emails from another catalog, you should specify it here. In the [Instance] section, change the name from synapse to exchange.

Start the instance

```
# systemctl enable --now synapse@exchange
```


In this documentation we use local addresses. When you connect externally then you should external IP under secure http - https://YOUR_IP.

8.1 Base API Guide

8.1.1 Authentication

Most API calls require authentication. Credentials can be provided using a session cookie, an API key or directly using HTTP basic authentication (when enabled).

Using API key

Session cookie is suitable for browser authentication, not for a dedicated tool. The easiest solution if you want to write a tool that leverages Base module's API is to use API key authentication. API keys can be generated using the Web interface of the product, under the user admin area. For example, to list cases, use the following curl command:

```
curl -H 'Authorization: Bearer ***API*KEY***' http://127.0.0.1:9000/base/api/case
```

Using basic authentication

Base module also supports basic authentication (disabled by default). You can enable it by adding `auth.method.basic=true` in the configuration file.

```
curl -u mylogin:mypassword http://127.0.0.1:9000/base/api/case
```

8.1.2 Alert

Model definition

Required attributes:

- **title** (text) : title of the alert
- **description** (text) : description of the alert
- **severity** (number) : severity of the alert (1: low; 2: medium; 3: high) **default=2**
- **date** (date) : date and time when the alert was raised **default=now**

- **tags** (multi-string) : case tags **default=empty**
- **tlp** (number) : **TLP** (0: white; 1: green; 2: amber; 3: red) **default=2**
- **status** (AlertStatus) : status of the alert (*New, Updated, Ignored, Imported*) **default=New**
- **type** (string) : type of the alert (read only)
- **source** (string) : source of the alert (read only)
- **sourceRef** (string) : source reference of the alert (read only)
- **artifacts** (multi-artifact) : artifact of the alert. It is a array of JSON object containing artifact attributes **default=empty**
- **follow** (boolean) : if true, the alert becomes active when updated **default=true**

Optional attributes:

- **caseTemplate** (string) : case template to use when a case is created from this alert. If the alert specifies a non-existent case template or doesn't supply one, TheHive will import the alert into a case using a case template that has the exact same name as the alert's type if it exists. For example, if you raise an alert with a type value of **splunk** and you do not provide the **caseTemplate** attribute or supply a non-existent one (for example **splink**), Base module will import the alert using the case template called **splunk** if it exists. Otherwise, the alert will be imported using an empty case (i.e. from scratch).

Attributes generated by the backend:

- **lastSyncDate** (date) : date of the last synchronization
- **case** (string) : id of the case, if created

Alert ID is computed from **type**, **source** and **sourceRef**.

Alert Manipulation

Alert methods

Get an alert

An alert's details can be retrieve using the url:

```
GET      /api/alert/:alertId
```

The alert ID is obtained by List alerts or Find alerts API.

If the parameter **similarity** is set to "1" or "true", this API returns information on cases which have similar observables. With this feature, output will contain the **similarCases** attribute which list case details with:

- **artifactCount**: number of observables in the original case
- **iocCount**: number of observables marked as IOC in original case
- **similarArtifactCount**: number of observables which are in alert and in case
- **similarIocCount**: number of IOCs which are in alert and in case

warning IOCs are observables

Examples

Get alert without similarity data:


```
curl -H 'Authorization: Bearer ***API*KEY***' http://127.0.0.1:9000/api/alert/
↪ce2c00f17132359cb3c50dfbb1901810
```

It returns:

```
{
  "_id": "ce2c00f17132359cb3c50dfbb1901810",
  "_type": "alert",
  "artifacts": [],
  "createdAt": 1495012062014,
  "createdBy": "myuser",
  "date": 1495012062016,
  "description": "N/A",
  "follow": true,
  "id": "ce2c00f17132359cb3c50dfbb1901810",
  "lastSyncDate": 1495012062016,
  "severity": 2,
  "source": "instance1",
  "sourceRef": "alert-ref",
  "status": "New",
  "title": "New Alert",
  "tlp": 2,
  "type": "external",
  "user": "myuser"
}
```

Get alert with similarity data:

```
curl -H 'Authorization: Bearer ***API*KEY***' http://127.0.0.1:9000/api/alert/
↪ce2c00f17132359cb3c50dfbb1901810?similarity=1
```

It returns:

```
{
  "_id": "ce2c00f17132359cb3c50dfbb1901810",
  "_type": "alert",
  "artifacts": [],
  "createdAt": 1495012062014,
  "createdBy": "myuser",
  "date": 1495012062016,
  "description": "N/A",
  "follow": true,
  "id": "ce2c00f17132359cb3c50dfbb1901810",
  "lastSyncDate": 1495012062016,
  "severity": 2,
  "source": "instance1",
  "sourceRef": "alert-ref",
  "status": "New",
  "title": "New Alert",
  "tlp": 2,
  "type": "external",
  "user": "myuser",
  "similarCases": [
```

(continues on next page)

(continued from previous page)

```

    {
      "_id": "AVwwrym-Rw5vhyJUfdJW",
      "artifactCount": 5,
      "endDate": null,
      "id": "AVwwrym-Rw5vhyJUfdJW",
      "iocCount": 1,
      "resolutionStatus": null,
      "severity": 1,
      "similarArtifactCount": 2,
      "similarIocCount": 1,
      "startDate": 1495465039000,
      "status": "Open",
      "tags": [
        "src:MISP"
      ],
      "caseId": 1405,
      "title": "TEST",
      "tlp": 2
    }
  ]
}

```

Create an alert

An alert can be created using the following url:

```
POST    /api/alert
```

Required case attributes (cf. models) must be provided.

If an alert with the same tuple type, source and sourceRef already exists, Base module will refuse to create it.

This call returns attributes of the created alert.

Examples

Creation of a simple alert:

```

curl -XPOST -H 'Authorization: Bearer ***API*KEY***' -H 'Content-Type: application/json' \
  http://127.0.0.1:9000/api/alert -d '{
  "title": "New Alert",
  "description": "N/A",
  "type": "external",
  "source": "instance1",
  "sourceRef": "alert-ref"
}'

```

It returns:

```

{
  "_id": "ce2c00f17132359cb3c50dfbb1901810",
  "_type": "alert",
  "artifacts": [],

```

(continues on next page)

(continued from previous page)

```

    "createdAt": 1495012062014,
    "createdBy": "myuser",
    "date": 1495012062016,
    "description": "N/A",
    "follow": true,
    "id": "ce2c00f17132359cb3c50dfbb1901810",
    "lastSyncDate": 1495012062016,
    "severity": 2,
    "source": "instance1",
    "sourceRef": "alert-ref",
    "status": "New",
    "title": "New Alert",
    "tlp": 2,
    "type": "external",
    "user": "myuser"
  }

```

Creation of another alert:

```

curl -XPOST -H 'Authorization: Bearer ***API*KEY***' -H 'Content-Type: application/json' \
  http://127.0.0.1:9000/api/alert -d '{
  "title": "Other alert",
  "description": "alert description",
  "type": "external",
  "source": "instance1",
  "sourceRef": "alert-ref",
  "severity": 3,
  "tlp": 3,
  "artifacts": [
    { "dataType": "ip", "data": "127.0.0.1", "message": "localhost" },
    { "dataType": "domain", "data": "energysoar.com", "tags": ["home", "file"] },
    { "dataType": "file", "data": "logo.svg;image/svg+xml;
    PD94bWwgdmlVyc2lvbj0iMS4wIiBlbmNvZGluZz0idXRmLTgiPz4NCjwhLS0gR2VuZXJhdG9yOiBBZG9iZSBJbGx1c3RyYXRvcjAxO
    ", "message": "logo" }
  ],
  "caseTemplate": "external-alert"
}'

```

Merge an alert

An alert can merge in a case using the URL:

```
POST /api/alert/:alertId/merge/:caseId
```

Each observable of the alert will be added to the case if it doesn't exist in the case. The description of the alert will be appended to the case's description.

The HTTP response contains the updated case.

Example

Merge the alert `ce2c00f17132359cb3c50dfbb1901810` in case `AVXeF-pZmeHK_2HEYj2z`:

```
curl -XPOST -H 'Authorization: Bearer ***API*KEY***' http://127.0.0.1:9000/api/alert/
→ce2c00f17132359cb3c50dfbb1901810/merge/AVXeF-pZmeHK_2HEYj2z
```

The call returns:

```
{
  "severity": 3,
  "createdBy": "myuser",
  "createdAt": 1488918582777,
  "caseId": 1,
  "title": "My first case",
  "startDate": 1488918582836,
  "owner": "myuser",
  "status": "Open",
  "description": "This case has been created by my custom script

  ### Merged with alert #10 my alert title

  This is my alert description",
  "user": "myuser",
  "tlp": 2,
  "flag": false,
  "id": "AVXeF-pZmeHK_2HEYj2z",
  "_id": "AVXeF-pZmeHK_2HEYj2z",
  "_type": "case"
}
```

Bulk merge alert

This API merge several alerts with one case:

```
POST    /api/alert/merge/_bulk
```

The observable of each alert listed in `alertIds` field will be imported into the case (identified by `caseId` field). The description of the case *is not* modified.

The HTTP response contains the case.

Example

Merge the alerts `ce2c00f17132359cb3c50dfbb1901810` and `a97148693200f731cfa5237ff2edf67b` in case `AVXeF-pZmeHK_2HEYj2z`:

```
curl -XPOST -H 'Authorization: Bearer ***API*KEY***' -H 'Content-Type: application/json' -
→http://127.0.0.1:9000/api/alert/merge/_bulk -d '{
  "caseId": "AVXeF-pZmeHK_2HEYj2z",
  "alertIds": ["ce2c00f17132359cb3c50dfbb1901810", "a97148693200f731cfa5237ff2edf67b"]
}'
```

The call returns:

```
{
  "severity": 3,
```

(continues on next page)

(continued from previous page)

```

"createdBy": "myuser",
"createdAt": 1488918582777,
"caseId": 1,
"title": "My first case",
"startDate": 1488918582836,
"owner": "myuser",
"status": "Open",
"description": "This case has been created by my custom script",
"user": "myuser",
"tlp": 2,
"flag": false,
"id": "AVXeF-pZmeHK_2HEYj2z",
"_id": "AVXeF-pZmeHK_2HEYj2z",
"_type": "case"
}

```

8.1.3 Observable

Model definition

Required attributes:

- **data** (string) : content of the observable (read only). An observable can't contain data and attachment attributes
- **attachment** (attachment) : observable file content (read-only). An observable can't contain data and attachment attributes
- **dataType** (enumeration) : type of the observable (read only)
- **message** (text) : description of the observable in the context of the case
- **startDate** (date) : date of the observable creation **default=now**
- **tlp** (number) : **TLP** (0: white; 1: green; 2: amber; 3: red) **default=2**
- **ioc** (boolean) : indicates if the observable is an IOC **default=false**
- **status** (artifactStatus) : status of the observable (*Ok* or *Deleted*) **default=Ok**

Optional attributes:

- **tags** (multi-string) : observable tags

Observable manipulation

Observable methods

List Observables of a Case

Complete observable list of a case can be retrieved by performing a search:

```
POST    /api/case/artifact/_search
```

Parameters:

- **query**: { "_parent": { "_type": "case", "_query": { "_id": "<<caseId>>" } } }

- range: all

<<caseId>> must be replaced by case id (not the case number !)

8.1.4 Case

Model definition

Required attributes:

- title (text) : title of the case
- description (text) : description of the case
- severity (number) : severity of the case (1: low; 2: medium; 3: high) **default=2**
- startDate (date) : date and time of the begin of the case **default=now**
- owner (string) : user to whom the case has been assigned **default=use who create the case**
- flag (boolean) : flag of the case **default=false**
- tlp (number) : **TLP** (0: white; 1: green; 2: amber; 3: red) **default=2**
- tags (multi-string) : case tags **default=empty**

Optional attributes:

- resolutionStatus (caseResolutionStatus) : resolution status of the case (*Indeterminate, FalsePositive, TruePositive, Other* or *Duplicated*)
- impactStatus (caseImpactStatus) : impact status of the case (*NoImpact, WithImpact* or *NotApplicable*)
- summary (text) : summary of the case, to be provided when closing a case
- endDate (date) : resolution date
- metrics (metrics) : list of metrics

Attributes generated by the backend:

- status (caseStatus) : status of the case (*Open, Resolved* or *Deleted*) **default=Open**
- caseId (number) : Id of the case (auto-generated)
- mergeInto (string) : ID of the case created by the merge
- mergeFrom (multi-string) : IDs of the cases that were merged

Case Manipulation

Case methods

Create a Case

A case can be created using the following url :

POST	/api/case
------	-----------

Required case attributes (cf. models) must be provided.

This call returns attributes of the created case.

Examples

Creation of a simple case:

```
curl -XPOST -H 'Authorization: Bearer ***API*KEY***' -H 'Content-Type: application/json' \
→http://127.0.0.1:9000/base/api/case -d '{
  "title": "My first case",
  "description": "This case has been created by my custom script"
}'
```

It returns:

```
{
  "severity": 3,
  "createdBy": "myuser",
  "createdAt": 1488918582777,
  "caseId": 1,
  "title": "My first case",
  "startDate": 1488918582836,
  "owner": "myuser",
  "status": "Open",
  "description": "This case has been created by my custom script",
  "user": "myuser",
  "tlp": 2,
  "flag": false,
  "id": "AVqqdpY2yQ6w1DNC8aDh",
  "_id": "AVqqdpY2yQ6w1DNC8aDh",
  "_type": "case"
}
```

Creation of another case:

```
curl -XPOST -H 'Authorization: Bearer ***API*KEY***' -H 'Content-Type: application/json' \
→http://127.0.0.1:9000/base/api/case -d '{
  "title": "My second case",
  "description": "This case has been created by my custom script, its severity is high,
→tlp is red and it contains tags",
  "severity": 3,
  "tlp": 3,
  "tags": ["automatic", "creation"]
}'
```

Creating a case with Tasks & Customfields:

```
curl -XPOST -H 'Authorization: Bearer ***API*KEY***' -H 'Content-Type: application/json' \
→http://127.0.0.1:9000/base/api/case -d '{
  "title": "My first case",
  "description": "This case has been created by my custom script"
  "tasks": [{
    "title": "mytask",
    "description": "description of my task"
  }],
}
```

(continues on next page)

(continued from previous page)

```

    "customFields": {
      "cvss": {
        "number": 9,
      },
      "businessImpact": {
        "string": "HIGH"
      }
    }
  }
}'

```

For the `customFields` object, the attribute names should correspond to the `ExternalReference` (`cvss` and `businessImpact` in the example above) not to the name of custom fields.

8.1.5 Log

Model definition

Required attributes:

- `message` (text) : content of the Log
- `startDate` (date) : date of the log submission **default=now**
- `status` (`logStatus`) : status of the log (*Ok* or *Deleted*) **default=Ok**

Optional attributes:

- `attachment` (attachment) : file attached to the log

Log manipulation

Log methods

Create a log

The URL used to create a task is:

```
POST /api/case/task/<<taskId>>/log
```

<<taskId>> must be replaced by task id

Required log attributes (cf. models) must be provided.

This call returns attributes of the created log.

Examples

Creation of a simple log in task `AVqqeXc9yQ6w1DNC8aDj`:

```

curl -XPOST -H 'Authorization: Bearer ***API*KEY***' -H 'Content-Type: application/json' \
  http://127.0.0.1:9000/base/api/case/task/AVqqeXc9yQ6w1DNC8aDj/log -d '{
  "message": "Some message"
}'

```

It returns:


```
{
  "startDate": 1488919949497,
  "createdBy": "admin",
  "createdAt": 1488919949495,
  "user": "myuser",
  "message": "Some message",
  "status": "Ok",
  "id": "AVqqi3C-yQ6w1DNC8aDq",
  "_id": "AVqqi3C-yQ6w1DNC8aDq",
  "_type": "case_task_log"
}
```

If log contains an attachment, the request must be in multipart format:

```
curl -XPOST -H 'Authorization: Bearer ***API*KEY***' http://127.0.0.1:9000/base/api/case/
task/AVqqeXc9yQ6w1DNC8aDj/log -F '_json={"message": "Screenshot of fake site"}';
type=application/json' -F 'attachment=@screenshot1.png;type=image/png'
```

It returns:

```
{
  "createdBy": "myuser",
  "message": "Screenshot of fake site",
  "createdAt": 1488920587391,
  "startDate": 1488920587394,
  "user": "myuser",
  "status": "Ok",
  "attachment": {
    "name": "screenshot1.png",
    "hashes": [
      "086541e99743c6752f5fd4931e256e6e8d5fc7afe47488fb9e0530c390d0ca65",
      "8b81e038ae0809488f20b5ec7dc91e488ef601e2",
      "c5883708f42a00c3ab1fba5bbb65786c"
    ],
    "size": 15296,
    "contentType": "image/png",
    "id": "086541e99743c6752f5fd4931e256e6e8d5fc7afe47488fb9e0530c390d0ca65"
  },
  "id": "AVqq1Sy0yQ6w1DNC8aDx",
  "_id": "AVqq1Sy0yQ6w1DNC8aDx",
  "_type": "case_task_log"
}
```

8.1.6 Task

Model definition

Required attributes:

- **title** (text) : title of the task
- **status** (taskStatus) : status of the task (*Waiting*, *InProgress*, *Completed* or *Cancel*) **default=Waiting**
- **flag** (boolean) : flag of the task **default=false**

Optional attributes:

- **owner** (string) : user who owns the task. This is automatically set to current user when status is set to *InProgress*
- **description** (text) : task details
- **startDate** (date) : date of the beginning of the task. This is automatically set when status is set to *Open*
- **endDate** (date) : date of the end of the task. This is automatically set when status is set to *Completed*

Task manipulation

Task methods

Create a task

The URL used to create a task is:

```
POST /api/case/<<caseId>>/task
```

<<caseId>> must be replaced by case id (not the case number !)

Required task attributes (cf. models) must be provided.

This call returns attributes of the created task.

Examples

Creation of a simple task in case AVqqdpY2yQ6w1DNC8aDh:

```
curl -XPOST -H 'Authorization: Bearer ***API*KEY***' -H 'Content-Type: application/json' -d '{
  "title": "Do something"
}'
```

It returns:

```
{
  "createdAt": 1488918771513,
  "status": "Waiting",
  "createdBy": "myuser",
  "title": "Do something",
  "order": 0,
  "user": "myuser",
  "flag": false,
  "id": "AVqqeXc9yQ6w1DNC8aDj",
}
```

(continues on next page)

(continued from previous page)

```
{
  "_id": "AVqqeXc9yQ6w1DNC8aDj",
  "_type": "case_task"
}
```

Creation of another task:

```
curl -XPOST -H 'Authorization: Bearer ***API*KEY***' -H 'Content-Type: application/json' -
→http://127.0.0.1:9000/base/api/case/AVqqdpY2yQ6w1DNC8aDh/task -d '{
  "title": "Analyze the malware",
  "description": "The malware XXX is analyzed using sandbox ...",
  "owner": "Joe",
  "status": "InProgress"
}'
```

8.1.7 Base module Model Definition

Field Types

- **string** : textual data (example “malware”).
- **text** : textual data. The difference between **string** and **text** is in the way content can be searched. **string** is searchable as-is whereas **text**, words (token) are searchable, not the whole content (example “Ten users have received this ransomware”).
- **date** : date and time using timestamps with milliseconds format.
- **boolean** : true or false
- **number** : numeric value
- **metrics** : JSON object that contains only numbers

Field can be prefixed with **multi-** in order to indicate that multiple values can be provided.

Common Attributes

All entities share the following attributes:

- **createdBy** (text) : login of the user who created the entity
- **createdAt** (date) : date and time of the creation
- **updatedBy** (text) : login of the user who last updated the entity
- **upadtedAt** (date) : date and time of the last update
- **user** (text) : same value as **createdBy** (this field is deprecated) These attributes are handled by the back-end and can’t be directly updated.

8.1.8 Request formats

Base module accepts several parameter formats within a HTTP request. They can be used indifferently. Input data can be:

- a query string
- URL-encoded form
- multi-part
- JSON

Hence, the requests below are equivalent.

Query String

```
curl -XPOST 'http://127.0.0.1:9000/api/login?user=me&password=secret'
```

URL-encoded Form

```
curl -XPOST 'http://127.0.0.1:9000/api/login' -d user=me -d password=secret
```

JSON

```
curl -XPOST http://127.0.0.1:9000/api/login -H 'Content-Type: application/json' -d '{
  "user": "me",
  "password": "secret"
}'
```

Multi-part

```
curl -XPOST http://127.0.0.1:9000/api/login -F '_json=<-;type=application/json' << _EOF_
{
  "user": "me",
  "password": "secret"
}
_EOF_
```

Response Format

Base module outputs JSON data.

8.1.9 User

Model definition

Required attributes:

- **login / id** (string) : login of the user
- **userName** (text) : Full name of the user
- **roles** (multi-userRole) : Array containing roles of the user (read, write or admin)
- **status** (userStatus) : Ok or Locked **default=Ok**
- **preference** (string) : JSON object containing user preference **default={}**

Optional attributes:

- **avatar** (string) : avatar of user. It is an image encoded in base 64
- **password** (string) : user password if local authentication is used

Attributes generated by the backend:

- **key** (uuid) : API key to authenticate this user (deprecated)

User Manipulation

User methods

- **with-key** (boolean)

Create a User

A user can be created using the following URL:

```
POST    /api/user
```

Required case attributes (cf. models) must be provided.

This call returns attributes of the created user.

This call is authenticated and requires admin role.

Examples

Creation of a user:

```
curl -XPOST -H 'Authorization: Bearer ***API*KEY***' -H 'Content-Type: application/json' \
  http://127.0.0.1:9000/api/user -d '{
  "login": "georges",
  "name": "Georges Abitbol",
  "roles": ["read", "write"],
  "password": "La classe"
}'
```

It returns:

```
{
  "createdBy": "myuser",
  "name": "Georges Abitbol",
  "roles": ["read", "write" ],
  "_id": "georges",
  "user": "myuser",
  "createdAt": 1496561862924,
  "status": "Ok",
  "id": "georges",
  "_type": "user",
  "has-key": false
}
```

If external authentication is used (LDAP or AD) password field must not be provided.

8.2 Automation API Guide

8.2.1 Introduction

Automation module offers a REST API that can be leveraged by various applications and programs to interact with it. The following guide describe the Automation API to allow developers to interface the powerful observable analysis engine with other SIRPs (Security Incident Response Platforms) besides Base module, TIPs (Threat Intelligence Platforms), SIEMs or scripts. Please note that the Web UI of Automation module exclusively leverage the REST API to interact with the back-end.

Note: You can use [Cortex4py](#), the Python library we provide, to facilitate interaction with the REST API of Automation module. You need Cortex4py 2.0.0 or later as earlier versions are not compatible with Cortex 2.

All the exposed APIs share the same *request & response formats* and *authentication strategies* as described below.

There are also some transverse parameters supported by several calls, in addition to *utility APIs*.

If you want to create an analyzer, please read the *How to Write and Submit an Analyzer* guide.

Request & Response Formats

Automation module accepts several parameter formats within a HTTP request. They can be used indifferently. Input data can be:

- A query string
- A URL-encoded form
- A multi-part
- JSON

Hence, the requests shown below are equivalent.

Query String

```
curl -XPOST 'https://127.0.0.1/automation/api/login?user=me&password=secret'
```

URL-encoded Form

```
curl -XPOST 'https://127.0.0.1/automation/api/login' -d user=me -d password=secret
```

JSON

```
curl -XPOST https://127.0.0.1/automation/api/login -H 'Content-Type: application/json' -
  ↪d '{
    "user": "me",
    "password": "secret"
  }'
```

Multi-part

```
curl -XPOST https://127.0.0.1/automation/api/login -F '_json=<-;type=application/json' <
  ↪< _EOF_
{
  "user": "me",
  "password": "secret"
}
_EOF_
```

Response Format

For each request submitted, Automation module will respond back with JSON data. For example, if the authentication request is successful, Automation module should return the following output:

```
{"id": "me", "name": "me", "roles": ["read", "analyze", "orgadmin"]}
```

If not, Automation module should return an authentication error:

```
{"type": "AuthenticationError", "message": "Authentication failure"}
```

Authentication

Most API calls require authentication. Credentials can be provided using a **session cookie**, an **API key** or directly using HTTP **basic authentication** (if this method is specifically enabled).

Session cookies are better suited for browser authentication. Hence, **we recommend authenticating with API keys** when calling the Automation module APIs.

Generating API Keys with an orgAdmin Account

API keys can be generated using the Web UI. To do so, connect using an `orgAdmin` account then click on *Organization* and then on the *Create API Key* button in the row corresponding to the user you intend to use for API authentication. Once the API key has been created, click on *Reveal* to display the API key then click on the *copy to clipboard* button if you wish to copy the key to your system's clipboard.

If the user is not yet created, start by clicking on *Add user* to create it then follow the steps mentioned above.

Generating API Keys with a superAdmin Account

You can use a `superAdmin` account to achieve the same result as described above. Once authenticated, click on *Users* then on the *Create API Key* button in the row corresponding to the user you intend to use for API authentication. Please **make sure the user is in the right organization** by thoroughly reading its name, which is shown below the user name. Once the API key has been created, click on *Reveal* to display the API key then click on the *copy to clipboard* button if you wish to copy the key to your system's clipboard.

Authenticating with an API Key

Once you have generated an API key you can use it, for example, to list the Automation module jobs thanks to the following `curl` command:

```
### Using API key
curl -H 'Authorization: Bearer **API_KEY**' https://127.0.0.1/automation/api/job
```

As you can see in the example above, we instructed `curl` to add the *Authorization* header to the request. The value of the header is `Bearer: **API_KEY**`. So if your API key is `GPX20GUAQWwpqnhA6JpOwNGPMfWuxsX3`, the `curl` command above would look like the following:

```
### Using API key
curl -H 'Authorization: Bearer GPX20GUAQWwpqnhA6JpOwNGPMfWuxsX3' https://127.0.0.1/
↳ automation/api/job
```

Using Basic Authentication

Automation module also supports basic authentication but it is disabled by default for security reasons. **If you absolutely need to use it**, you can enable it by adding `auth.method.basic=true` to the configuration file (`/etc/cortex/application.conf` by default). Once you do, restart the Automation module service. You can then, for example, list the Automation module jobs using the following `curl` command:

```
### Using basic authentication
curl -u mylogin:mypassword https://127.0.0.1/automation/api/job
```


8.2.2 Organization APIs

Automation module offers a set of APIs to create, update and list organizations.

Organization Model

An organization (org) is defined by the following attributes:

Please note that `id` and `name` are essentially the same. Also, `createdAt` and `updatedAt` are in *epoch*.

List

It is possible to list all the organizations using the following API call, which requires the API key associated with a `superAdmin` account:

```
curl -H 'Authorization: Bearer **API_KEY**' 'https://127.0.0.1/automation/api/
↳organization'
```

You can also search/filter organizations using the following query:

```
curl -H 'Authorization: Bearer **API_KEY**' -H 'Content-Type: application/json' 'https://
↳127.0.0.1/automation/api/organization/_search' -d '{
  "query": {"status": "Active"}
}'
```

Both APIs supports the `range` and `sort` query parameters described in *paging and sorting details*.

Create

It is possible to create an organization using the following API call, which requires the API key associated with a `superAdmin` account:

```
curl -XPOST -H 'Authorization: Bearer **API_KEY**' -H 'Content-Type: application/json'
↳'https://127.0.0.1/automation/api/organization' -d '{
  "name": "demo",
  "description": "Demo organization",
  "status": "Active"
}'
```

Update

You can update an organization's description and status (Active or Locked) using the following API call. This requires the API key associated with a `superAdmin` account:

```
curl -XPATCH -H 'Authorization: Bearer **API_KEY**' -H 'Content-Type: application/json'
↳'https://127.0.0.1/automation/api/organization/ORG_ID' -d '{
  "description": "New Demo organization",
}'
```

or

```
curl -XPATCH -H 'Authorization: Bearer **API_KEY**' -H 'Content-Type: application/json'
↳ 'https://127.0.0.1/automation/api/organization/ORG_ID' -d '{
  "status": "Active",
}'
```

Delete

Deleting an organization just marks it as **Locked** and doesn't remove the associated data from the DB. To “delete” an organization, you can use the API call shown below. It requires the API key associated with a **superAdmin** account.

```
curl -XDELETE -H 'Authorization: Bearer **API_KEY**' 'https://127.0.0.1/automation/api/
↳ organization/ORG_ID'
```

Obtain Details

This API call returns the details of an organization as described in the *Organization model* section.

```
curl -H 'Authorization: Bearer **API_KEY**' 'https://127.0.0.1/automation/api/
↳ organization/ORG_ID'
```

Let's assume that the organization we are seeking to obtain details about is called *demo*. The `curl` command would be:

```
curl -H 'Authorization: Bearer **API_KEY**' 'https://127.0.0.1/automation/api/
↳ organization/demo'
```

and it should return:

```
{
  "id": "demo",
  "name": "demo",
  "status": "Active",
  "description": "Demo organization",
  "createdAt": 1520258040437,
  "createdBy": "superadmin",
  "updatedBy": "superadmin",
  "updatedAt": 1522077420693
}
```

List Users

As mentioned above, you can use the API to return the list of **all** the users declared withing an organization. For that purpose, use the API call shown below with the API key of an **orgAdmin** or **superAdmin** account. It supports the range and sort query parameters declared in *paging and sorting details*.

```
curl -H 'Authorization: Bearer **API_KEY**' 'https://127.0.0.1/automation/api/
↳ organization/ORG_ID/user'
```

and should return a list of *users*.

If one wants to filter/search for some users (active ones for example), there is a search API to use as below:

```
curl -XPOST -H 'Authorization: Bearer **API_KEY**' -H 'Content-Type: application/json'
→ 'https://127.0.0.1/automation/api/organization/ORG_ID/user/_search' -d '{
  "query": {}
}'
```

It also supports the range and sort query parameters declared in *paging and sorting details*.

List Enabled Analyzers

To list the analyzers that have been enabled within an organization, use the following API call with the API key of an orgAdmin user:

```
curl -H 'Authorization: Bearer **API_KEY**' 'https://127.0.0.1/automation/api/analyzer'
```

It should return a list of *Analyzers*.

Please note that this API call does not display analyzers that are disabled. It supports the range and sort query parameters declared in *paging and sorting details*.

8.2.3 User APIs

The following section describes the APIs that allow creating, updating and listing users within an organization.

User Model

A user is defined by the following attributes:

List All

This API call allows a superAdmin to list and search all the users of all defined organizations:

```
curl -H 'Authorization: Bearer **API_KEY**' 'https://127.0.0.1/automation/api/user'
```

This call supports the range and sort query parameters declared in *paging and sorting details*.

List Users within an Organization

This call is described in *organization APIs*.

Search

This API call allows a superAdmin to perform search on the user accounts created in a Automation module instance:

```
curl -XPOST -H 'Authorization: Bearer **API_KEY**' -H 'Content-Type: application/json'
→ 'https://127.0.0.1/automation/api/user/_search' -d '{
  "query": {}
}'
```

This call supports the range and sort query parameters declared in *paging and sorting details*

Create

This API call allows you to programmatically create user creation. If the call is made by a `superAdmin` user, the request must specify the organization to which the user belongs in the `organization` field.

If the call is made by an `orgAdmin` user, the value of `organization` field must be the same as the user who makes the call: `orgAdmin` users are allowed to create users only in their organization.

```
curl -XPOST -H 'Authorization: Bearer **API_KEY**' -H 'Content-Type: application/json'
↪ 'https://127.0.0.1/automation/api/user' -d '{
  "name": "Demo org Admin",
  "roles": [
    "read",
    "analyze",
    "orgadmin"
  ],
  "organization": "demo",
  "login": "demo"
}'
```

If successful, the call returns a JSON object representing the created user as described *above*.

```
{
  "id": "demo",
  "organization": "demo",
  "name": "Demo org Admin",
  "roles": [
    "read",
    "analyze",
    "orgadmin"
  ],
  "status": "Ok",
  "createdAt": 1526050123286,
  "createdBy": "superadmin",
  "hasKey": false,
  "hasPassword": false
}
```

Update

This API call allows updating the writable attributes of a user account. It's available to users with `superAdmin` or `orgAdmin` roles. Any user can also use it to update their own information (but obviously not their roles).

```
curl -XPATCH -H 'Authorization: Bearer **API_KEY**' -H 'Content-Type: application/json'
↪ 'https://127.0.0.1/automation/api/user/USER_LOGIN' -d '{
  "name": "John Doe",
  "roles": [
    "read",
    "analyze"
  ],
  "status": "Locked"
}'
```

It returns a JSON object representing the updated user as described *above*.

Get Details

This call returns the user details. It's available to users with `superAdmin` roles and to users in the same organization. Every user can also use it to read their own details.

```
curl -H 'Authorization: Bearer **API_KEY**' 'https://127.0.0.1/automation/api/user/USER_LOGIN'
```

It returns a JSON object representing the user as described *previously*.

Set a Password

This call sets the user's password. It's available to users with `superAdmin` or `orgAdmin` roles. Please note that the request needs to be made using HTTPS with a valid certificate on the server's end to prevent credential sniffing or other PITM (Person-In-The-Middle) attacks.

```
curl -XPOST -H 'Authorization: Bearer **API_KEY**' -H 'Content-Type: application/json'
  -d '{
    "password": "SOMEPASSWORD"
  }'
https://127.0.0.1/automation/api/user/USER_LOGIN/password/set'
```

If successful, the call returns 204 (success / no content).

Change a password

This call allows a given user to change only **their own** existing password. It is available to all users including `superAdmin` and `orgAdmin` ones. Please note that if a `superAdmin` or an `orgAdmin` needs to update the password of another user, they must use the `/password/set` call described in the previous subsection.

```
curl -XPOST -H 'Authorization: Bearer **API_KEY**' -H 'Content-Type: application/json'
  -d '{
    "currentPassword": "password",
    "password": "new-password"
  }'
https://127.0.0.1/automation/api/user/USER_LOGIN/password/change'
```

If successful, the call returns 204 (success / no content).

Set and Renew an API Key

This calls allows setting and renewing the API key of a user. It's available to users with `superAdmin` or `orgAdmin` roles. Any user can also use it to renew their own API key. Again, the request needs to be made using HTTPS with a valid certificate on the server's end to prevent credential sniffing or other PITM (Person-In-The-Middle) attacks. You know the drill ;-)

```
curl -XPOST -H 'Authorization: Bearer **API_KEY**' 'https://127.0.0.1/automation/api/
  user/USER_LOGIN/key/renew'
```

If successful, it returns the generated API key in a `text/plain` response.

Get an API Key

This call allows getting a user's API key. It's available to users with `superAdmin` or `orgAdmin` roles. Any user can also use it to obtain their own API key.

```
curl -H 'Authorization: Bearer **API_KEY**' 'https://127.0.0.1/automation/api/user/USER_LOGIN/key'
```

If successful, the generated API key is returned in `text/plain` response

Revoke an API Key

This call allows revoking a user's API key. This call allows revoking a user's API key.

```
curl -XDELETE -H 'Authorization: Bearer **API_KEY**' 'https://127.0.0.1/automation/api/user/USER_LOGIN/key'
```

A successful request returns nothing (HTTP 200 OK).

8.2.4 Job APIs

The following section describes the APIs that allow manipulating jobs. Jobs are basically submissions made to analyzers and the resulting reports.

Job Model

A job is defined by the following attributes:

List and Search

This call allows a user with `read`, `analyze` or `orgAdmin` role to list and search all the analysis jobs made by their organization.

If you want to list all the jobs:

```
curl -XPOST -H 'Authorization: Bearer **API_KEY**' 'https://127.0.0.1/automation/api/job/_search?range=all'
```

If you want to list 10 jobs:

```
curl -XPOST -H 'Authorization: Bearer **API_KEY**' 'https://127.0.0.1/automation/api/job/_search'
```

If you want to list 100 jobs:

```
curl -XPOST -H 'Authorization: Bearer **API_KEY**' 'https://127.0.0.1/automation/api/job/_search?range=0-100'
```

If you want to search jobs according to various criteria:

```
curl -XPOST -H 'Authorization: Bearer **API_KEY**' -H 'Content-Type: application/json'
↪ 'https://127.0.0.1/automation/api/job/_search' -d '{
  "query": {
    "_and": [
      {"status": "Success"},
      {"dataType": "ip"}
    ]
  }
}'
```

This call supports the `range` and `sort` query parameters declared in *paging and sorting details*

Get Details

This call allows a user with `read,analyze` or `orgAdmin` role to get the details of a job. It does not fetch the job report.

```
curl -H 'Authorization: Bearer **API_KEY**' 'https://127.0.0.1/automation/api/job/JOB_ID'
```

It returns a JSON response with the following structure:

```
{
  "id": "AWN4vH3rJ8unegCPB9",
  "analyzerDefinitionId": "Abuse_Finder_2_0",
  "analyzerId": "220483fde9608c580fb6a2508ff3d2d3",
  "analyzerName": "Abuse_Finder_2_0",
  "status": "Success",
  "data": "8.8.8.8",
  "parameters": "{}",
  "tlp": 0,
  "message": "",
  "dataType": "ip",
  "organization": "demo",
  "startDate": 1526299593923,
  "endDate": 1526299597064,
  "date": 1526299593633,
  "createdAt": 1526299593633,
  "createdBy": "demo",
  "updatedAt": 1526299597066,
  "updatedBy": "demo"
}
```

Get Details and Report

This call allows a user with `read,analyze` or `orgAdmin` role to get the details of a job including its report.

```
curl -H 'Authorization: Bearer **API_KEY**' 'https://127.0.0.1/automation/api/job/JOB_ID/
↪report'
```

It returns a JSON response with the structure below. If the job is not yet completed, the `report` field contains a string representing the job status:

```
{
  "id": "AWNei4vH3rJ8unegCPB9",
  "analyzerDefinitionId": "Abuse_Finder_2_0",
  "analyzerId": "220483fde9608c580fb6a2508ff3d2d3",
  "analyzerName": "Abuse_Finder_2_0",
  "status": "Success",
  "data": "8.8.8.8",
  "parameters": "{}",
  "tlp": 0,
  "message": "",
  "dataType": "ip",
  "organization": "demo",
  "startDate": 1526299593923,
  "endDate": 1526299597064,
  "date": 1526299593633,
  "createdAt": 1526299593633,
  "createdBy": "demo",
  "updatedAt": 1526299597066,
  "updatedBy": "demo",
  "report": {
    "summary": {
      "taxonomies": [
        {
          "predicate": "Address",
          "namespace": "Abuse_Finder",
          "value": "network-abuse@google.com",
          "level": "info"
        }
      ]
    },
    "full": {
      "abuse_finder": {
        "raw": "...",
        "abuse": [
          "network-abuse@google.com"
        ],
        "names": [
          "Google LLC",
          "Level 3 Parent, LLC"
        ],
        "value": "8.8.8.8"
      }
    },
    "success": true,
    "artifacts": []
  }
}
```


Wait and Get Job Report

This call is similar the one described above but allows the user to provide a timeout to wait for the report in case it is not available at the time the query was made:

```
curl -H 'Authorization: Bearer **API_KEY**' 'https://127.0.0.1/automation/api/job/JOB_ID/  
↪waitreport?atMost=1minute'
```

The atMost is a duration using the format Xhour, Xminute or Xsecond.

Get Artifacts

This call allows a user with read,analyze or orgAdmin role to get the extracted artifacts from a job if such extraction has been enabled in the corresponding analyzer configuration. Please note that extraction is imperfect and you might have inconsistent or incorrect data.

```
curl -H 'Authorization: Bearer **API_KEY**' 'https://127.0.0.1/automation/api/job/JOB_ID/  
↪artifacts'
```

It returns a JSON array with the following structure:

```
[  
  {  
    "dataType": "ip",  
    "createdBy": "demo",  
    "data": "8.8.8.8",  
    "tlp": 0,  
    "createdAt": 1525432900553,  
    "id": "AWMq4tvLjidKq_asiwcl"  
  }  
]
```

Delete

This API allows a user with analyze or orgAdmin role to delete a job:

```
curl -XDELETE -H 'Authorization: Bearer **API_KEY**' 'https://127.0.0.1/automation/api/  
↪job/JOB_ID'
```

This marks the job as Deleted. However the job's data is not removed from the database.

8.2.5 Analyzer APIs

The following section describes the APIs that allow manipulating analyzers.

Analyzer Model

An analyzer is defined by the following attributes:

Enable

This call allows a user with an `orgAdmin` role to enable an analyzer.

```
curl -XPOST -H 'Authorization: Bearer **API_KEY**' 'https://127.0.0.1/automation/api/
↪organization/analyzer/:analyzerId' -d '{
  "name": "Censys_1_0",
  "configuration": {
    "uid": "XXXX",
    "key": "XXXXXXXXXXXXXXXXXXXX",
    "proxy_http": "http://proxy:9999",
    "proxy_https": "http://proxy:9999",
    "auto_extract_artifacts": false,
    "check_tlp": true,
    "max_tlp": 2
  },
  "rate": 1000,
  "rateUnit": "Day",
  "jobCache": 5
}'
```

List and Search

These calls allow a user with a `analyze` or `orgAdmin` role to list and search all the enabled analyzers within the organization.

```
curl -H 'Authorization: Bearer **API_KEY**' 'https://127.0.0.1/automation/api/analyzer'
```

or

```
curl -XPOST -H 'Authorization: Bearer **API_KEY**' -H 'Content-Type: application/json'
↪'https://127.0.0.1/automation/api/analyzer/_search' -d '{
  "query": {}
}'
```

Both calls supports the `range` and `sort` query parameters declared in *paging and sorting details*, and both return a JSON array of analyzer objects as described in *Analyzer Model section*.

If called by a user with only an `analyzer` role, the `configuration` attribute is not included on the JSON objects.

Get Details

This call allows a user with a `analyze` or `orgAdmin` role to get an analyzer's details.

```
curl -H 'Authorization: Bearer **API_KEY**' 'https://127.0.0.1/automation/api/analyzer/
↳ANALYZER_ID'
```

It returns a analyzer JSON object as described in *Analyzer Model section*.

If called by a user with only an `analyze` role, the `configuration` attribute is not included on the JSON objects.

Get By Type

This call is mostly used by TheHive and allows to quickly get the list of analyzers that can run on the given datatype. It requires an `analyze` or `orgAdmin` role.

```
curl -H 'Authorization: Bearer **API_KEY**' 'https://127.0.0.1/automation/api/analyzer/
↳type/DATA_TYPE'
```

It returns a JSON array of analyzer objects as described in *Analyzer Model section* without the `configuration` attribute, which could contain sensitive data.

Update

This call allows an `orgAdmin` user to update the name, configuration and jobCache of an enabled analyzer.

```
curl -XPATCH -H 'Authorization: Bearer **API_KEY**' -H 'Content-Type: application/json'
↳'https://127.0.0.1/automation/api/analyzer/ANALYZER_ID' -d '{
  "configuration": {
    "key": "XXXXXXXXXXXXXXXXXXXXXXXXXXXX",
    "polling_interval": 60,
    "proxy_http": "http://localhost:8080",
    "proxy_https": "http://localhost:8080",
    "auto_extract_artifacts": true,
    "check_tlp": true,
    "max_tlp": 1
  },
  "name": "Shodan_Host_1_0",
  "rate": 1000,
  "rateUnit": "Day",
  "jobCache": null
}'
```

It returns a JSON object describing the analyzer as defined in *Analyzer Model section*.

Run

This API allows a user with a `analyze` or `orgAdmin` role to run analyzers on observables of different datatypes.

For file observables, the API call must be made as described below:

```
curl -XPOST -H 'Authorization: Bearer **API_KEY**' -H 'Content-Type: application/json'
↪ 'https://127.0.0.1/automation/api/analyzer/ANALYZER_ID/run' \
-F 'attachment=@/path/to/observable-file' \
-F '_json=<-;type=application/json' << _EOF_
{
  "dataType": "file",
  "tlp": 0
}
_EOF_
```

for all the other types of observables, the request is:

```
curl -XPOST -H 'Authorization: Bearer **API_KEY**' -H 'Content-Type: application/json'
↪ 'https://127.0.0.1/automation/api/analyzer/ANALYZER_ID/run' -d '{
  "data": "8.8.8.8",
  "dataType": "ip",
  "tlp": 0,
  "message": "A message that can be accessed from the analyzer",
  "parameters": {
    "key1": "value1",
    "key2": "value2"
  }
}'
```

This call will fetch a similar job from the cache, and if it finds one, it returns it from the cache, based on the duration defined in `jobCache` attribute of the analyzer.

To force bypassing the cache, one can add the following query parameter: `force=1`

```
curl -XPOST -H 'Authorization: Bearer **API_KEY**' -H 'Content-Type: application/json'
↪ 'https://127.0.0.1/automation/api/analyzer/ANALYZER_ID/run?force=1' -d '{
  "data": "8.8.8.8",
  "dataType": "ip",
  "tlp": 0,
  "message": "A message that can be accessed from the analyzer",
  "parameters": {
    "key1": "value1",
    "key2": "value2"
  }
}'
```

Disable

This API allows an orgAdmin to disable an existing analyzer in their organization and delete the corresponding configuration.

```
curl -XDELETE -H 'Authorization: Bearer **API_KEY**' 'https://127.0.0.1/automation/api/
↪ analyzer/ANALYZER_ID'
```

8.2.6 Miscellaneous APIs

Paging and Sorting

All the search API calls allow sorting and paging parameters, in addition to a query in the request's body. These calls usually have URLs ending with the `_search` keyword but that's not always the case.

The followings are query parameters:

- `range`: all or `x-y` where `x` and `y` are numbers (ex: 0-10).
- `sort`: you can provide multiple sort criteria such as: `-createdAt` or `+status`.

Example:

```
curl -XPOST -H 'Authorization: Bearer **API_KEY**' -H 'Content-Type: application/json'
↪ 'http://127.0.0.1/automation/api/organization/ORG_ID/user?range=0-10&sort=-createdAt&
↪ sort=+status' -d '{
  "query": {}
}'
```