
Project Report : The Hive

CSE 406 : Computer Security Sessional

Syed Jarullah Hisham: 1805004
Abdur Rafi : 1805008

Department of Computer Science and Engineering
Bangladesh University of Engineering and Technology

September 13, 2023

Contents

1	High Level Overview	4
2	Architecture	5
3	Workflow	7
4	Purpose and Use Case	9
5	Source Code Overview	10
5.1	Language Used	10
5.2	Main Modules/Folders	10
5.2.1	app/org/thp/thehive	10
5.2.2	client/src/main/scala/org/thp/thehive/client	10
5.2.3	client-common/src	10
5.2.4	conf	11
5.2.5	cortex	11
5.2.6	dto	11
5.2.7	frontend	11
5.2.8	migration	11
5.2.9	misp	11
5.2.10	thehive	11
5.2.11	package	11
6	Analyst Features : Cases	12
6.1	Introduction	12
6.2	Case Creation	12
6.2.1	Empty Case Creation	14
6.2.2	Case Creation from MISP template	15
6.2.3	Case Creation from EDR template	16
6.2.4	Case Creation from Phishing template	17
6.2.5	Apply Case template	18
6.3	Addition to a Case	19
6.4	Details of a Case	20
6.4.1	Left Side View	20
6.4.2	TLP and PAP	21
6.4.3	General Tab	22
6.4.4	Tasks Tab	23
6.4.5	Observables Tab	24
6.4.6	TTPs	25
6.4.7	Attachments Tab	26
6.4.8	History	26
6.5	Other Actions on A Case	27
6.5.1	Statistics	27
6.5.2	Filtering and Sorting	27
6.5.3	Flag a Case	27
6.5.4	Close a Case	28

7 Analyst Features : Alerts	29
7.1 Introduction	29
7.2 Details of an alert	29
7.2.1 Left Side View	30
7.2.2 General Tab	32
7.2.3 Observables Tab	33
7.2.4 TTPs	34
7.2.5 Similar Cases	35
7.2.6 Similar Alerts	35
7.2.7 Responders	35
7.2.8 History	35
7.3 Actions on An Alert	36
7.3.1 Start	37
7.3.2 Close	37
7.3.3 Ignore New Updates	37
7.3.4 New Case from Selection	37
7.3.5 Merge selection into case	39
7.3.6 Responders	39
8 Analyst Features : Tasks	40
8.1 Introduction	40
8.2 Creating a task	40
8.3 Viewing Tasks	41
8.4 Actions on a Task	42
8.5 Adding Activities	43
9 Analyst Features : Dashboard	44
9.1 Introduction	44
9.2 Add a Dashboard	44
9.3 Import Dashboard	46
9.4 Other Actions of Dashboard	47
9.4.1 Edit, Delete, Duplicate and Export Dashboard	47
9.4.2 Filtering and Sorting	47
10 Analyst Features : Search	48
10.1 Introduction	48
10.2 Search Alerts	49
10.3 Search Cases	49
10.4 Search Observables	50
10.5 Search Tasks	50
11 Admin Features : Organisations And Accounts Management	51
11.1 Manage Organisations	51
11.1.1 Create Organisation	51
11.1.2 Details of An Organisation	52
11.1.3 Adding User to An Organisation	52
11.2 Manage Users	53
11.2.1 User Preview	53
11.2.2 Create A User	55
12 Admin Features : Entities Management	56
12.1 Introduction	56
12.2 Profiles	57
12.3 Custom Fields	57
12.3.1 Adding Custom Field	58
12.3.2 Editing Custom Field	59
12.4 Observable Types	59
12.4.1 Adding Observable Type	60
12.4.2 Deleting Observable Type	60
12.5 Case Status	60

12.6	Alert Status	61
12.7	Analyzer Templates	61
12.7.1	Adding Template	62
12.7.2	Modifying Template	63
12.8	Taxonomies	63
12.8.1	Adding Taxonomy	64
12.8.2	Activating Taxonomy	65
12.9	Attack Patterns	65
12.9.1	Details of An Attack Pattern	65
12.9.2	Adding Attack Pattern	66
13	Admin Features : Platform Management	67
13.1	Introduction	67
13.2	License	68
13.3	Platform Status	69
13.4	Cortex	70
13.4.1	Add Cortex Server	70
13.4.2	Delete Cortex Server	71
13.5	MISP	71
13.5.1	Add MISP Server	71
13.5.2	Configure MISP Server Settings	72
13.5.3	Delete MISP Server	72
13.6	Authentication	73
13.7	SMTP	73
13.8	Global EndPoint Creation	74
14	Platform Integration : Integration With Cortex	76
14.1	Introduction	76
14.2	Analyzers	76
14.2.1	Available Analyzers	76
14.2.2	Enabling an Analyzer	77
14.2.3	Using Enabled Analyzer From Hive	78
14.3	Responders	79
14.3.1	Available Responders	79
14.3.2	Enabling a Responder	79
14.3.3	Using Enabled Responder From Hive	80
15	Platform Integration : Integration With MISP	82
15.1	Introduction	82
15.2	Add MISP Server	82
15.3	MISP Alerts	83
15.4	Case Creation From MISP Template	83
16	Platform Integration : Integration With Other Platforms	84
17	Conclusion	85
18	References	86

Chapter 1

High Level Overview

The Hive is a free and open-source Security Incident Response Platform (SIRS) developed by Strange-Bee. It is designed to make life easier for SOCs, CSIRTs, CERTs, and any information security practitioner dealing with security incidents that need to be investigated and acted upon swiftly. The Hive is a web-based application that can be deployed on a single server or as a cluster. It relies on Apache Cassandra for data storage and Elasticsearch for indexing. A file storage solution is also required.

The Hive comes with various features and benefits in terms of security incident response. We will firstly show very brief overview of them. The step by step details will be discussed in the upcoming chapters and sections.

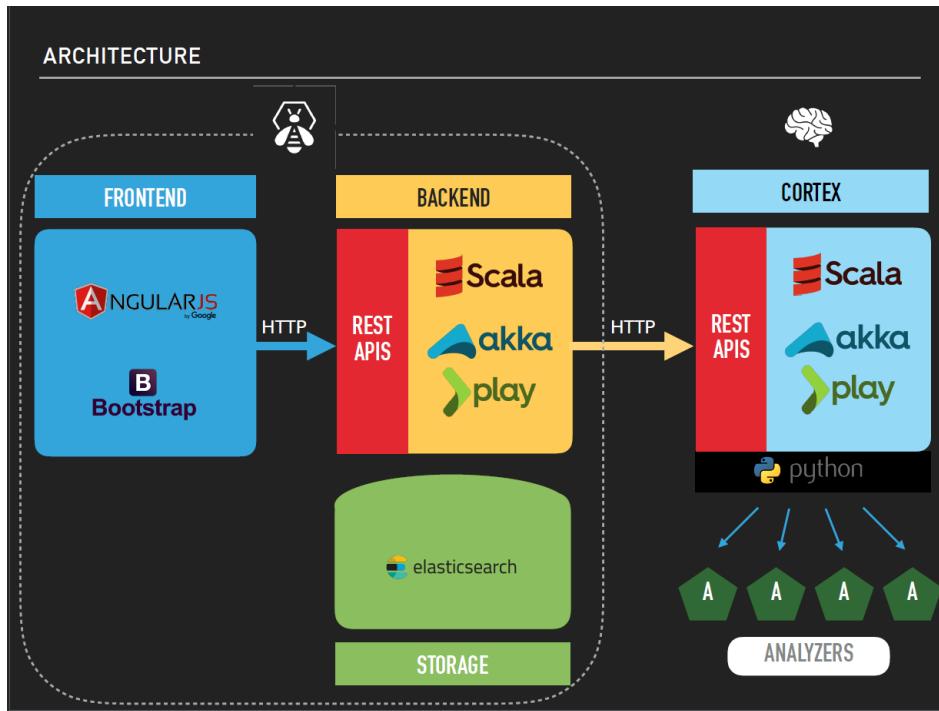
Overview of Features

The Hive provides a variety of features to help with incident response, including:

- **Alert management:** The Hive can ingest alerts from a variety of sources, such as SIEMs, firewalls, and IDS/IPS systems. It provides a dedicated and detailed alert page where us can view the alert details, make comments, and identify similar alerts.
- **Case management:** The Hive allows us to create cases and associate them with alerts, tasks, and observables. us can also define custom statuses and fields for cases.
- **Task management:** The Hive allows us to create tasks and assign them to users. us can also track the progress of tasks and set due dates. Observable management: The Hive allows us to store and manage a variety of observables, such as IP addresses, domains, and hashes. us can also define custom observable types.
- **User management:** The Hive allows us to create and manage user accounts. us can also define user permissions.
- **Integration Capabilities:** The Hive supports a wide range of integrations with external security tools and services. This includes integrations with SIEM systems, threat intelligence feeds, and various data enrichment sources.
- **Observables and Analyzers:** The platform provides the ability to analyze observables (e.g., IP addresses, domains, hashes) through the use of analyzers. Analyzers query external services or databases to gather additional information about observables, aiding in incident investigation.
- **Reporting:** The Hive provides a variety of reports to help us track usr incident response activities. This helps organizations assess their incident response effectiveness.

Chapter 2

Architecture



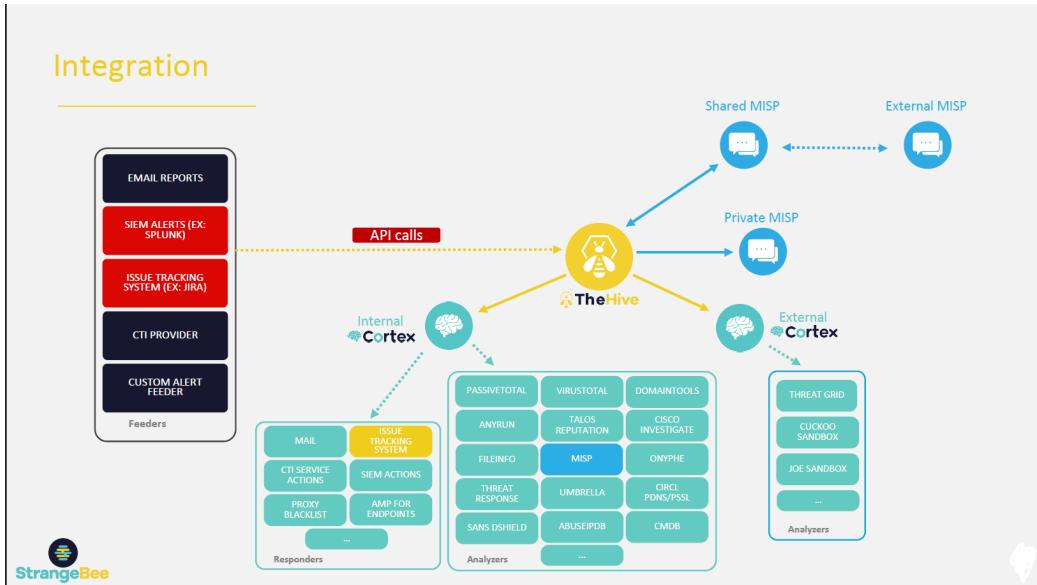
Source: https://chrissanders.org/wp-content/uploads/2017/03/hive_arch-1024x687.png

Figure 2.1: The Hive Architecture

The overall system architecture is made up of the following components:

- **Frontend:** The frontend is responsible for displaying the content of the system to the user. It is built using AngularJS and Bootstrap.
- **Backend:** The backend is responsible for processing the data and providing the data to the frontend. It is built using Scala, Akka, Play Framework, and Slick.
- **Cortex:** Cortex is a real-time streaming analytics platform that is used to process the data from the backend. It is built using Scala, Akka, Play Framework, and Python.
- **Storage:** The storage layer is used to store the data from the system. It is made up of a distributed database, such as Elasticsearch.
- **Analyzers:** The analyzers are used to analyze the data from the system. They can be used to perform tasks such as anomaly detection, fraud detection, and trend analysis.

The system is designed to be scalable and fault-tolerant. The frontend and backend are decoupled, which allows them to be scaled independently. The Cortex platform is also designed to be scalable and fault-tolerant.



Source: https://github.com/randorisec/talks/blob/upload/RandoriSec-Friends2020-Enlarge_your_toolkit/RandoriSec-Friends-Speed_up_IR_with_TheHive_Jerome_Leonard_Nabil_Aduani.pdf

Figure 2.2: The Hive Integration Architecture

The components of the integration architecture are labeled as follows:

- **Integration:** This component is responsible for collecting data from various sources, such as SIEM alerts, email reports, and CTI providers.
- **Feeders:** This component is responsible for ingesting the data from the Integration component and storing it in the storage layer.
- **Analyzers:** This component is responsible for analyzing the data from the storage layer and identifying potential threats.
- **Responders:** This component is responsible for taking action on the threats identified by the analyzers.
- **Storage:** This component is responsible for storing the data from the feeders.

The data flows through the architecture in the following way:

- Data is collected from various sources and sent to the Integration component.
- The Integration component ingests the data and sends it to the Feeders.
- The Feeders store the data in the Storage layer.
- The Analyzers analyze the data from the Storage layer and identify potential threats.
- The Responders take action on the threats identified by the analyzers.

Chapter 3

Workflow

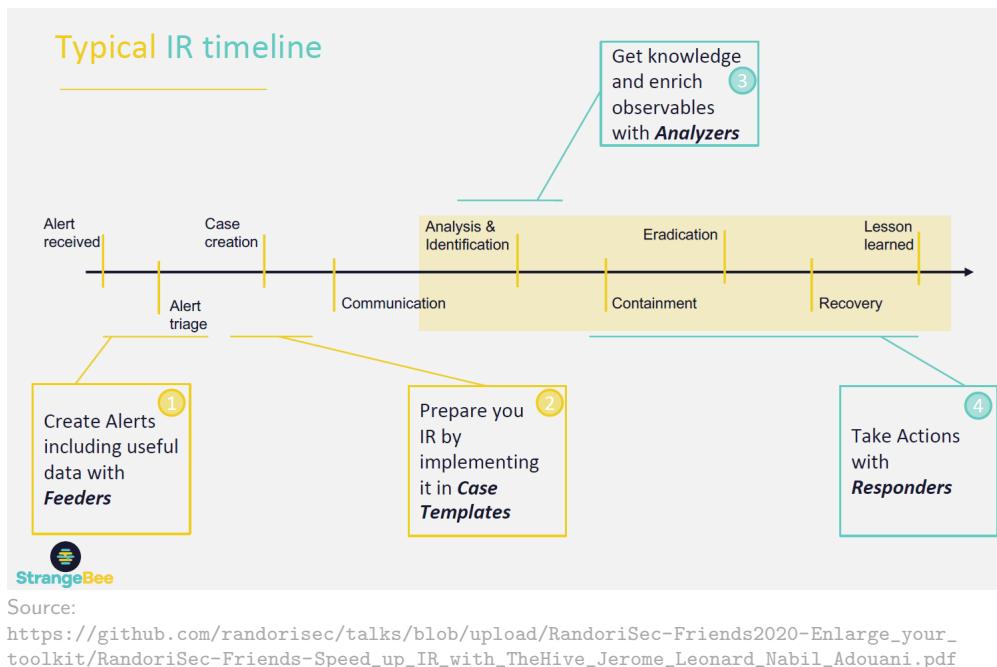


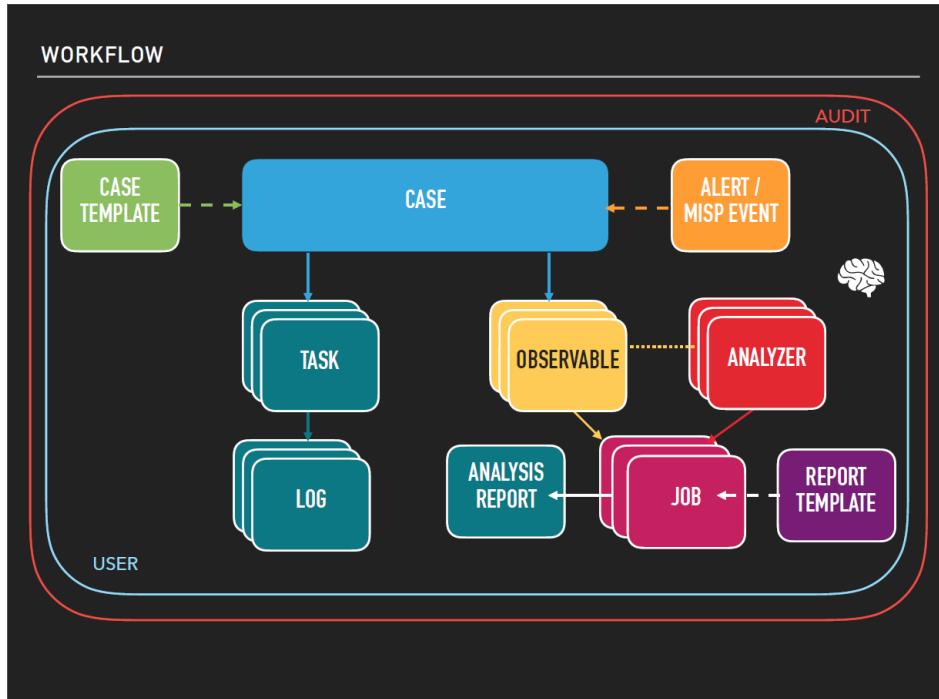
Figure 3.1: Typical Incident Response Timeline

A typical incident response (IR) timeline is divided into the following phases:

- **Alert received:** This is the initial phase, where an alert is received from a source such as a SIEM or firewall.
- **Alert triage:** This phase involves triaging the alert to determine its severity and whether it requires further investigation.
- **Case creation:** If the alert is deemed to be significant, a case is created to track the incident.
- **Analysis & identification:** This phase involves analyzing the data from the alert to identify the threat actor and their methods.
- **Communication:** This phase involves communicating with stakeholders about the incident, such as the incident commander, affected users, and law enforcement.
- **Get knowledge and enrich observables with Analyzers:** This phase involves using analyzers to enrich the data from the alert with additional information, such as threat intelligence and malware signatures.

- **Eradication:** This phase involves removing the threat from the environment.
- **Containment:** This phase involves preventing the threat from spreading.
- **Lesson learned:** This phase involves reviewing the incident to identify lessons learned and improve future incident response.
- **Recovery:** This phase involves restoring the environment to its pre-incident state.

The timeline is not always linear, and some phases may overlap. For example, analysis and identification may be ongoing while eradication and containment are being performed. The IR timeline is a critical tool for organizations to manage incidents effectively.



Source: <https://blogthehiveproject.files.wordpress.com/2017/06/workflow.png>

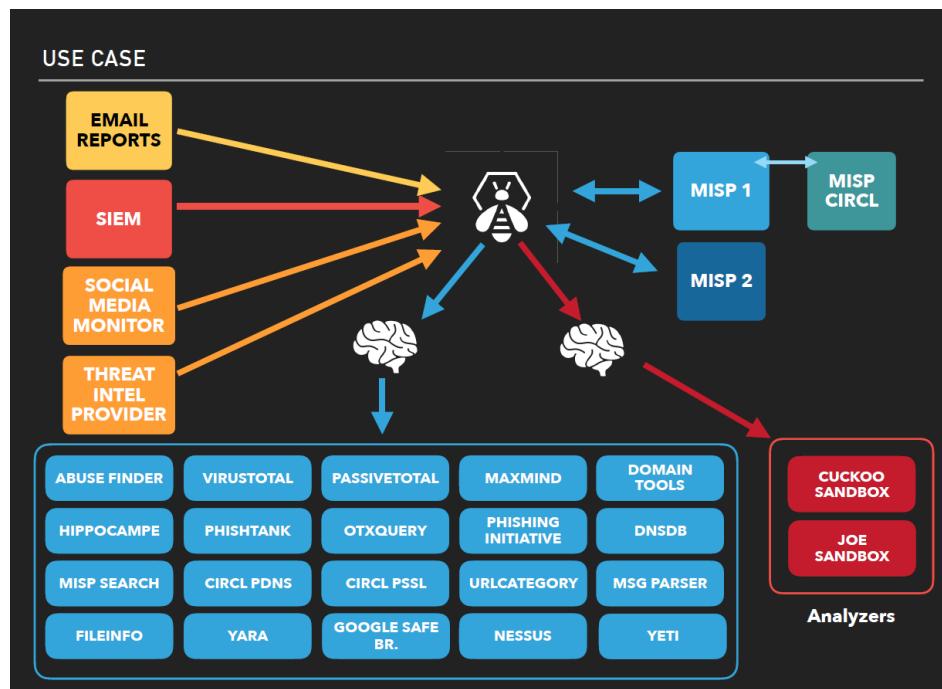
Figure 3.2: The Hive Workflow

The Hive workflow consists of the following steps:

- **Create a case:** This step is used to create a new case in the case management system. The case should be given a unique identifier and a name that describes the incident.
- **Assign the case to an analyst:** This step is used to assign the case to an analyst who will be responsible for investigating the incident. The analyst should have the appropriate skills and experience to investigate the incident.
- **Gather evidence:** This step is used to gather evidence related to the incident. The evidence can include logs, network traffic, and screenshots. The evidence should be collected in a systematic way so that it can be easily analyzed.
- **Analyze the evidence:** This step is used to analyze the evidence to identify the threat actor and their methods. The analyst should use a variety of tools and techniques to analyze the evidence.
- **Respond to the incident:** This step is used to respond to the incident, such as by isolating the affected systems or removing the threat from the environment. The response should be proportionate to the severity of the incident.
- **Close the case:** This step is used to close the case once the incident has been resolved. The case should be closed in the case management system and the evidence should be archived.

Chapter 4

Purpose and Use Case



Source: https://isc.sans.edu/diaryimages/images/tlp-white-jigsaw_falling_into_place-2017-03-001.png

Figure 4.1: The Hive Use Case

A possible use case of the HIVE project consists of the following use cases:

- **Receive email reports:** This use case is used to receive email reports from SIEM systems.
- **Query MISP:** This use case is used to query the MISP threat intelligence platform.
- **Analyze observables:** This use case is used to analyze observables, such as IP addresses and domain names.
- **Respond to incidents:** This use case is used to respond to incidents

The users of the system are labeled as follows:

- **Analyst:** This is the user who is responsible for analyzing alerts and identifying threats.
- **Responder:** This is the user who is responsible for responding to incidents.

Chapter 5

Source Code Overview

The HIVE 5 is not open source. We used the community license for our project. But as the older version (for e.g: The HIVE 4) was open source, we have added a very brief overview of that source code. Although there might be significant difference between two codebase as a lot of things and implementations have changed.

5.1 Language Used

The main programming languages used are Scala and JavaScript.

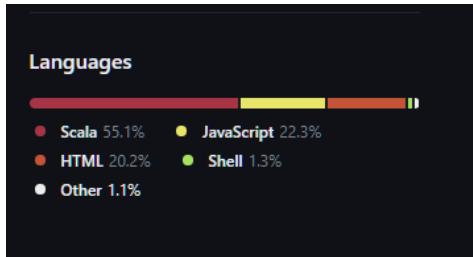


Figure 5.1: Languages Used in The Hive, From Github

5.2 Main Modules/Folders

5.2.1 app/org/thp/thehive

This folder contains a custom http server for the hive. This is the server which is launched when the hive starts and works as a backend.

5.2.2 client/src/main/scala/org/thp/thehive/client

This folder contains the hive client, which is a type of Web Socket client. This is the client used in front end to connect with the backend server. The client uses multiple base clients, which is defined in client-common/src folder.

5.2.3 client-common/src

main/scalal/org/thp/client

Contains code for the base client of the hive. It also contains code for authentication and some kind of proxy web socket client.

test/scalal/org/thp/client

contains tests for the code in the former folder.

5.2.4 conf

Contains configurations of various aspects of the hive, such as default locations of cortex server, misp server, default username and password

5.2.5 cortex

This folder contains codes for integration with cortex. this includes client code of cortex, connectors and various controllers, models and services classes, DTOs for passing data to and from cortex. It also includes test codes.

5.2.6 dto

This folder contains various DTOs (date transfer objects), which are used to carry data from one process to other. All the DTOs have 2 versions, contained in v0 and v1 folders. These mainly defines how the input and outputs of various operations should be. For example, in Alert.scala, 2 classes, InputAlert and OutputSimilarCase are defined. InputAlert contains fields for different attributes an alert can have. Similarly, OutputSimilarCse contains fields relating to the atrributes that are visible in the similar cases section in alert view.

5.2.7 frontend

This contains the code for the web front end of the hive and is a major portion of the code base. The front end is built on pure HTML and vanilla JavaScript. The scripts are organized into various folders based on the features of the hive. For example, there are folders for alert, charts, search, organisation etc.

5.2.8 migration

Contains code for migrating from older versions to newer versions

5.2.9 misp

Contains code for integrating with misp server. Similar to the cortex folder, it also contains client, connector and dtos.

5.2.10 thehive

Contains the bulk of the backend, with various controllers, models and services classes in separate folders. The models folder contains classes for alerts, cases, tasks, observables etc. These model classes define the attributes of the objects. Similarly the controller folder contains classes for the various views available in the hive. For example, the AlertCtrl.scala defines various endpoints for various operations in the alert view.

5.2.11 package

contains code for supporting various ways of installing the hive.

Chapter 6

Analyst Features : Cases

6.1 Introduction

A case provides information on suspicious activity in the environment, security incidents, observables, alerts, and affected users etc. Security analysts can conduct specific analysis based on cases to assess the possibilities of threats. These cases contain essential details like titles, tags, rules for tasks and observables, incident descriptions, and information about impacted users. They serve as a structured framework for security analysts to investigate threats systematically and derive actionable insights for threat mitigation.

Case	Status	Title	Severity	Tasks	Observables	TTPs	Assigned To	Created On	Last Updated On
template task for demo	New	template task for demo	Low	2	0	0	S	S. 24/08/2023 11:33	C. 24/08/2023 11:33
test 1	False positive	test 1	Low	1	3	2	T	S. 24/08/2023 10:36	C. 24/08/2023 10:36

Figure 6.1: Example of Cases

6.2 Case Creation

The first thing comes in this feature that an organization admin can create cases. The page header contains a button named **CREATE CASE +**



Figure 6.2: Create Case Button

If we click on the button, a new dialog window will appear

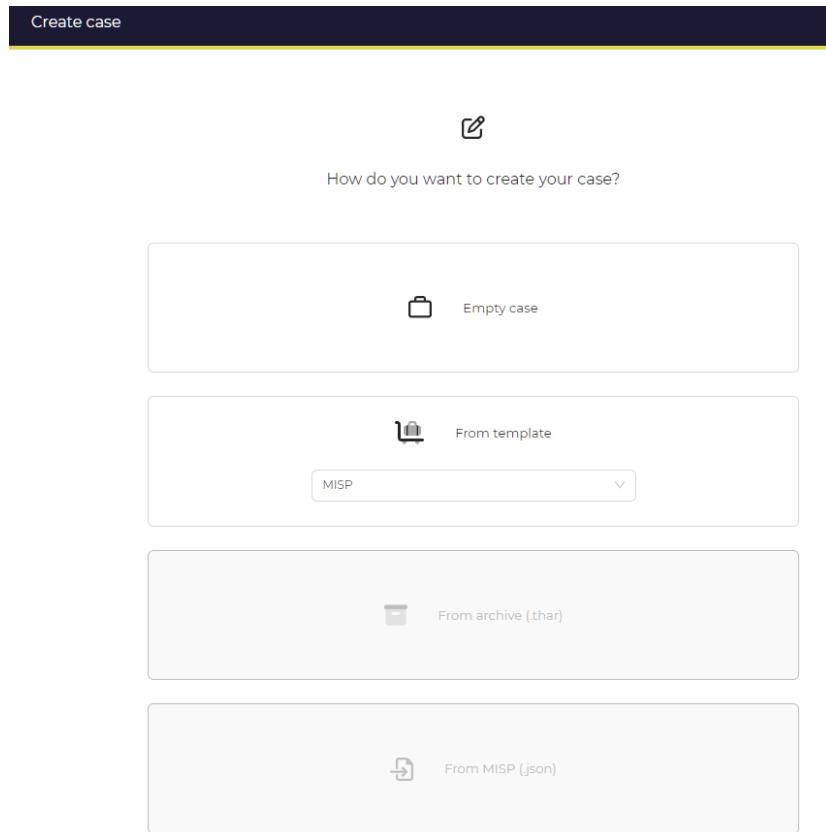


Figure 6.3: Create Case Tab View

6.2.1 Empty Case Creation

An empty case can be created by entering relevant details in the provided fields.

The screenshot shows a 'Create case' dialog box with the following fields:

- Title:** A text input field labeled 'Case title...'.
- Date:** A date input field showing '2023-08-31'.
- Severity:** A horizontal row of four buttons: 'LOW' (gray), 'MEDIUM' (orange), 'HIGH' (gray), and 'CRITICAL' (gray).
- TLP:** A horizontal row of five buttons: 'TLP:CLEAR' (gray), 'TLP:GREEN' (gray), 'TLP:AMBER' (orange), 'TLP:AMBER+STRICT' (gray), and 'TLP:RED' (gray).
- PAP:** A horizontal row of four buttons: 'PAP:CLEAR' (gray), 'PAP:GREEN' (gray), 'PAP:AMBER' (orange), and 'PAP:RED' (gray).
- Tags:** A text input field labeled 'Tags'.
- Description:** A rich text editor with a toolbar containing icons for bold, italic, underline, etc., and a preview button.

At the bottom right are 'Cancel' and 'Confirm' buttons.

Figure 6.4: Create Empty Case

6.2.2 Case Creation from MISP template

We can also create a new case from builtin MISP template where few tasks, observables and some other routines already added to make things easy.

The screenshot shows the 'Create case from template: MISP' dialog box. It includes fields for Title (Case title...), Date (2023-08-31), Severity (MEDIUM selected), TLP (TLP:AMBER selected), PAP (PAP:AMBER selected), Tags (hunting), and a Description rich text area (Check if IOCs shared by the community have been seen on the network). Below the dialog, a table lists three tasks: 'default - Search for IOCs on Mail gateway logs', 'default - Search for IOCs on Firewall logs', and 'default - Search for IOCs on Web proxy logs', each with Edit and Delete links.

Tasks	Custom fields	Pages	Add a task
default - Search for IOCs on Mail gateway logs			Edit Delete
default - Search for IOCs on Firewall logs			Edit Delete
default - Search for IOCs on Web proxy logs			Edit Delete

Figure 6.5: Create Case from MISP

6.2.3 Case Creation from EDR template

An Endpoint Detection and Response (EDR) is a key part of endpoint protection strategy and can help analysts investigate and respond to attacks as they happen. We can make such a case from the already given EDR template

Create case from template: Worm infection (CERT-SC IRM1)

Title
EDR Worm infection

Date
2023-06-26

Severity
LOW MEDIUM HIGH CRITICAL

TLP
TLP:CLEAR TLP:GREEN TLP:AMBER TLP:AMBER+STRICT TLP:RED

PAP
PAP:CLEAR PAP:GREEN PAP:AMBER PAP:RED

Tags
CERT-XLM:malicious-code="worm"

Description
Worm infection

Tasks

Preparation - Preparation	Edit	Delete
Identification - Detect the infection	Edit	Delete
Identification - Identify the infection	Edit	Delete
Containment - Containment	Edit	Delete
Containment - Mobile devices	Edit	Delete
Remediation - Identify	Edit	Delete
Remediation - Test	Edit	Delete
Remediation - Deploy	Edit	Delete
Remediation - Recovery	Edit	Delete
Aftermatch - Report	Edit	Delete
Aftermatch - Capitalize	Edit	Delete

Add a task

Confirm

Figure 6.6: Create Case from EDR

6.2.4 Case Creation from Phishing template

Phishing templates let the analyst think in a attacker's way. So, creation of such cases from attacker's perspective sometimes give analysts a great advantage in analysis and study.

Create case from template: Smishing infection

* Title
Phishing SMS fraud

* Date
2023-06-26

Severity
LOW MEDIUM HIGH CRITICAL

TLP
TLP:CLEAR TLP:GREEN TLP:AMBER TLP:AMBER+STRICT TLP:RED

PAP
PAP:CLEAR PAP:GREEN PAP:AMBER PAP:RED

Tags
CERT-XLM:fraud="phishing"

* Description
Smishing infection

Tasks

Task	Action
Preparation - Preparation	Edit Delete
Identification - Detect the infection	Edit Delete
Identification - Identify the infection	Edit Delete
Containment - Containment	Edit Delete
Containment - Mobile devices	Edit Delete
Remediation - Identify	Edit Delete
Remediation - Test	Edit Delete
Remediation - Deploy	Edit Delete
Remediation - Recovery	Edit Delete
Aftermatch - Report	Edit Delete
Aftermatch - Capitalize	Edit Delete

Add a task

Cancel Confirm

Figure 6.7: Create Case from Phishing Template

6.2.5 Apply Case template

Additionally, we can also manually apply any templates to any cases.

Apply case template X

* Select case template
MISP

Merge tags hunting

Merge custom fields

Import tasks Select all Deselect all

Filter tasks...

⊖ default - Search for IOCs on Mail gateway logs Run queries in Mail gateway logs and look for IO...
⊖ default - Search for IOCs on Firewall logs Run queries in firewall logs and look for IOcs of type IP,...
⊖ default - Search for IOCs on Web proxy logs Run queries in web proxy logs and look for IOcs of t...

Add description
Check if IOCs shared by the community have been seen on the network

Apply severity SEV:MEDIUM

Apply TLP

Cancel Confirm

Figure 6.8: Apply template to case

6.3 Addition to a Case

We can select various tags from the taxonomy and also custom field values(e.g: location/business-unit/detection-source/test) according to the necessity of cases

The screenshot shows a user interface for selecting tags. At the top, a dark header bar says "Select tags from library" and has a close button. Below it, a section titled "Selected tags: (1)" shows a single tag: "circ:incident-classification='phishing'" with a delete icon. A "Clear selection" link is to the right. Below this, a section titled "Choose tags from taxonomy: circl" shows a list of taxonomy terms. One term, "circ:incident-classification='phishing'", is highlighted with a red box and has a question mark icon next to it. Other terms listed include "circ:topic='individual'", "circ:incident-classification='system-compromise'", "circ:incident-classification='screenlocker'", "circ:incident-classification='sabotage'", "circ:incident-classification='sql-injection'", "circ:incident-classification='covid-19'", and "circ:topic='finance'". A "Filter tags..." input field is above the list. At the bottom of this section is a blue "Add selected tags" button with a red box around it. The final section at the bottom is titled "Adding a Custom Field Value" with a "Name" field containing a placeholder "Choose a type...".

Figure 6.9: Addition of tags and custom field value on cases

6.4 Details of a Case

Clicking on a case preview shows the detailed preview about it and clicking on the case opens the detailed view of a case

The screenshot shows a detailed view of a case named "Case #2". At the top, there are fields for TLP (TLP:AMBER), Assignee (thehive), Start date (2023-08-24), End date (None), Tasks (2), Observables (0), and TTPs (0). Below these, the "Title" field contains "template task for demo". The "Status" is set to "New". Under "Tags", there is a single tag "hunting". The "Description" field contains the text "Check if IOCs shared by the community have been seen on the network". In the "Custom Fields" section, there is one entry labeled "default (1)". The "Hits" section has an "Add" button and a placeholder "Enter a value...". At the bottom, there is an "Actions" dropdown and a blue "Go to details" button.

Figure 6.10: Case Preview

6.4.1 Left Side View

The left side pane shows general information about the case. When it was created, its source, its severity, TLP (Traffic Light Protocol) and PAP(Permissible Actions Protocol). It also contains a field called Assignee to assign any user on handling the case.

#2 template task for demo

⌚ id ~20528
👤 Created by thehive
📅 Created at 24/08/2023 11:33

Severity: MEDIUM

TLP: AMBER PAP: AMBER

Assignee
thehive

Status
New

Start date
2023-08-24

Tasks completion

Contributors

Time to detect
37 seconds

Figure 6.11: Left Side Pane of Case Details

6.4.2 TLP and PAP

The detailed description about TLP(Traffic Lighting Protocol) and PAP(Permissible Access Protocol) explained in Alerts section TLP and PAP

6.4.3 General Tab

The details of the case summarized in this view which holds the middle view of the page

The screenshot shows the 'General' tab selected in a case details interface. The top navigation bar includes links for Tasks (2), Observables (0), TTPs (0), Attachments, and Timeliner. The main content area contains the following fields:

- Title:** template task for demo
- Tags:** hunting
- Description:** Check if IOCs shared by the community have been seen on the network
- Custom Fields:** A section showing 'default (1)' with a dropdown menu set to '3'. An 'Add' button is available.
- Hits:** A section with an 'Add' button and a field labeled 'Enter a value...' with a red trash icon.

Figure 6.12: Case Details

6.4.4 Tasks Tab

The details of this section fully explained in Chapter Tasks

The screenshot shows the 'Tasks' tab within a software application. At the top, there are tabs for General, Tasks (2), Observables (0), TTPs (0), Attachments, Timeline, Pages, and History. Below the tabs are buttons for '+', 'default', 'Quick Filters', 'Export list', and three toggle switches. The main area displays two tasks in a table:

Task	Activity	Assignee	Dates
default Search for IOCs on Mail gateway logs Closed 7 days ago	Activity	S. 24/08/2023 11:35 C. 24/08/2023 11:33 U. 24/08/2023 11:35	...
default Search for IOCs on Web proxy logs	Activity	C. 24/08/2023 11:33	...

A modal window titled 'Task preview' is open for the first task. It contains the following details:

- Title:** Search for IOCs on Mail gateway logs
- Flag:** On
- Status:** Completed
- Group:** default
- Assignee:** (empty)
- Start date:** 2023-08-24 11:35:08
- End date:** 2023-08-24 11:35:08
- Mandatory:** Off
- Description:** Run queries in Mail gateway logs and look for IOCs of type IP, email addresses, hostnames, free text.
- Activity:** Show 10 (with a '+' button)
- No task logs have been found. [Create a Task Log](#)
- Responder Reports:** (empty)

At the bottom of the modal are 'Actions' and 'Go to details' buttons.

Figure 6.13: Task view on cases

6.4.5 Observables Tab

The details of this section fully explained in section Observables of chapter Alerts

FLAGS	DATA TYPE	VALUE/Filename	DATES
TLP:AMBER PAP:AMBER	ip	127.0.0.1:2222	S. 24/08/2023 19:50 C. 24/08/2023 19:50
TLP:GREEN PAP:GREEN	ip	127.0.0.1:8888	S. 24/08/2023 10:58 C. 24/08/2023 10:58
TLP:AMBER PAP:CLEAR	ip	localhost:8888	S. 24/08/2023 10:51 C. 24/08/2023 10:51

Observable preview

Id ~4136 Created by thehive Created at 24/08/2023 19:50

Tags
Tags

Reports
CCT:C2 Search=0 hits

Description
Not specified

ANALYZER	LAST ANALYSIS
Abuse_Finder_3_0	No Data
CyberCrime-Tracker_1_0	✓ 24/08/2023 19:50
DShield_lookup_1_0	No Data
GoogleDNS_resolve_1_0_0	No Data
Maliverse_Report_1_0	No Data
MaxMind_GeoIP_4_0	No Data
TalosReputation_1_0	No Data
Threatcrowd_1_0	No Data
URLhaus_2_0	No Data

Figure 6.14: Observables and Analyzers view on cases

6.4.6 TTPs

TTPs(Tactics, Techniques and Procedures) are patterns of activities or methods associated with a threat or attack!. These are included in the TTPs tab if any found.

Figure 6.15: TTPs Preview and Details

Operations

We can add new TTPs and even can delete them as needed

Figure 6.16: TTPs Addition and Deletion

6.4.7 Attachments Tab

We can also add relevant attachments which may be based on any tasks, new reports etc

FILENAME	TYPE	SIZE	DATE	...
description.txt	text/plain	144 KB	24/08/2023 10:48	[...] button

Figure 6.17: Attachment to cases

6.4.8 History

This tab contains history of all activities, modifications or actions taken regarding this case.

DATES	ACTION	FIELD	USER
24/08/2023 11:10	Update	4 changes endDate, status, stage, summary	[User icon]
24/08/2023 11:04	Update	1 change customFields	[User icon]
24/08/2023 10:48	Update	2 changes status, stage	[User icon]
24/08/2023 10:36	Create	24 changes _id, _type, _createdBy, _createdAt, number, title, description, severity, severityLabel, startDate, tags, flag, tlp, tlpLabel, pap, papLabel, status, stage, assignee, customFields, userPermissions, extraData, newDate, timeToDetect	[User icon]
24/08/2023 10:36	Update	1 change share	[User icon]

Figure 6.18: History of a case

6.5 Other Actions on A Case

There are some other actions which can also be done on cases.

6.5.1 Statistics

We can view the statistics by enabling the stats toggle button



Figure 6.19: Case Statistics

6.5.2 Filtering and Sorting

We can add manual sort or filtering options to cases to preview accordingly

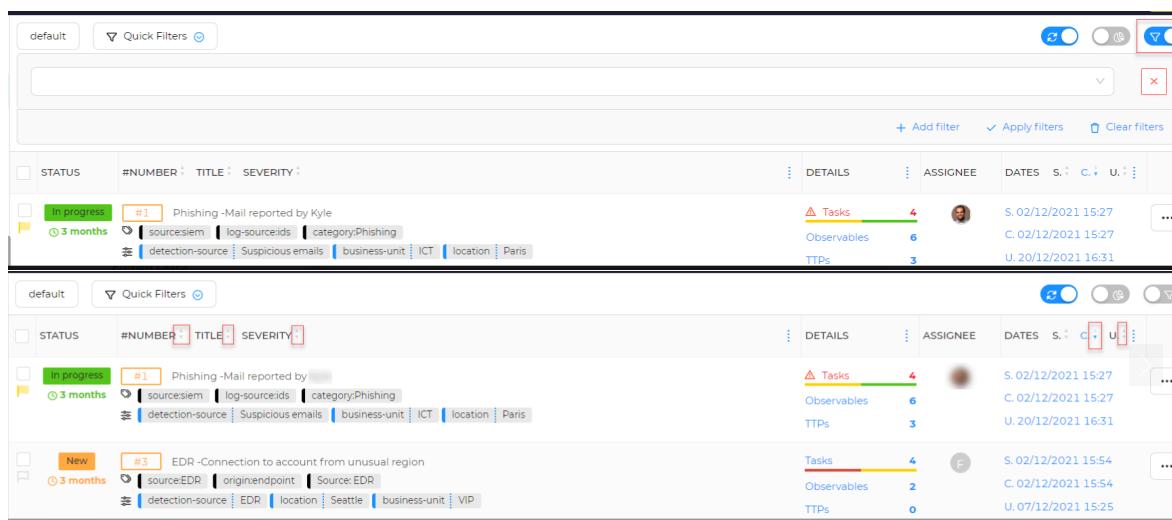


Figure 6.20: Case Filtering and Sorting

6.5.3 Flag a Case

We can click on flag/unflag option to flag or unflag any case

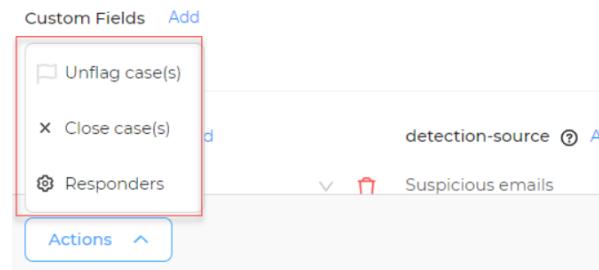


Figure 6.21: Case Flagging

6.5.4 Close a Case

Finally, we can close a case after all actions have been done or there is nothing new to do or observe. Here we can set a status(for e.g: False Positive) saying about the final verdict of that specific closed case

A screenshot of a "Close case #1" dialog box. It contains a warning message: "This case contains the following open or unassigned tasks. Closing the case will permanently remove the unassigned ones. This action cannot be undone." Below this is a table with columns "Task", "Date", and "Assignee". It shows two entries: "default Analysis" (date 02/12/2021 15:27, assignee F) and "default Remediation" (date 02/12/2021 15:27, assignee F). Both entries have a note "(Started 3 months ago)". Below the table are sections for "Status *" (set to "InProgress") and "Summary *". The summary area includes a rich text editor toolbar and a "Preview" button. At the bottom are "Cancel" and "Close tasks and Case" buttons, with "Close tasks and Case" highlighted by a red box.

Figure 6.22: Closing cases

Chapter 7

Analyst Features : Alerts

7.1 Introduction

The alert tab provides information about current security issues, vulnerabilities, and exploits in a timely manner. These alerts are collected from various MISP (Malware Information Sharing Platform) instances.

A screenshot of a web-based alert interface. The top navigation bar includes 'SEVERITY' (Low), 'STATUS' (New), 'TITLE' (CISA.gov - AA21-062A Mitigate Microsoft Exchange Server Vulnerabilities), '# CASE' (1), 'TYPE' (misp), 'SOURCE' (misp server), 'REFERENCE' (None), 'DETAILS' (Observables: 6, TTPs: 0, ID: 1311), 'ASSIGNEE' (None), and 'DATES' (O. 13/07/2023 12:55, C. 13/07/2023 12:55, U. 13/07/2023 12:55). The alert card itself shows 'tip:pwhite' and 'osint:lifetime="perpetual"' tags.

Figure 7.1: An Example of An Alert

7.2 Details of an alert

Clicking on an alert shows more details about it.

A detailed view of an alert titled 'CISA.gov - AA21-062A Mitigate Microsoft Exchange Server Vulnerabilities'. The left sidebar lists alert metadata: id (~3211296), created by 'thehive' at '13/07/2023 12:55', severity 'LOW', and source 'misp server'. The right panel displays alert details under tabs: General, Observables (6), TTPs (0), Similar Cases, Similar Alerts, Responders, and History. The General tab shows tags 'tip:pwhite', 'type:OSINT', and 'osint:lifetime="perpetual"', a description 'Imported from MISP Event #1311.', a summary 'Not specified', and a 'Custom Fields' section with 'default (1)'. The Hits section is empty. The status is 'New'.

Figure 7.2: An Example of An Alert

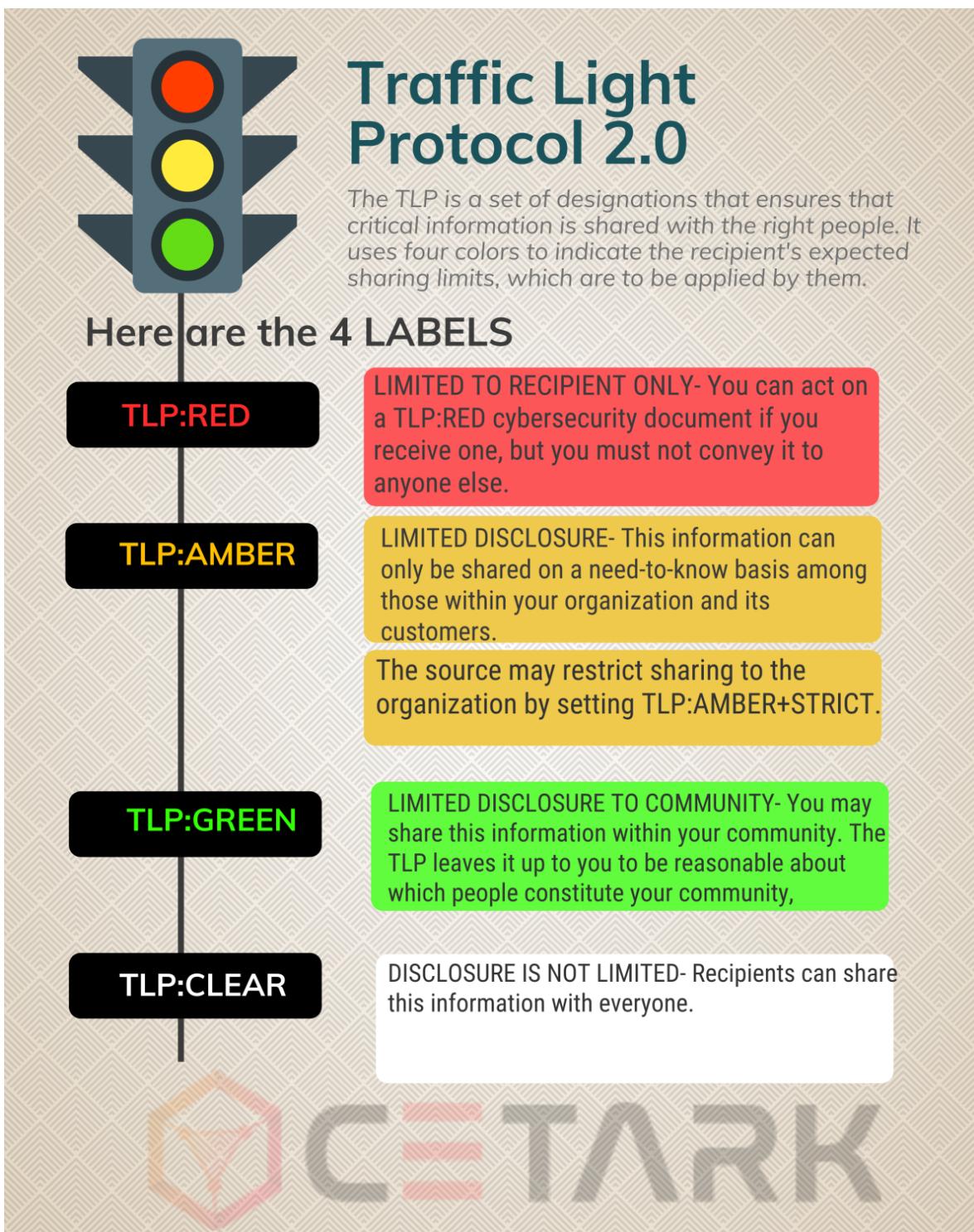
7.2.1 Left Side View

The left side pane shows general information about the alert. When it was created, its source, its severity, TLP (Traffic Light Protocol) and PAP(Permissible Actions Protocol). Details about TLP and PAP are given in the figure 7.4 and 7.5 respectively. It also contains a field called Assignee to assign any user on handling the alert.

The screenshot shows a left-side pane with various alert details:

- General Information:**
 - id**: ~3211296
 - Created by**: thehive
 - Created at**: 13/07/2023 12:55
- Severity:** SEVERITY:LOW
- TLP:** TLP:CLEAR (highlighted in black)
- PAP:** PAP:AMBER (highlighted in orange)
- Assignee:** thehive (represented by a user icon)
- Source:** misp server
- Reference:** 1311
- Type:** misp
- Occurred date:** 2023-07-13 12:55:26
- Status:** New (indicated by a red dot)

Figure 7.3: Left Side Pane of Alert Details



Source: <https://www.linkedin.com/pulse/new-improved-traffic-light-protocol-20-cybersecurity-cetarkcorp>

Figure 7.4: TLP

RED**PAP:RED**

(PAP:RED) Non-detectable actions only. Recipients may not use PAP:RED information on the network. Only passive actions on logs, that are not detectable from the outside.

AMBER**PAP:AMBER**

(PAP:AMBER) Passive cross check. Recipients may use PAP:AMBER information for conducting online checks, like using services provided by third parties (e.g. VirusTotal), or set up a monitoring honeypot.

GREEN**PAP:GREEN**

(PAP:GREEN) Active actions allowed. Recipients may use PAP:GREEN information to ping the target, block incoming/outgoing traffic from/to the target or specifically configure honeypots to interact with the target.

WHITE**PAP:WHITE**

(PAP:WHITE) No restrictions in using this information.

Source: <https://www.misp-project.org/taxonomies.html>

Figure 7.5: PAP

7.2.2 General Tab

Contains tags, description and summary of the alert. Allows addition of custom fields

General Observables (6) TTPs (0) Similar Cases Similar Alerts Responders History

Tags

- tip:pwhite
- type:OSINT
- osint:lifetime="perpetual"

Description

Imported from MISP Event #1311.

Summary

Not specified

Figure 7.6: General Tab



Figure 7.7: Adding custom field in general tab

7.2.3 Observables Tab

Shows list of observables related to an alert. Observables are metadata that are linked to alerts that are affecting a network, for example, an ip address that triggered a firewall rule,

FLAG	DATA TYPE	VALUE/FILENAME	DESCRIPTION	DATES
TLP:CLEAR PAP:AMBER	hash	2b6f1ebb200e93ade4a6424555d6a8341fd69f60c25e44afe11008f5ciaad1	Cybersecurity and Infrastructure Security (CISA) partners have observed active exploitation of vulnerabilities in Microsoft Exchange Server products. Successful exploitation of these vulnerabilities allows an unauthenticated attacker to execute arbitrary code on vulnerable Exchange Servers, enabling the attacker to gain persistent system access, as well as access to files and mailboxes on the server and to credentials stored on that system. Successful exploitation may additionally enable the attacker to compromise trust and identity in a vulnerable network. Microsoft released out-of-band patches to address vulnerabilities in Microsoft Exchange Server. The vulnerabilities impact on-premises Microsoft Exchange Servers and are not known to impact Exchange Online or Microsoft 365 (formerly O365) cloud email services. This Alert includes both tactics, techniques and procedures (TTPs) and the indicators of compromise (IOCs) associated with this malicious activity. To secure against this threat, CISA recommends organizations examine their systems for the TTPs and use the IOCs to detect any malicious activity. If an organization discovers exploitation activity, they should assume network identity compromise and follow incident response procedures. If an organization finds no activity, they should apply available patches immediately and implement the mitigations in this Alert.	S. 13/07/2023 12:55 C. 13/07/2023 12:55
TLP:CLEAR PAP:AMBER	IP	211[.]56[.]98[.]146		S. 13/07/2023 12:55 C. 13/07/2023 12:55
TLP:CLEAR PAP:AMBER	other	65149e036fff06026d80ac9ad4d156332822dc93142cf1a122b1841ec8de34b5		S. 13/07/2023 12:55 C. 13/07/2023 12:55
TLP:CLEAR PAP:AMBER	IP	5[.]2[.]69[.]14		S. 13/07/2023 12:55 C. 13/07/2023 12:55
TLP:CLEAR PAP:AMBER	IP	5[.]254[.]43[.]18		S. 13/07/2023 12:55 C. 13/07/2023 12:55

Figure 7.8: Observables Tab

We can click on an observable to view its details

Figure 7.9: Details on an observable

In the details view, we can set the TLP, PAP level of the observable. We can also mark it as an IOC (Indicators of Compromise). Here we can also view the report of any analyzers that have been run on this observable. For example, the URLhaus analyzer was run on the observable shown in 7.9 and its result is shown in 7.10

```
{
  "query_status": "no_results",
  "data_type": "hash"
}
```

Figure 7.10: Report of an analysis

The continuation of figure 7.9 is shown in 7.11

ANALYZER	LAST ANALYSIS
Maltiverse_Report_1_0	27/08/2023 16:40
TeamCymruMHR_1_0	No Data
URLhaus_2_0	27/08/2023 17:13
Urlscan_io_Search_0_1_1	No Data

Figure 7.11: Run analyzer on observables

The figure 7.11 shows that we can run analyzers on the observables. These analyzers are various Threat Intelligence Feed Providers. They gather intelligence on various security threats and can be queried for intelligence on the observables. For example, given an ip, a provider may inform us if the ip has been associated with threats or attacks in any other place. Or given a hash of a suspicious file, a provider may tell us if it is infected with some malwares seen till now.

7.2.4 TTPs

TTPs(Tactics, Techniques and Procedures) are patterns of activities or methods associated with a threat or attack. These are included in the TTPs tab if any found.

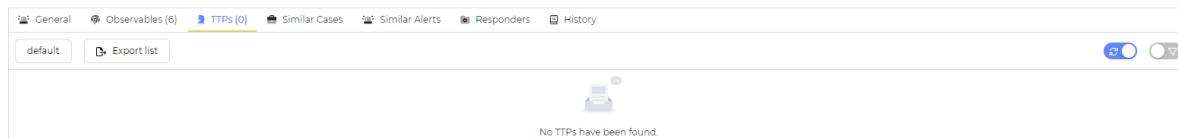


Figure 7.12: TTPs Tab

7.2.5 Similar Cases

This tab contains similar cases if any found

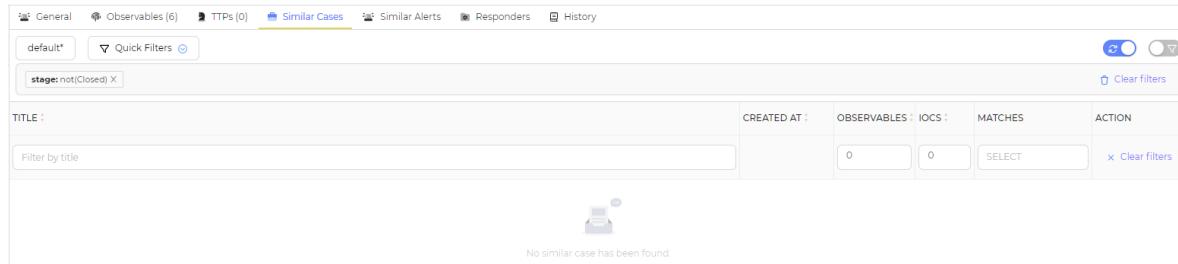


Figure 7.13: Similar Cases Tab

7.2.6 Similar Alerts

This tab contains similar alerts if any found

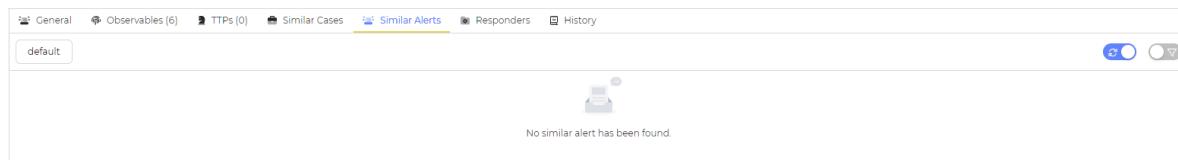


Figure 7.14: Similar Alerts Tab

7.2.7 Responders

This tab contains reports from responders if any available

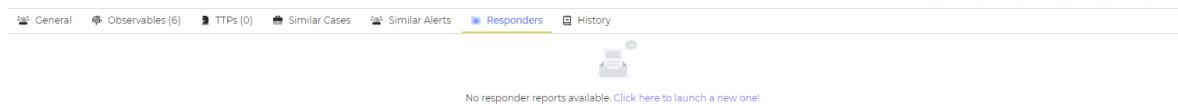


Figure 7.15: Responders Tab

7.2.8 History

This tab contains history of all activities, modifications or actions taken regarding this alert. For example, the figure 7.16 shows that an user has been assigned on the alert.

The screenshot shows the 'History' tab of an alert. At the top, there are tabs for General, Observables (6), TTPs (0), Similar Cases, Similar Alerts, Responders, and History. The History tab is selected. A search bar contains the query 'operation: any(update) X'. Below the search bar, there are filters for DATES, ACTION, FIELD, and USER. A single update entry is listed: '27/08/2023 13:02' under DATES, 'Update' under ACTION, '1 change assignee' under FIELD, and 'USER' under USER. There is also a small circular icon with a 'T'.

Figure 7.16: History Tab

7.3 Actions on An Alert

Actions on alerts are available in 2 places in the GUI as shown in 7.18 and 7.18

The screenshot shows the 'Details' view of an alert. At the top, there are tabs for General, Observables (6), TTPs (0), Similar Cases, Similar Alerts, Responders, and History. The General tab is selected. A search bar contains the query 'tip:pwhite type:OSINT osint:lifetime="perpetual"'. On the right side, there is a 'Comments' section with a text input field and a small icon. At the top right, there is a red-bordered actions menu with icons for copy, cut, paste, refresh, and delete.

Figure 7.17: Actions Menu in Details View

The screenshot shows the 'Alert preview' screen. At the top, it displays basic information: id ~3211296, Created by thehive, Created at 13/07/2023 12:55, Last reviewed by thehive, and Last reviewed at 27/08/2023 13:02. Below this, there are sections for TLP levels (TLP:CLEAR, PAP:AMBER, SEV:LOW), Type (misp), Source (misp server), Reference (1311), and Occurred date (2023-07-13 12:55:26). To the right, there are counts for Observables (6), TTPs (0), Similar Alerts (0), and Similar Cases (0). The main body of the preview includes fields for Title (CISA.gov - AA21-062A Mitigate Microsoft Exchange Server Vulnerabilities), Assignee (thehive), Tags (tip:pwhite type:OSINT osint:lifetime="perpetual"), Description (Imported from MISP Event #1311.), Status (New), and Summary. A large red box highlights the 'Actions' dropdown menu on the right, which contains options: Start, Close, Ignore new updates, New case from selection, Merge selection into case, and Responders. At the bottom right is a 'Go to details' button.

Figure 7.18: Actions Menu in Preview

Available actions are discussed below

7.3.1 Start

We can start alert with in progress or pending status as shown in 7.19. We can also assign users to this alert.

The screenshot shows a user interface for starting an alert. At the top, there is a field labeled "Status" with a dropdown menu showing "In Progress". Below this is a "Summary" section containing a rich text editor toolbar and a "Preview" button. Underneath is an "Assignee" section with a dropdown menu showing "thehive".

Figure 7.19: Start Alert

7.3.2 Close

This closes an alert

7.3.3 Ignore New Updates

The updates of the alert are not notified.

7.3.4 New Case from Selection

Create new case from this alert.

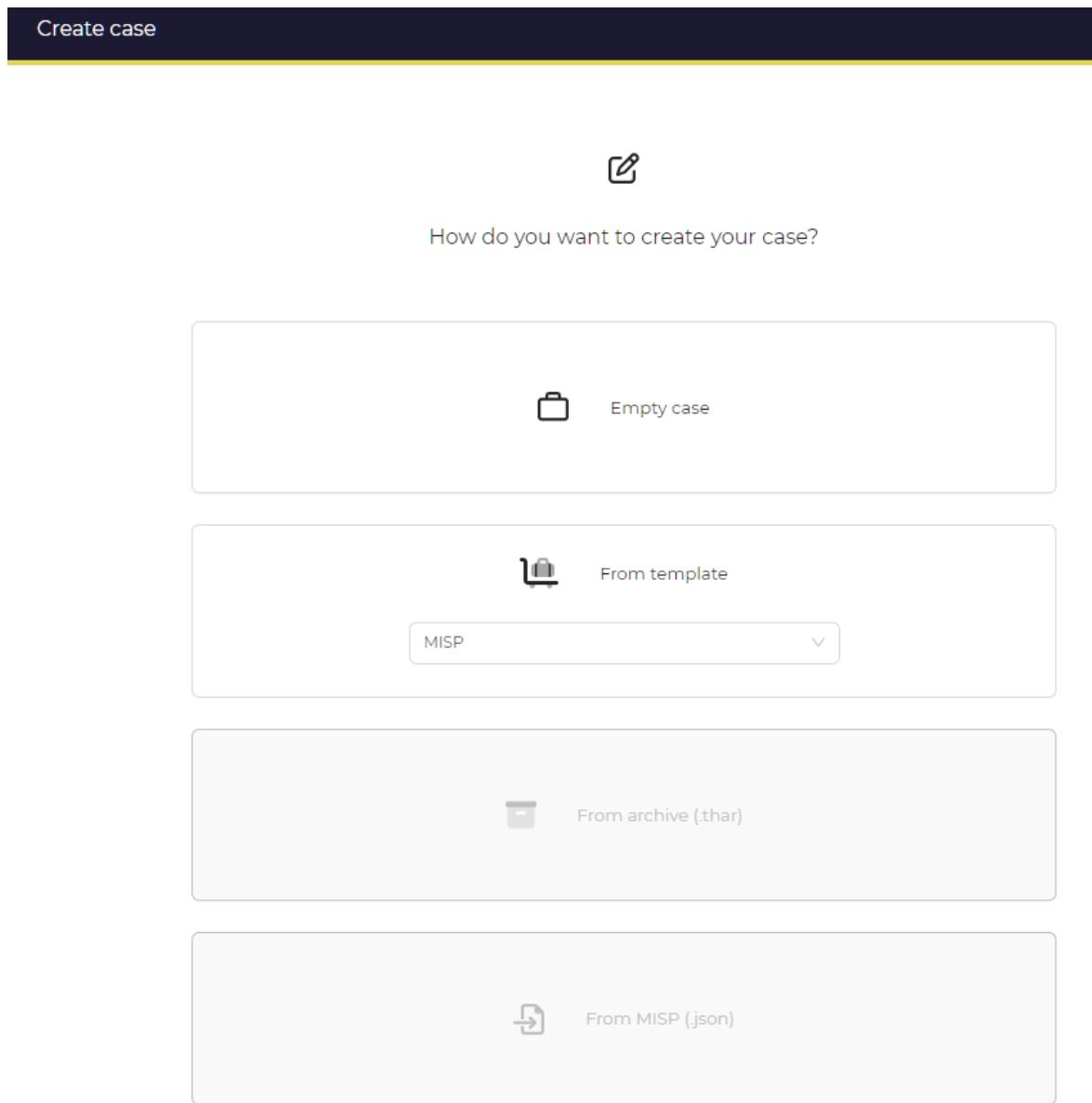


Figure 7.20: Create Case From Alert

Choosing empty case takes to 7.21

Create case

* Title
CISA.gov - AA21-062A Mitigate Microsoft Exchange Server Vulnerabilities

* Date
2023-08-27

Severity
LOW MEDIUM HIGH CRITICAL

TLP
TLP:CLEAR TLP:GREEN TLP:AMBER TLP:AMBER+STRICT TLP:RED

PAP
PAP:CLEAR PAP:GREEN PAP:AMBER PAP:RED

Tags
| tlp:pwhite | type:OSINT | osint:lifetime="perpetual"

* Description

Imported from MISP Event #1311.

[Tasks](#) [Custom fields](#) [Pages](#) [Add a task](#)

No tasks have been found. [Add a task](#)

[Cancel](#) [Confirm](#)

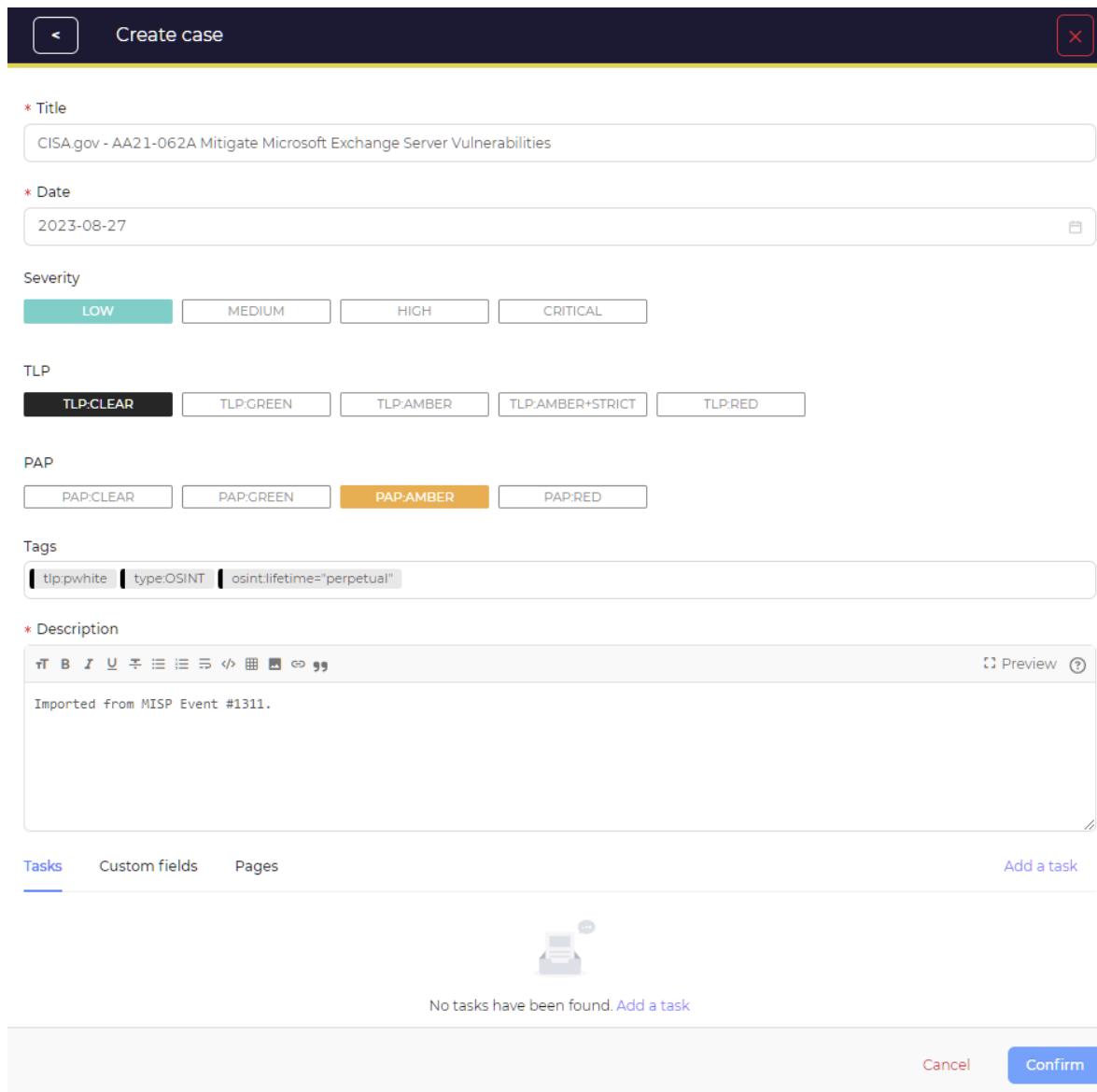


Figure 7.21: Create Empty Case From Alert

7.3.5 Merge selection into case

Merge alert into an existing case

7.3.6 Responders

Similar to responders tab in details view

Chapter 8

Analyst Features : Tasks

8.1 Introduction

Tasks are basically stuff that need to be done to handle a case.

8.2 Creating a task

Tasks are created under a case, from the task tab in the details view of a case.

The screenshot shows the 'Tasks' tab selected within a 'Cases / #1 / Tasks' interface. The top navigation bar includes links for General, Tasks (0), Observables (6), TTPs (0), Attachments, Timeline, Pages, and History. A search bar at the top right allows entering a case number. Below the tabs, there's a summary row with fields for ID (#1), Created by (thehive), and Creation date (27/08/2023 19:56). Buttons for '+', 'default', 'Quick Filters', and 'Export list' are present. On the left, a sidebar shows severity levels (SEVERITYLOW, TLP:CLEAR, PAP:AMBER) and a note indicating no tasks have been found. A small icon of a person with a speech bubble is visible on the right.

Figure 8.1: Creating Task

Clicking on the plus icon show 8.2 on the right.

Adding a Task X

* Group
default

* Title
Examine IP

Mandatory
 At least one log must be present

Description

Suspicious activity from ip 8.8.8.8. Examine if it is malicious

Assignee
 Demo

Flag this task?

Due date
2023-08-31 17:39:03

[Cancel](#) [Save and add another](#) [Confirm](#)

Figure 8.2: Creating Task

We can assign the task to a user from the assignee drop down as shown in 8.3. Here we are creating a task to examine an ip from which suspicious activities were detected.

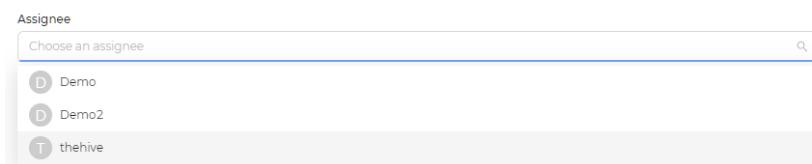


Figure 8.3: Creating Task

8.3 Viewing Tasks

The task tab in case details view enlists all the tasks created for the particular case.

The screenshot shows a task list interface. At the top, there are tabs for General, Tasks (1), Observables (6), TTPs (0), Attachments, Timeline, Pages, History, and Related alerts. Below the tabs, there are buttons for 'default', 'Quick Filters', and 'Export list'. A search bar is present above the main list. The main list displays one task: 'TASK: ORDER *' with the title 'Examine IP'. To the right of the task, there are columns for DETAILS, ASSIGNEE, and DATES. The task details show 'Activity' (empty), 'ASSIGNEE' (empty), and 'DATES' (C. 28/08/2023 17:44). A red star icon is visible next to the task title.

Figure 8.4: Task List

Clicking on a task shows its details

The screenshot shows the details of the 'Examine IP' task. At the top, there are tabs for General, Tasks (1), Observables (6), TTPs (0), Attachments, Timeline, Pages, History, and Related alerts. Below the tabs, there is a message: 'This task requires an activity to be completed'. The task details include: Title (Examine IP), Flag (off), Status (Waiting), Group (default), Assignee (Demo), Start date (Select date), Due date (2023-08-31 17:39:03), Mandatory (on), Description (Suspicious activity from ip 8.8.8.8. Examine if it is malicious), and Activity (empty). A red box highlights the 'Activity' section. At the bottom, there is a message: 'No task logs have been found. Create a Task Log'.

Figure 8.5: Details of a Task

8.4 Actions on a Task

Action on tasks can be initiated from the task details view or task list view.

The screenshot shows the details of the 'Examine IP' task with the actions menu open. The menu options are: Start (radio button selected), Delete, Flag, and Responders. A red box highlights the 'Start' option.

Figure 8.6: Actions Menu of Task (In task details)

The screenshot shows the task list interface with the actions menu open for the 'Examine IP' task. The menu options are: Start (radio button selected), Delete, Flag, Pin, and Responders. A red box highlights the 'Start' option.

Figure 8.7: Actions Menu of Task (In task list)

Available actions are start, delete, flag, pin etc.

8.5 Adding Activities

Users who have conducted some work or investigation on a task can give updates about their findings by adding activity. This is available in the details view of a task, visible in the bottom part of 8.5. For example, a report generated by running analysis tool on an ip address maybe included as an activity in the activity section of the task shown in 8.5

The screenshot shows a modal dialog titled "Create a Task Log". At the top left is a red asterisk icon followed by the word "Log". On the right is a close button (an "X"). Below the title is a rich text editor toolbar with icons for bold, italic, underline, etc. To the right of the toolbar is a "Preview" button and a help icon. The main content area contains the text "report generated on ip using analyzers". Below this is a section labeled "Include in timeline" with a toggle switch that is turned off. Under "Attachment", there is a dashed box with the placeholder "Drop file or click" and a file named "report.json" attached. At the bottom of the dialog are three buttons: "Cancel", "Save and close the task" (disabled), and a blue "Confirm" button.

Figure 8.8: Adding Activity

The added activity, with attached files is shown in the activity section of details view of a task

Activity (1)		+	Show 10
thehive	28/08/2023 19:09		
report generated on ip using analyzers			
@ report.json			
		🔗	⊕

Figure 8.9: Activity List

Chapter 9

Analyst Features : Dashboard

9.1 Introduction

The dashboard comprehensively presents case details, encompassing status, title, version, widgets, creator, creation dates, and update dates. Users can leverage filters to refine displayed content, implement sorting based on specific attributes, and effectively manage different viewing arrangements.

The screenshot shows a user interface for managing dashboards. At the top, there is a search bar with the placeholder "status: any(Shared) X" and a "Clear filters" button. Below the search bar, there is a toolbar with a "+" icon, "Import Dashboard", and "default*". On the left, there is a sidebar with links for "Cases", "Alerts", "Tasks", "Dashboards" (which is selected and highlighted in blue), "Search", and "Organisation". The main area displays a table of dashboards. The columns are: STATUS, NAME, VERSION, # WIDGET, OWNER, DATES, C., and U. The data in the table is as follows:

STATUS	NAME	VERSION	# WIDGET	OWNER	DATES	C.	U.
Shared	Alerts statistics	1	8	A	C. 13/07/2023 12:55		
Shared	Cases statistics	1	9	A	C. 13/07/2023 12:55		
Shared	Observables statistics	1	6	A	C. 13/07/2023 12:55		
Shared	TTPs statistics	1	2	A	C. 13/07/2023 12:55		

Figure 9.1: Dashboards

9.2 Add a Dashboard

Clicking on the + icon on the upper side will pop a new dashboard window.

Create a new dashboard X

* Group
default

* Title
CSE 406 Demo

* Description
tests

* Visibility
 Private Shared

Cancel Confirm

Figure 9.2: Add New Dashboard

9.3 Import Dashboard

We can import any pre-configured json format dashboard from our local machine. This json file mainly generated from the exported file of the hive project

The screenshot shows a web-based form titled "Import a dashboard". At the top, there is a message: "You can use the exported dashboard directly from TheHive platform". Below this is a section labeled "Attachment" with a placeholder box containing the text "Drop file or click". A note below the box states "The attachment must be a valid JSON file". The main form area has a dark header with the text "Import a dashboard" and a red "X" button. The form fields include:

- * Group:** A dropdown menu set to "default".
- * Title:** A text input field containing "Alerts statistics".
- * Description:** A text input field containing "Alerts statistics".
- * Visibility:** A radio button group where "Shared" is selected.

At the bottom right of the form are "Cancel" and "Confirm" buttons.

Figure 9.3: Import Dashboard

9.4 Other Actions of Dashboard

We can edit or duplicate already created dashboards. Besides, any old dashboard can be deleted. Lastly, we can export dashboard in json format which can be shared later.

9.4.1 Edit, Delete, Duplicate and Export Dashboard

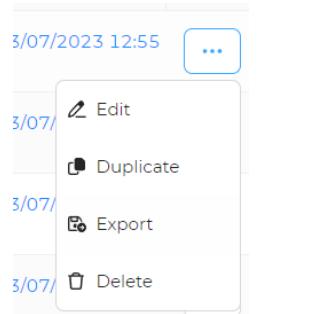


Figure 9.4: Dashboard Actions

9.4.2 Filtering and Sorting

This is same as the feature described in section case filtering and sorting

A screenshot of a dashboard management interface. At the top, there is a search bar with dropdowns for 'status' (set to 'any') and 'any' (set to 'Private'), and a red 'X' button. Below the search bar is a filter bar with a 'status: any[Private] X' button, an 'Add filter' button, an 'Apply filters' button, and a 'Clear filters' button. The main area shows a table titled 'default'. The columns are: STATUS, NAME, VERSION, # WIDGET, OWNER, DATES, C., U., and a three-dot menu column. There are two rows in the table: 'Alerts statistics' (version 1, 8 widgets, owner A, created on 13/07/2023 12:55) and 'Cases statistics' (version 1, 9 widgets, owner A, created on 13/07/2023 12:55).

Figure 9.5: Dashboard Filtering and Sorting

Chapter 10

Analyst Features : Search

10.1 Introduction

The Search feature can search across all elements in the hive project and find relevant results. It is useful as the hive contains lots of diverse functionalities which sometimes not very easy to find quickly.

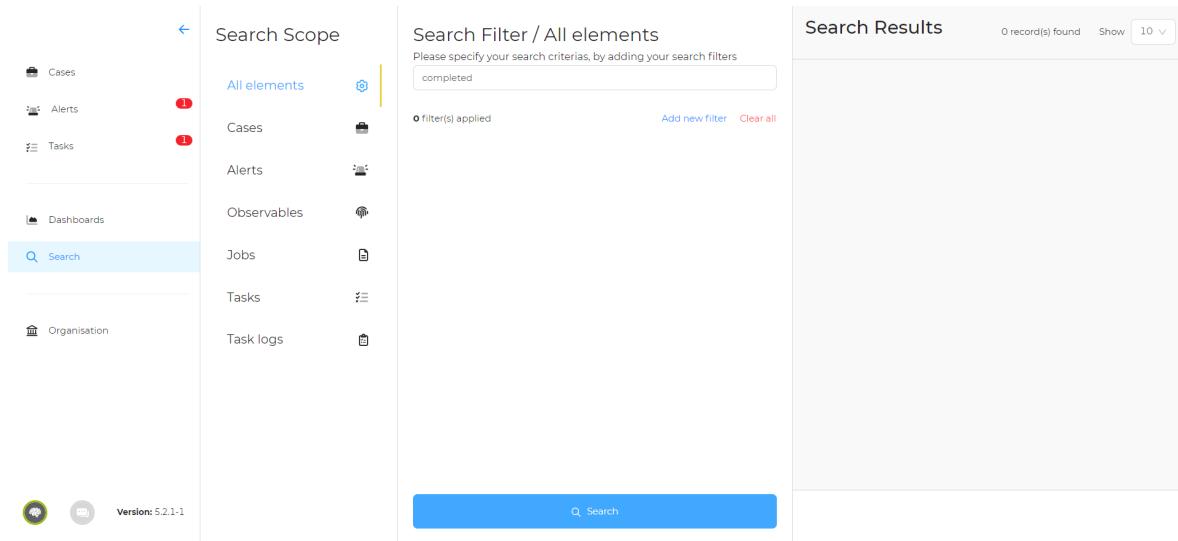


Figure 10.1: Search View

10.2 Search Alerts

Clicking on the Alerts icon and then using keywords and filters we can find relevant alerts organized in a list.

Figure 10.2: Search Alerts

10.3 Search Cases

Clicking on the Cases icon and then using keywords and filters we can find relevant cases organized in a list.

Figure 10.3: Search Cases

10.4 Search Observables

We can find observables from this criteria

The screenshot shows the 'Search Scope' sidebar with options: All elements, Cases, Alerts, Observables (selected), Jobs, Tasks, and Task logs. The 'Search Filter / Observables' section has a search bar containing 'test'. The 'Search Results' section displays two records:

- [ip]: 127[.]0[.]0[.]1:8888
24/08/2023 10:58
dummy test for visualization
test 2 observables
test 1
- [ip]: localhost:8888
24/08/2023 10:51
dummy test observable
test
test 1

Figure 10.4: Search Observables

10.5 Search Tasks

We can also search the tasks to quickly view relevant tasks

The screenshot shows the 'Search Scope' sidebar with options: All elements, Cases, Alerts, Observables, Jobs, Tasks (selected), and Task logs. The 'Search Filter / Tasks' section has a search bar containing 'test'. The 'Search Results' section displays one record:

- please resolve the test1 case
24/08/2023 10:48
Completed 9 days ago
test demo

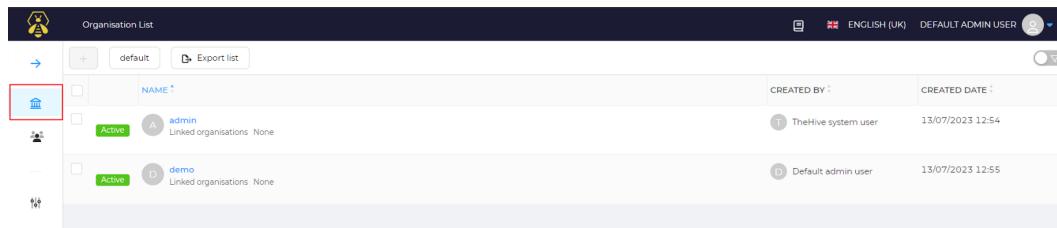
Figure 10.5: Search Tasks

Chapter 11

Admin Features : Organisations And Accounts Management

11.1 Manage Organisations

The organisations view is available in the Organisations tab in admin view.



NAME	CREATED BY	CREATED DATE
A admin	TheHive system user	13/07/2023 12:54
D demo	Default admin user	13/07/2023 12:55

Figure 11.1: Organisations List

11.1.1 Create Organisation

Organisations can be created by adding the + icon in top bar of the organisations view.

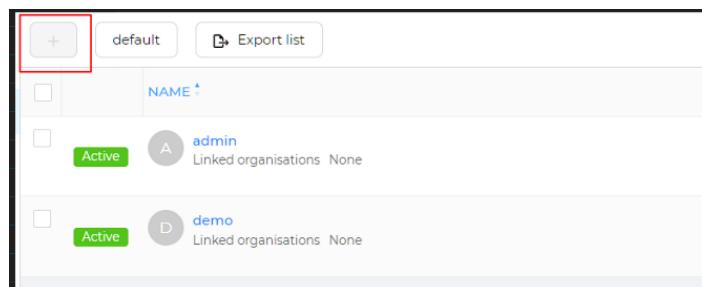


Figure 11.2: Add Organisation

However, this feature is not available in the demo VM with community license. It is only available to users with valid license.

11.1.2 Details of An Organisation

Clicking on an organisation in the list takes to details of that organisation.

DETAILS	FULL NAME	LOGIN	PROFILE	MFA	DATES	C.	U.	⋮
<input type="checkbox"/>	D Default admin user admin@thehive.local		admin		C. 13/07/2023 12:54			...
<input type="checkbox"/>	C cse406 cse406@gmail.com		admin		C. 09/09/2023 14:17			...

Figure 11.3: Details of An Organisation

11.1.3 Adding User to An Organisation

By clicking the + icon in the top bar of organisation details view, we can add a user to an organisation.

Adding a User

Type: Normal

Service users are essentially used for bots (API key authentication).

Organisation: admin

* Login: cse406@gmail.com

* Name: cse406

* Profile: admin

Permissions:

- manageAnalyzerTemplate
- manageConfig
- manageCustomField
- manageKnowledgeBase
- manageObservableTemplate
- manageOrganization
- managePattern
- managePlatform
- manageProfile
- manageTaxonomy
- manageUser

Cancel Save and add another Confirm

Figure 11.4: Add User to An Organisation

11.2 Manage Users

Similar to organisations, users view is available in the Users tab.

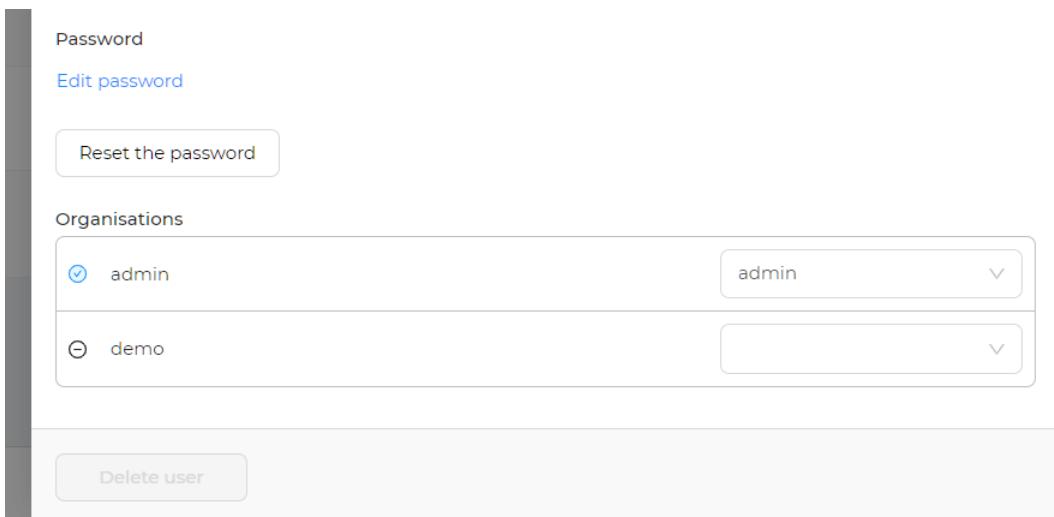


Figure 11.5: Users List

11.2.1 User Preview

Hovering on a user in the users list shows a preview button. Clicking on the button opens a drawer at the right which shows details of a user.

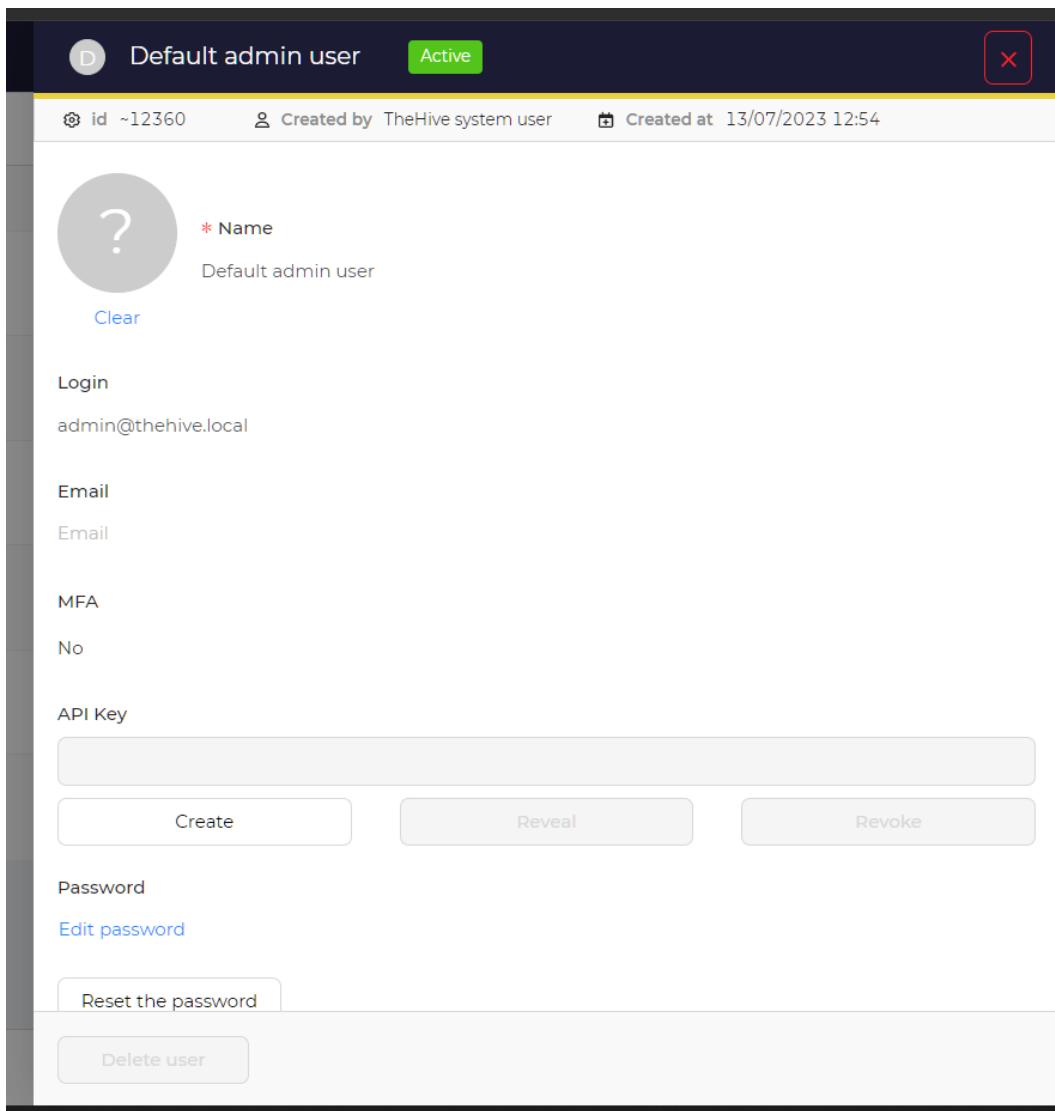


Figure 11.6: Preview of A User

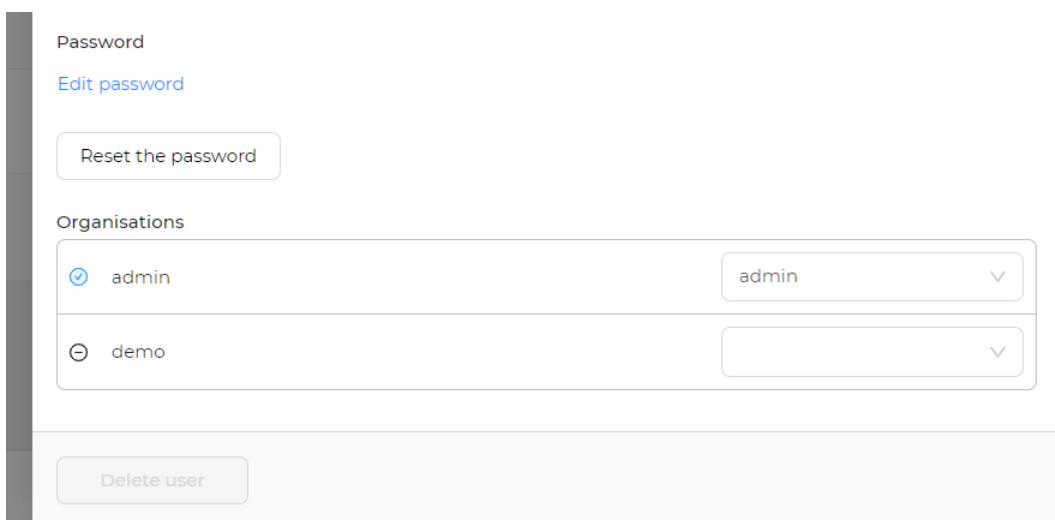


Figure 11.7: Preview of A User Continued

11.2.2 Create A User

Clicking on the + button in the top bar of users list view opens a drawer at the right which allows to add a new user.

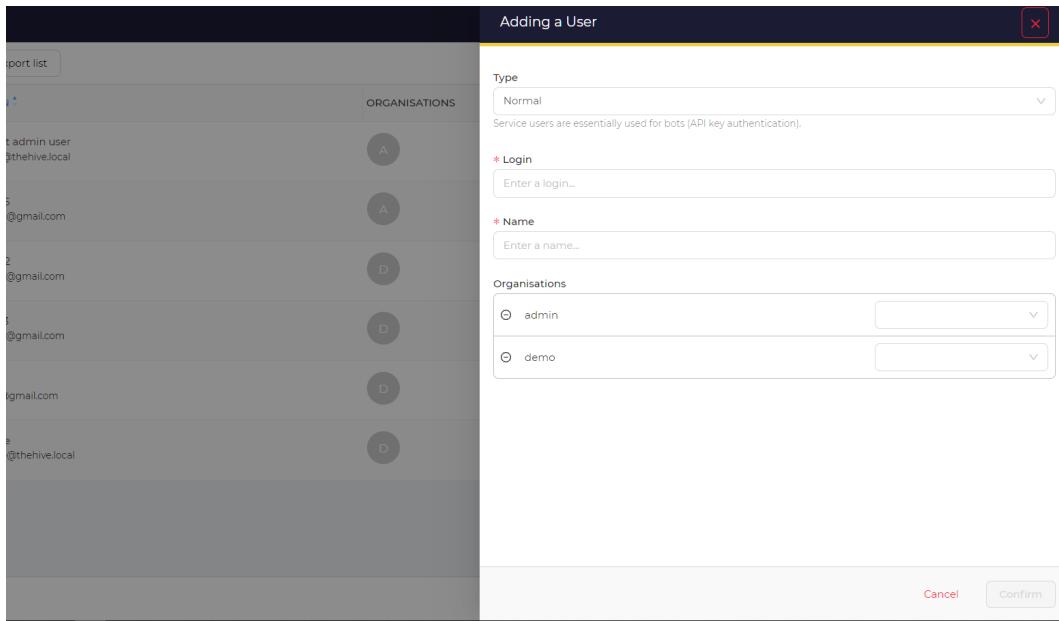


Figure 11.8: Create A User

Chapter 12

Admin Features : Entities Management

12.1 Introduction

The entities management options are available in admin's view, from the entities management option in the left taskbar.

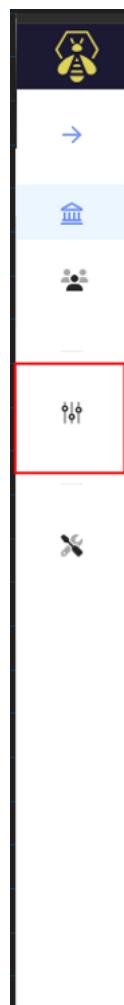


Figure 12.1: Admin view Taskbar

The various options in entities management are seen from the tabs at the top.

Figure 12.2: Options In Entities Management

12.2 Profiles

Some profiles are predefined in hives. These profiles are basically roles, each with various permissions. Users can be assigned one or more of these profiles. The Hive allows creating or customizing roles. However, a valid license is required to do so.

NAME *	PERMISSIONS
default	
admin	[manageAnalyzerTemplate, manageConfig, manageCustomField, manageKnowledgeBase, manageObservableTemplate, manageOrganization, managePattern, managePlatform, manageProfile, manageEconomy, manageUser]
analyst	[accessTheHive, manageAction, manageAlertCreate, manageAlertImport, manageAlertUpdate, manageAnalysis, manageCaseChangeOwnership, manageCaseCreate, manageCaseDelete, manageCaseMerge, manageCaseUpdate, manageCaseReport, manageCaseReportTemplate, manageCaseTemplate, manageComment, manageCustomEvent, manageFunctionCreate, manageFunctionInvoke, manageKnowledgeBase, manageObservable, managePage, manageProcedure, managePage, manageTask, manageUser]
org-admin	[accessTheHive, manageAction, manageAlertCreate, manageAlertImport, manageAlertUpdate, manageAnalysis, manageCaseChangeOwnership, manageCaseCreate, manageCaseDelete, manageCaseMerge, manageCaseUpdate, manageCaseReport, manageCaseReportTemplate, manageCaseTemplate, manageComment, manageConfig, manageCustomEvent, manageFunctionCreate, manageFunctionInvoke, manageKnowledgeBase, managePage, manageProcedure, managePageTemplate, manageProcedure, manageShare, manageTag, manageTask, manageUser]
read-only	No permissions

Figure 12.3: Profiles

12.3 Custom Fields

Custom fields can be used to add custom information to alert or cases. Although custom information can be added in details field of alert or cases, custom fields are useful, since they are discrete and so, statistics can be generated on them.

GROUP	DETAILS *	MANDATORY	OPTIONS	TYPE
default	businessimpact / BusinessImpact Impact of the incident on business	No	[Critical, High, Medium, Low]	string
default	businessunit / BusinessUnit Targeted business unit	No	[VIP, HR, Security, Sys Administrators, Developers, Sales, Marketing, Procurement, Legal]	string
default	contact / Contact email address of the contact	No	None	string
default	cse406-demon / cse406-demon demo	No	None	boolean
default	hits / Hits Numbers of hits found during the hunting	No	None	integer
default	sla / SLA	No	[4, 8, 12, 24]	integer

Figure 12.4: Custom Fields

12.3.1 Adding Custom Field

Adding a Custom Field X

* Display name
cse406-demon

* Technical name ⓘ
cse406-demon

* Description
demo

Group
default

* Type
boolean

Mandatory ⓘ

Cancel Confirm custom field creation

Figure 12.5: Add Custom Fields

12.3.2 Editing Custom Field

The screenshot shows a modal dialog titled "Editing a Custom Field". The form contains the following fields:

- Display name:** cse406-demon
- Technical name:** cse406-demon
- Description:** demo
- Group:** default
- Type:** integer
- Options:** 1, 2, 3
- Mandatory:** (checkbox)

At the bottom right are "Cancel" and "Confirm custom field edition" buttons.

Figure 12.6: Edit Custom Field

12.4 Observable Types

The Hive comes with a rich collection of observable data types. However, custom data types can still be added if required.

The screenshot shows a list of observable types. The table has two columns: "NAME" and an action column represented by three dots. The data rows are:

NAME	
autonomous-system	...
cse-406-demo	...
domain	...
file	...
filename	...
fqdn	...
hash	...
hostname	...

At the bottom are navigation buttons: < Previous, 0-17 of 17, Next >, Show, and a dropdown for items per page (30).

Figure 12.7: Observable Types

12.4.1 Adding Observable Type

The screenshot shows a modal dialog titled "Adding a Custom Field". It contains the following fields:

- * Display name: cse406-demon
- * Technical name: cse406-demon
- * Description: demo
- Group: default
- * Type: boolean
- Mandatory:

At the bottom right are "Cancel" and "Confirm custom field creation" buttons.

Figure 12.8: Add Observable Types

12.4.2 Deleting Observable Type



Figure 12.9: Delete Observable Types

12.5 Case Status

New case status option can be added, existing case status options can be modified. This feature is only available to users with valid license.

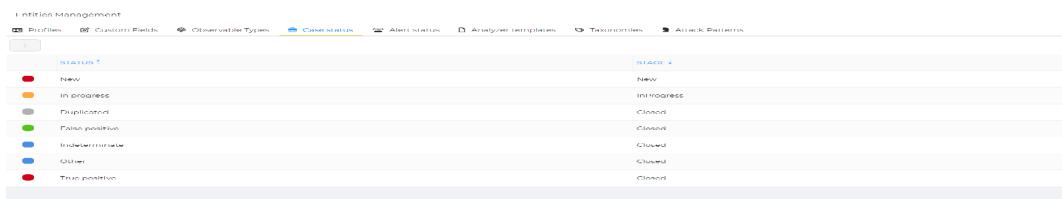


Figure 12.10: Case Status

12.6 Alert Status

Similar to case status.

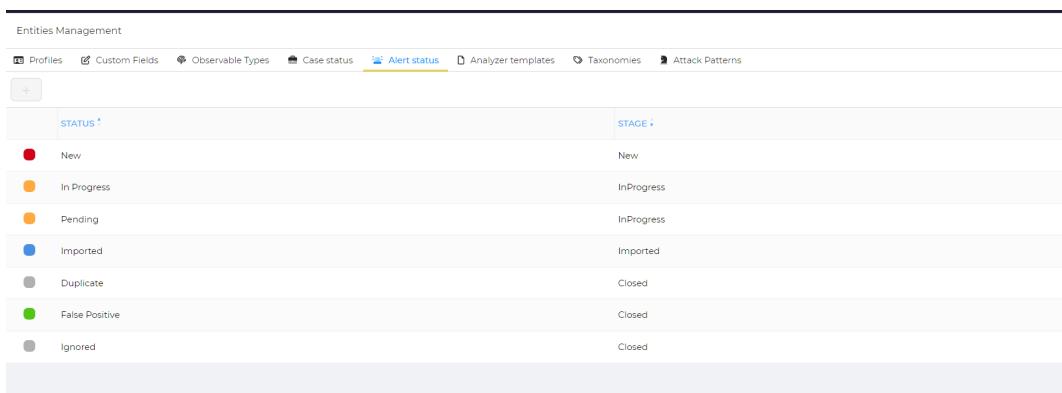


Figure 12.11: Alert Status

12.7 Analyzer Templates

Analyzers templates are used to format the reports generated by various analyzers. Typically, these reports are in json format, and so can be difficult to read. Analyzers template can be used to make them more readable.

Entities Management	
Profiles Custom Fields Observable Types Case status Alert status Analyzer templates Taxonomies Attack Patterns	
Import templates archive	
Name	
Abuse_Finder_3_0	Find abuse contacts associated with domain names, URLs, IPs and email addresses.
CyberCrime-Tracker_1_0	Search cybercrime-tracker.net for C2 servers.
DShield_Lookup_1_0	Query the SANS ISC DShield API to check for an IP address reputation.
EmailParser_2_1	Parse and visualise EML email message. Submit a .eml formatted file and extract some useful information.
FileInfo_8_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...
Fortiguard_URLCategory_2_1	Check the Fortiguard category of a URL, FQDN or a domain. Check the full available list at https://fortiguard.com/webfilter/categories
GoogleDNS_resolve_1_0_0	Request Google DNS over HTTPS service
Inoitusu_1_0	Query Inoitusu for a compromised email address.

Figure 12.12: Analyzers Templates

12.7.1 Adding Template

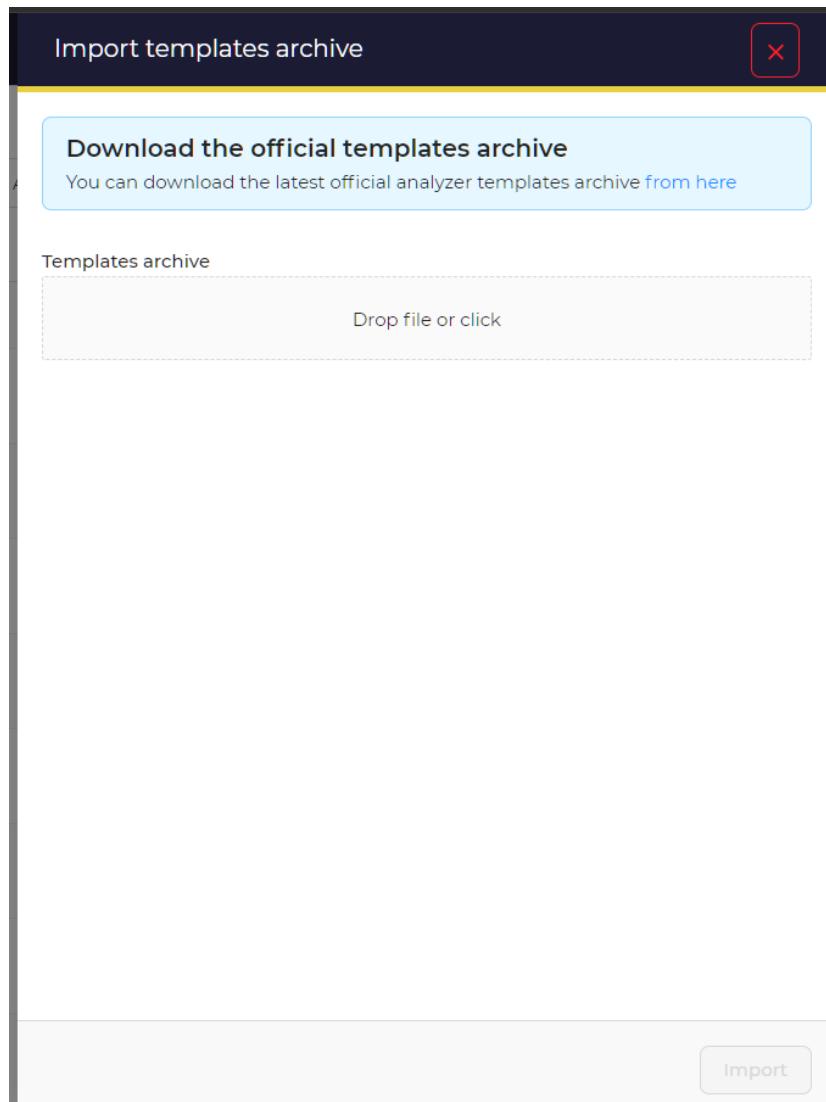
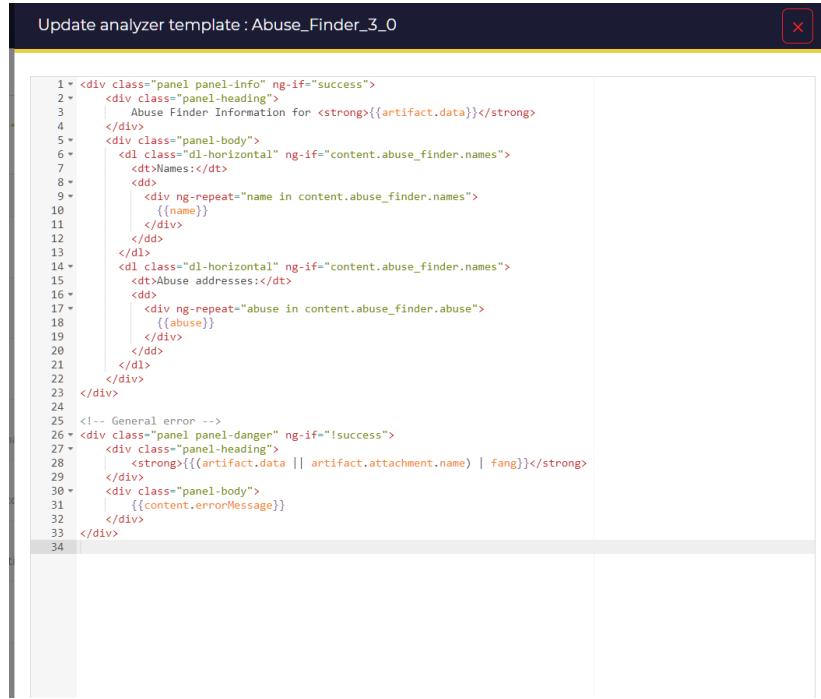


Figure 12.13: Add Analyzers Template

12.7.2 Modifying Template



```

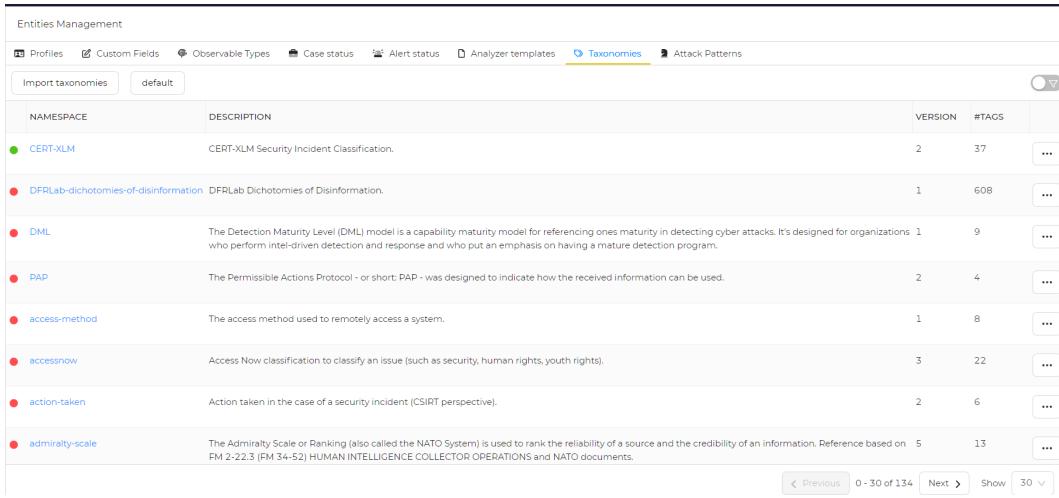
1 <div class="panel panel-info" ng-if="success">
2   <div class="panel-heading">
3     Abuse Finder Information for <strong>{{artifact.data}}</strong>
4   </div>
5   <div class="panel-body">
6     <dl class="dl-horizontal" ng-if="content.abuse_finder.names">
7       <dt>Names:</dt>
8       <dd>
9         <div ng-repeat="name in content.abuse_finder.names">
10           {{name}}
11         </div>
12       </dd>
13     </dl>
14     <dl class="dl-horizontal" ng-if="content.abuse_finder.names">
15       <dt>Abuse addresses:</dt>
16       <dd>
17         <div ng-repeat="abuse in content.abuse_finder.abuse">
18           {{abuse}}
19         </div>
20       </dd>
21     </dl>
22   </div>
23 </div>
24
25 <!-- General error -->
26 <div class="panel panel-danger" ng-if="!success">
27   <div class="panel-heading">
28     <strong>{{(artifact.data || artifact.attachment.name) | fang}}</strong>
29   </div>
30   <div class="panel-body">
31     {{content.errorMessage}}
32   </div>
33 </div>
34

```

Figure 12.14: Edit Analyzers Template

12.8 Taxonomies

A taxonomy is essentially a set of tags related to a topic. For example, the CERT-XLM taxonomoy contains all tags related to CERT-XLM security incident classification.



Entities Management			
Profiles	Custom Fields	Observable Types	Case status
Analyzer templates	Taxonomies	Attack Patterns	
Import taxonomies	default		
NAMESPACE	DESCRIPTION	VERSION	#TAGS
● CERT-XLM	CERT-XLM Security Incident Classification.	2	37
● DFRLab-dichotomies-of-disinformation	DFRLab Dichotomies of Disinformation.	1	608
● DML	The Detection Maturity Level (DML) model is a capability maturity model for referencing ones maturity in detecting cyber attacks. It's designed for organizations who perform intel-driven detection and response and who put an emphasis on having a mature detection program.	1	9
● PAP	The Permissible Actions Protocol - or short: PAP - was designed to indicate how the received information can be used.	2	4
● access-method	The access method used to remotely access a system.	1	8
● accessnow	Access Now classification to classify an issue (such as security, human rights, youth rights).	3	22
● action-taken	Action taken in the case of a security incident (CSIRT perspective).	2	6
● admiralty-scale	The Admiralty Scale or Ranking (also called the NATO System) is used to rank the reliability of a source and the credibility of an information. Reference based on PM 2-22.3 (FM 34-52) HUMAN INTELLIGENCE COLLECTOR OPERATIONS and NATO documents.	5	13

Figure 12.15: Taxonomies

CERT-XLM taxonomy					
Namespace	Version	Description			
CERT-XLM Security Incident Classification.					
Tags					
TAG	PREDICATE	VALUE	COLOUR		
CERT-XLMabusive-content="harmful-speech"	abusive-content	harmful-speech	#000000		
CERT-XLMabusive-content="spam"	abusive-content	spam	#000000		
CERT-XLMabusive-content="violence"	abusive-content	violence	#000000		
CERT-XLMavailability="outage"	availability	outage	#000000		
CERT-XLMavailability="dos"	availability	dos	#000000		
CERT-XLMavailability="ddos"	availability	ddos	#000000		
CERT-XLMavailability="sabotage"	availability	sabotage	#000000		
CERT-XLMconformity="standard"	conformity	standard	#000000		
CERT-XLMconformity="regulator"	conformity	regulator	#000000		

Figure 12.16: Cert Taxonomy

12.8.1 Adding Taxonomy

Import taxonomies archive

Download the official MISP taxonomies archive
You can download the latest archive of the official MISP Taxonomies [from here](#)

Taxonomies archive

Drop file or click

The taxonomies archive must be a valid ZIP file containing at least one file named machinetag.json

Import

Figure 12.17: Add Taxonomies

12.8.2 Activating Taxonomy

DML	The Detection Maturity Level (DML) model is a capability maturity model for referencing one's maturity in detecting cyber attacks. It's designed for organizations who perform intel-driven detection and response and who put an emphasis on having a mature detection program.	1	9	<input type="button" value="..."/>
PAP	The Permissible Actions Protocol - or short: PAP - was designed to indicate how the received information can be used.	2	<input checked="" type="checkbox"/> Activate <input type="checkbox"/> Delete <input type="button" value="..."/>	
access-method	The access method used to remotely access a system.	1	8	<input type="button" value="..."/>

Figure 12.18: Activate Taxonomies

12.9 Attack Patterns

This section contains details of various attack patterns.

NAME:	Enterprise Attack	CREATED BY:	TheHive system user
		CREATED DATE:	13/07/2023 12:54

Figure 12.19: Attack Pattern

12.9.1 Details of An Attack Pattern

Clicking on an attack pattern shows its details.

ID	NAME	SUB-TECHNIQUE OF	TACTICS	DESCRIPTION
T1003.008	/etc/passwd and /etc/shadow		credential-access	Adversaries may attempt to dump the contents of <code>/etc/passwd</code> and <code>/etc/shadow</code> to enable offline password cracking. Most modern Linux operating systems use a combination of <code>/etc/passwd</code> and <code>/etc/shadow</code> (...)
T1557.002	ARP Cache Poisoning		collection credential-access	Adversaries may poison Address Resolution Protocol (ARP) caches to position themselves between the communication of two or more networked devices. This activity may be used to enable follow-on behaviors such as
T1558.004	AS-REP Roasting		credential-access	Adversaries may reveal credentials of accounts that have disabled Kerberos preauthentication by Password Cracking Kerberos messages. (Citation: Harmj0y (...))
T1557	Adversary-in-the-Middle		collection credential-access	Adversaries may attempt to position themselves between two or more networked devices using an adversary-in-the-middle (ATM) technique to support follow-on behaviors such as
T1552.003	Bash History		credential-access	Adversaries may search the bash command history on compromised systems for insecurely stored credentials. Bash keeps track of the commands users type on the command-line with the <code>"history"</code> utility. Once a user logs out, the history is flushed to the (...)

Figure 12.20: Attack Pattern Details

T1003.008 - /etc/passwd and /etc/shadow

ID	Sub-technique Name	Data Sources
T1003.008	/etc/passwd and /etc/shadow	Command: Command Execution File: File Access
Permissions Required	Remote Support	
root	FALSE	

Description

Adversaries may attempt to dump the contents of `/etc/passwd` and `/etc/shadow` to enable offline password cracking. Most modern Linux operating systems use a combination of `/etc/passwd` and `/etc/shadow` to store user account information including password hashes in `/etc/shadow`. By default, `/etc/shadow` is only readable by the root user.(Citation: Linux Password and Shadow File Formats)

The Linux utility, unshadow, can be used to combine the two files in a format suited for password cracking utilities such as John the Ripper(Citation: nixCraft - John the Ripper) `/usr/bin/unshadow /etc/passwd /etc/shadow > /tmp/crack.password.db`

Figure 12.21: Attack Pattern Details

12.9.2 Adding Attack Pattern

Import MITRE ATT&CK patterns

Download the official MITRE ATT&CK library
You can download the latest archive of the official MITRE ATT&CK patterns
[enterprise-attack](#), [mobile-attack](#)

MITRE ATT&CK patterns

Name of the catalog

Drop file or click

Import

Figure 12.22: Add Attack Pattern

Chapter 13

Admin Features : Platform Management

13.1 Introduction

The platform management options are available in admin's view, from the platform management option in the left taskbar.

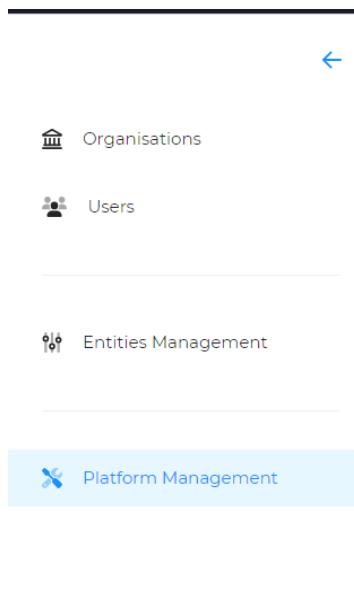


Figure 13.1: Admin view Taskbar

The various options in platform management are seen from the tabs at the top. We will discuss the functionalities through detailed snaps

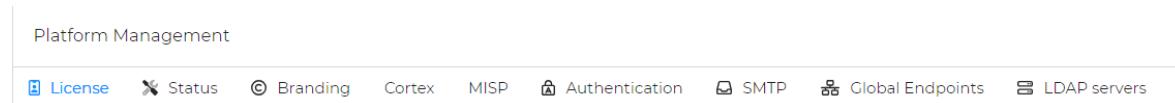


Figure 13.2: Options In Platform Management

13.2 License

By default TheHive includes the community edition license. It comes with some free and limited capabilities. We may generate a new license if we have any key or continue to use community edition if key unavailable. In our case, as we didn't have any key, we had to use the community edition

The screenshot shows the 'License Management' section of the TheHive interface. At the top, there are tabs for License, Status, Branding, Cortex, MISP, Authentication, and SMTP. The 'License' tab is selected. Below the tabs, it says 'License Management' and 'No license'. There is a blue button labeled 'Activate a license'. A table lists various resource counts: User (community), Readonly users (0 / Unlimited), Normal users (1 / 2), Service users (0 / Unlimited), Organisations (1 / 1), Dashboards (4 / Unlimited), Case templates (1 / Unlimited), Nodes cluster (1 / 1), MISP servers (0 / 1), and Cortex servers (1 / 1).

Figure 13.3: Community License

The screenshot shows a modal dialog titled 'Set a license key'. It contains a message: 'The generated TheHive license is tied to your instance. This means that you will not be able to activate it on other instances after the license generation. If you want to move your license, please contact the customer support'. Below this is a 'Challenge' section containing a long, complex string of characters. To the right of the challenge is a 'Copy this challenge' link. At the bottom of the dialog, there is a field labeled '* License' with the placeholder 'Enter a license...', a 'Cancel' button, and an 'Activate the license key' button.

Figure 13.4: Add New License (if key available)

13.3 Platform Status

We can check the current status of the platform by clicking on status tab

The screenshot shows the 'Status' tab selected in the top navigation bar. The main content area is divided into two sections: 'Database Schema status' and 'Database integrity check'.

Database Schema status:

Status	Schema name	Schema version
OK	thehive-enterprise	83
OK	thehive	98
OK	thehive-cortex	2

Database integrity check:

Control name	#Entities	Action
Action	0	<button>See details</button>
Alert	1	<button>See details</button>
AlertStatus	7	<button>See details</button>
AnalyzerTemplate	214	<button>See details</button>
Attachment	1	<button>See details</button>
AttachmentHash	0	<button>See details</button>
Audit	502	<button>See details</button>
Case	2	<button>See details</button>
CaseStatus	7	<button>See details</button>

Figure 13.5: Plaform Status

13.4 Cortex

Cortex is an analysis and automation engine that complements TheHive by providing additional capabilities. These includes benefits from Analyzers to gather information and intelligence about Observables and run active actions on your network or third party services with Responders. The installed demo vm comes with a cortex server. We can click on cortex tab to view the servers.

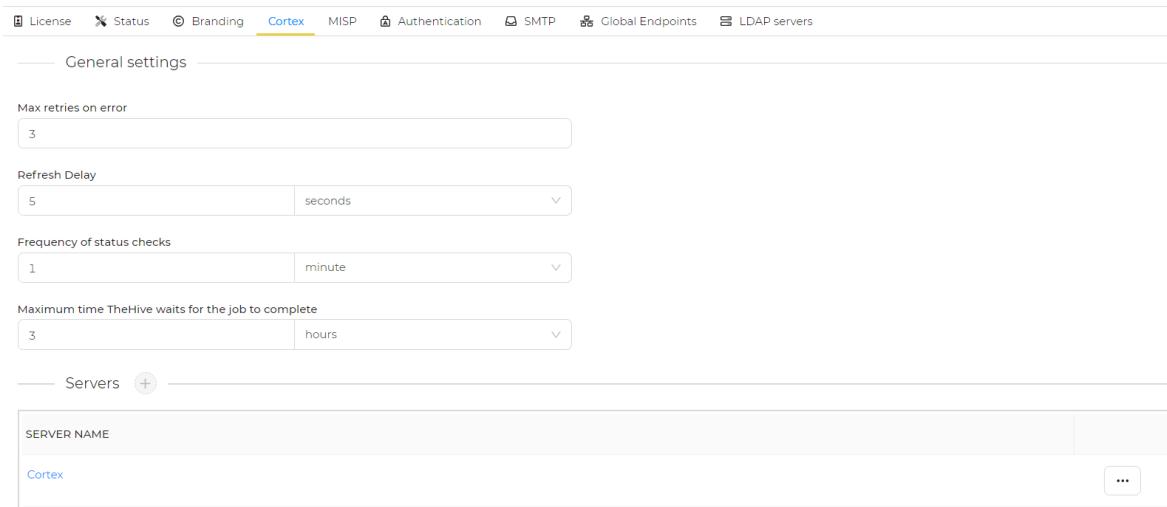


Figure 13.6: Cortex Tab View

13.4.1 Add Cortex Server

We can add cortex server by clicking on the + icon (if license permitted). In community license, we cannot add more than one server.

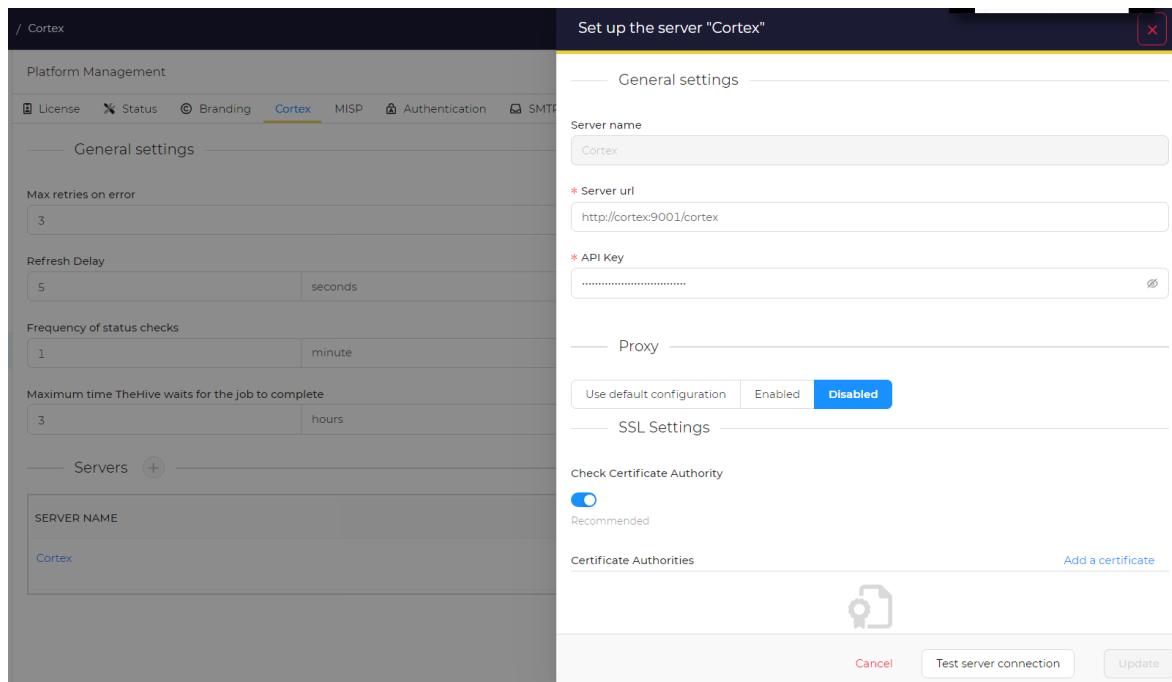


Figure 13.7: Add Cortex Server

13.4.2 Delete Cortex Server

We may also delete any existing cortex server.



Figure 13.8: Delete Cortex Server

13.5 MISP

MISP (Malware Information Sharing Platform and Threat Sharing) is an open-source threat intelligence platform which facilitates the sharing of structured threat information among organizations. We can integrate MISP with the hive where MISP events can be imported as Alerts in TheHive. A set of filter can refine the imported events. Moreover, Observables flagged as IOCs in a Case can be exported in a new event in MISP.

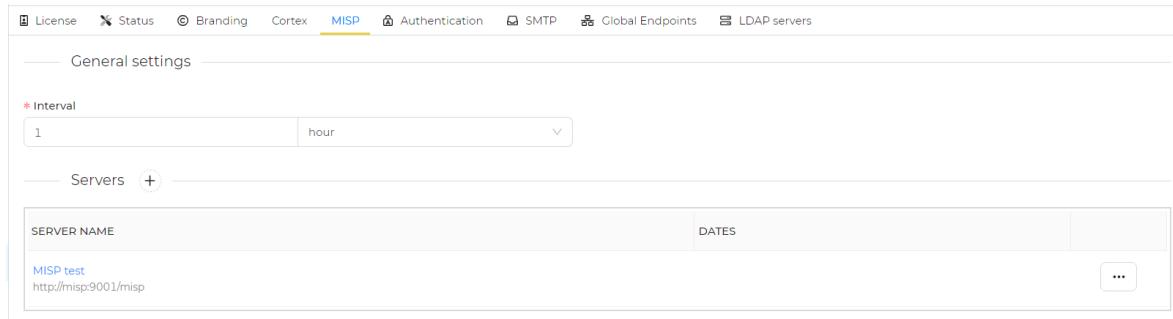


Figure 13.9: MISP Tab View

13.5.1 Add MISP Server

We can add MISP server by clicking on the + icon (if license permitted). In community license, we cannot add more than one server.

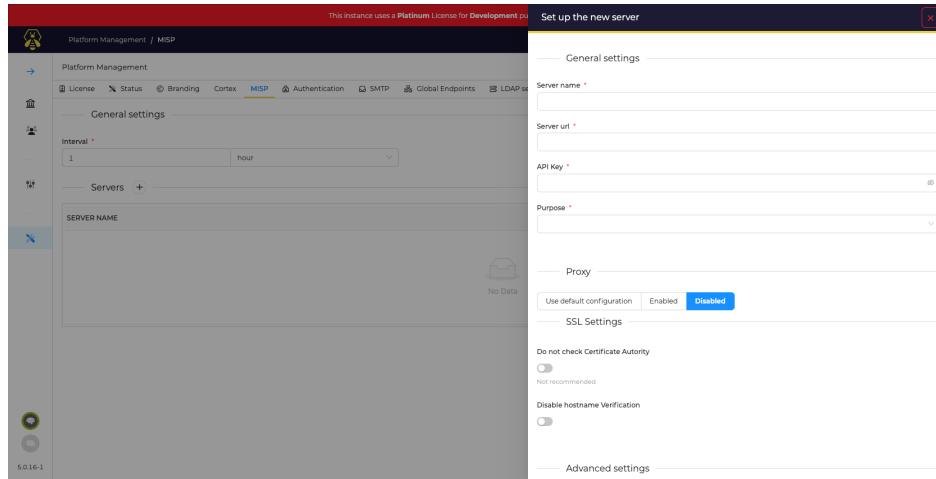


Figure 13.10: Add MISP Server

13.5.2 Configure MISP Server Settings

We can configure settings of a server by using **Advanced** and **Filter** Settings

—— Advanced settings ——

Choose the filter on TheHive organisations
Include all organisations

Tags
[Input field] [+]

Export case tags

Export observables tags

—— Filter settings ——

Maximum age
[Input field] minutes

Organisations to include
[Input field]

Organisations to exclude
[Input field]

Maximum number of attributes
[Input field]

List of allowed tags
[Input field] [+]

Prohibited tags list
[Input field] [+]

Figure 13.11: MISP Server Settings

13.5.3 Delete MISP Server

We may also delete any existing MISP server.

SERVER NAME	DATES	...
misp test https://www.google.com		<input type="button" value="Delete"/> <input type="button" value="..."/>

Figure 13.12: Delete MISP Server

13.6 Authentication

Admin can modify the authentication settings from authentication tab

The screenshot shows the 'Authentication' tab selected in the top navigation bar. The page is divided into several sections:

- Session settings** (highlighted in blue):
 - * Duration of user inactivity before session expiration: 1 hour
 - * Warning message display time, before session expiration: 5 minutes
- Advanced settings** (highlighted in blue):
 - Enable API Key authentication:
 - Enable Basic Authentication: * Realm: thehive
 - Enable HTTP header Authentication:
 - Enable Multifactor authentication:
- Default domain for user login**: @ thehive.local
- Authentication providers** (highlighted in blue):

ORDER	TYPE	STATUS
▲	Local Authentication	Enabled
▼	Directories Authentication	Disabled
▲	OAuth 2 Authentication	Disabled
▼	SAML Authentication	Disabled

Figure 13.13: Authentication Tab

13.7 SMTP

TheHive can connect to a SMTP server to send email notifications, and allow users to define or change their password when forgotten

Server settings

* Server name or IP address
localhost

* Port
25

Reset Password

* Send emails from
thehive@local.com

Token expiration
10 minutes

Security and authentication settings

Connection Security
none

Username

Password

Figure 13.14: SMTP Tab

13.8 Global EndPoint Creation

An endpoint is the point of entry in a communication channel when two systems interact with each other. We can create global endpoint according to necessity. The hive provides 5 different connectors (Webhook, Mattermost, Slack, MSTeams and Http) for this purpose. In the community license, only webhook connector can be utilized.

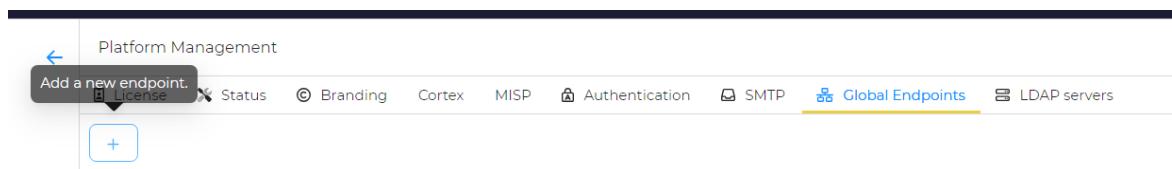


Figure 13.15: Add Global Endpoint

Add New Endpoint

By clicking on the + button, a new endpoint can be created

Endpoint creation

* Choose a connector

 Webhook

 Mattermost

 Slack

 Teams

 Http

Name
Enter a name

* Url
Enter a valid URL

Version
1

Organisations
Choose the filter on TheHive organisations
Choose filter organisation ▾

Authentication
Auth type
None ▾
Proxy

SSL Settings
Check Certificate Authority
 Recommended
Certificate Authorities
Add a certificate

No custom Certificate Authorities. [Add a certificate](#) ⓘ

Disable hostname Verification

Cancel Confirm

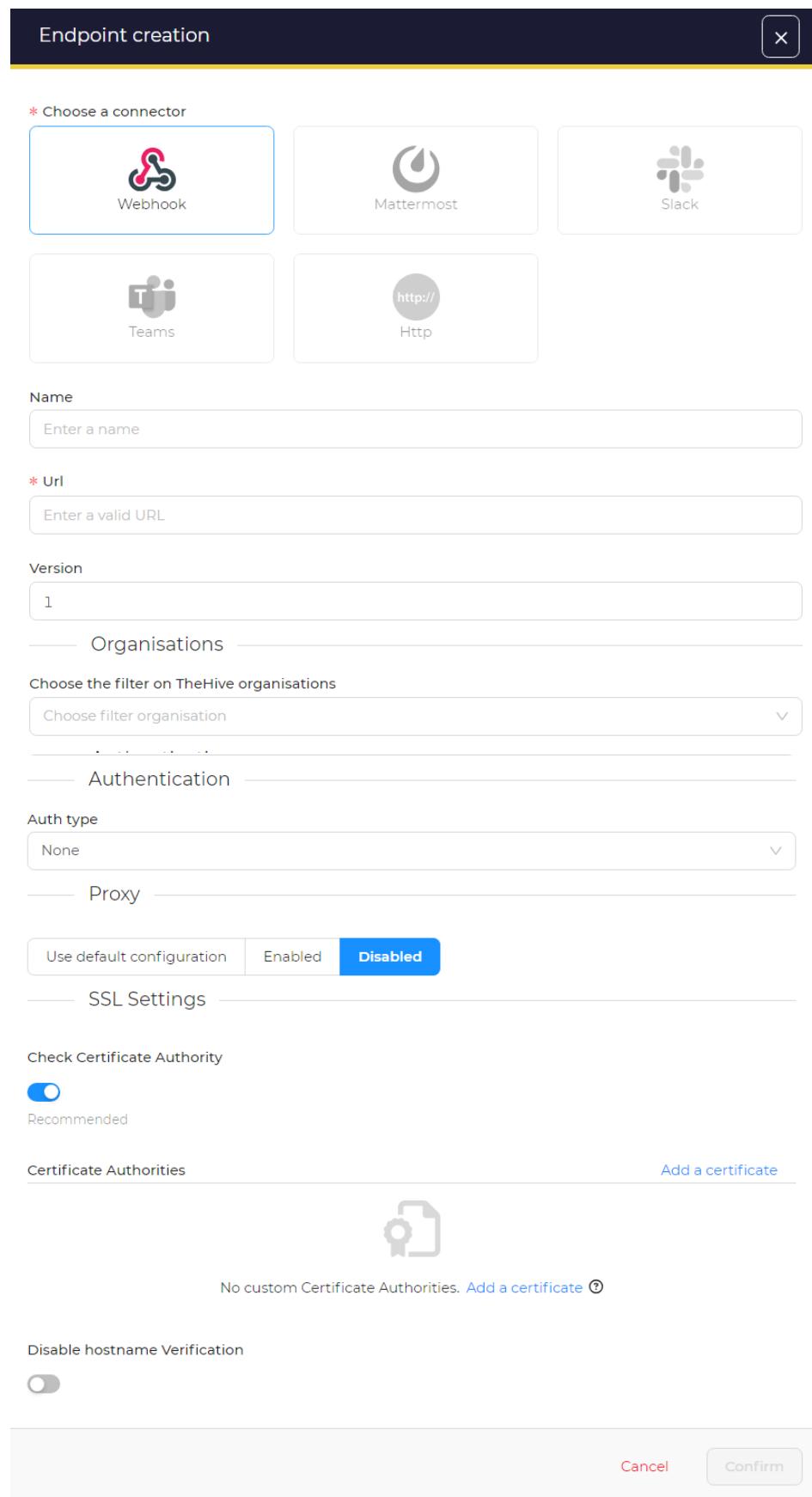


Figure 13.16: Endpoint Creation

Chapter 14

Platform Integration : Integration With Cortex

14.1 Introduction

Cortex mainly provides the following 2 functionalities.

- A.** Run various analyzers on observables from a single tool. Cyber security personnel often require to analyze an observable using multiple tools to gain as much information as possible. Going to each platform, querying, and storing the result properly can become cumbersome and unmanageable for individuals. Cortex lifts this burden by bringing all analyzers in one tool. Cortex can make api request to analyzers just from click of a button. It also stores the reports from the analyzers which can be viewed easily.
- B.** Launch responders for case, tasks, observables, logs, and alerts to perform some action.

The demo VM of the Hive comes with Cortex integration.

14.2 Analyzers

An analyzer is a program that takes an observable (eg. ip address, hash, file etc) as an input, analyzes it and produces result describing its findings. The analysis portion could be a range of activity. For example, analyzing an ip address may involve checking if any suspicious activity has been seen from it before. Analyzing a file may involve checking for suspicious instructions to understand if it is infected by a malware.

14.2.1 Available Analyzers

Cortex comes with a great numbers of analyzers already available.

Figure 14.1: Available Analyzers In Cortex

14.2.2 Enabling an Analyzer

We can enable an analyzer to make it available in The Hive. Here we are enabling the AbuseIPDB analyzer, which determines whether an ip was reported as malicious or not by AbuseIPDB.

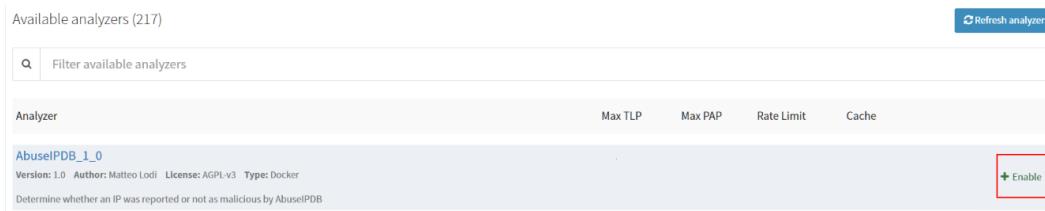


Figure 14.2: Enabling An Analyzer In Cortex

This screenshot shows the configuration page for enabling the 'AbuseIPDB_1_0' analyzer. The title is 'Enable analyzer AbuseIPDB_1_0'. The form is divided into sections: 'Base details' (Name: AbuseIPDB_1_0), 'Configuration' (key: API key for AbuseIPDB, days: 30), and 'Options' (Enable TLP check: True, Max TLP: AMBER; Enable PAP check: True, Max PAP: AMBER; HTTP Proxy: [empty], HTTPS Proxy: [empty], CA Certs: [empty]).

Figure 14.3: Enabling an Analyzer In Cortex Continued

HTTPS Proxy

CA Certs

Job cache

Job timeout

Extract observables

True False

Set to True to enable automatic observables extraction from analysis reports.

Rate Limiting

- choose unit -

Define the maximum number of requests and the associated unit if applicable.

Cancel

* Required field

Save

Figure 14.4: Enabling an Analyzer In Cortex Continued

14.2.3 Using Enabled Analyzer From Hive

The enabled analyzer will be available for use in The Hive's analyzers section.

Analyzers	
ANALYZER	LAST ANALYSIS
Abuse_Finder_3_0	No Data
CyberCrime-Tracker_1_0	No Data
DShield_lookup_1_0	No Data
GoogleDNS_resolve_1_0_0	No Data
Maltiverse_Report_1_0	No Data
MaxMind_GeoIP_4_0	No Data
TalosReputation_1_0	No Data
Threatcrowd_1_0	No Data

Figure 14.5: Analyzers Available in The Hive-Before

The screenshot shows a list of analyzers under the 'Analyzers' tab. The 'LAST ANALYSIS' column shows 'No Data' for all entries. The 'AbuseIPDB_1_0' entry is highlighted with a red border.

ANALYZER	LAST ANALYSIS
Abuse_Finder_3_0	No Data
AbuseIPDB_1_0	No Data
CyberCrime_Tracker_1_0	No Data
DShield_lookup_1_0	No Data
GoogleDNS_resolve_1_0_0	No Data
Maitiverse_Report_1_0	No Data
MaxMind_GeoIP_4_0	No Data

Figure 14.6: Analyzers Available in The Hive-After

14.3 Responders

A responder is basically a program that performs some actions based on an alert, task, or observables. These may have a wide range of activity. For example, a responder for an ip observable may add entry to a firewall to block that ip. A responder on a case may send detailed status information of a case to some predefined mail addresses.

14.3.1 Available Responders

Similar to analyzers, cortex comes a number of already available responders

The screenshot shows a list of available responders. The 'MSDefenderOffice365_block_1_0' responder is highlighted with a red border.

Responders	Max TLP	Max PAP	Rate Limit
MSDefenderOffice365_block_1_0			

Figure 14.7: Available Responders In Cortex

14.3.2 Enabling a Responder

We can enable a responder to make it available in The Hive. Here we are enabling the MSDefender, which add entries to microsoft 365 Defender.

The screenshot shows the 'MSDefenderOffice365_block_1_0' responder details page. The 'Enable' button is highlighted with a red border.

Figure 14.8: Enabling A Responder In Cortex

Enable responder MSDefenderOffice365_block_1_0

Base details

Name	MSDefenderOffice365_block_1_0
------	-------------------------------

Configuration

certificate_base64 *	<input type="text"/>	Apply defaults
Base64-encoded PFX certificate to be used for certificate-based authentication.		
certificate_password *	<input type="password"/>	
Password for the certificate used to authenticate		
app_id *	<input type="text"/>	
The application ID of the service principal that's used in certificate based authentication		
organization *	<input type="text"/>	
Tenant ID. Example: something.onmicrosoft.com		
block_expiration_days *	<input type="text" value="0"/>	
How many days out should we set the expiration? A value <= 0 means to set no expiration.		

Options

Enable TLP check	<input checked="" type="radio"/> True	<input type="radio"/> False	Max TLP	AMBER
------------------	---------------------------------------	-----------------------------	---------	-------

[Apply defaults](#)

Figure 14.9: Enabling a Responder In Cortex Continued

Tenant ID. Example: something.onmicrosoft.com				
block_expiration_days *	<input type="text" value="0"/>			
How many days out should we set the expiration? A value <= 0 means to set no expiration.				
Options	Apply defaults			
Enable TLP check	<input checked="" type="radio"/> True	<input type="radio"/> False	Max TLP	AMBER
Enable PAP check	<input checked="" type="radio"/> True	<input type="radio"/> False	Max PAP	AMBER
HTTP Proxy	<input type="text"/>			
HTTPS Proxy	<input type="text"/>			
CA Certs	<input type="text"/>			
Job timeout	<input type="text" value="30"/>			
Rate Limiting	<input type="text"/>	-- choose unit --		
Define the maximum number of requests and the associated unit if applicable.				
Cancel	* Required field			Save

Figure 14.10: Enabling a Responder In Cortex Continued

14.3.3 Using Enabled Responder From Hive

The enabled responder will be available for use in The Hive responders option.

The screenshot shows the Microsoft Exchange Server Vulnerabilities page in The Hive. The left panel displays observable details for Threatcrowd_1_0, URLhaus_2_0, and Urlscan_io_Search_0_1_1, all showing 'No Data'. Below this is a section for 'Responder Reports' which also shows 'No reports'. A 'Seen in following cases or alerts' section lists an alert from CISA.gov - AA21-062A Mitigate Microsoft Exchange vulnerabilities, with flags TLP:CLEAR and PAP:AMBER. The right panel shows a responder search interface with a search bar and a 'NAME *' field. A responder named 'MSDefenderOffice365_block_1_0' is listed with the note: 'Add entries to the Tenant Allow/Block List in the Microsoft 365 Defender'.

Figure 14.11: Responders Available in The Hive-Before

This screenshot is identical to Figure 14.11, showing the Microsoft Exchange Server Vulnerabilities page in The Hive. The left panel shows the same observables and alert details. The right panel shows the responder search interface, where the 'MSDefenderOffice365_block_1_0' responder has been added and is now listed with a 'Launch responder' button.

Figure 14.12: Responders Available in The Hive-After

Chapter 15

Platform Integration : Integration With MISP

15.1 Introduction

MISP (Malware Information Sharing Platform and Threat Sharing) is an open-source threat intelligence platform which facilitates the sharing of structured threat information among organizations. We can integrate MISP with the hive which mainly provides the following 3 functionalities.

- A. MISP events can be imported as Alerts in TheHive. A set of filter can refine the imported events. Thus we can sync data from different threat analysis and other organizations such as malicious ip, domain etc
- B. Observables flagged as IOCs in a Case can be exported in a new event in MISP
- C. We can also create a new case from a predefined MISP case template

15.2 Add MISP Server

We have already discussed the details of adding an MISP server in Add-MISP. We can also follow the link MISP-Integration to install MISP and generate MISP API key if not available

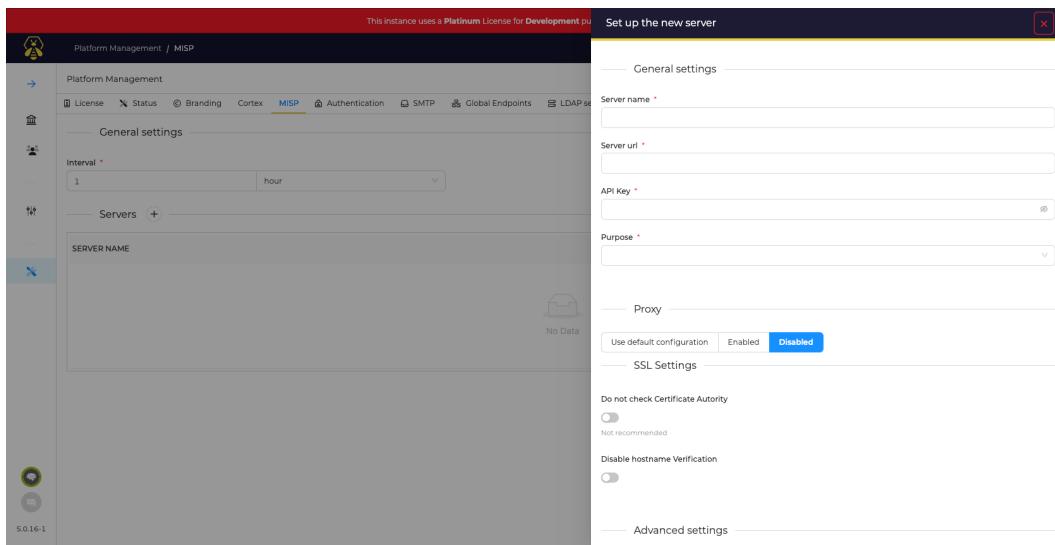


Figure 15.1: Add MISP Server

15.3 MISP Alerts

After successful addition of MISP server, we will be able to see alerts from the added MISP server

SEVERITY	STATUS	TITLE	# CASE	TYPE	SOURCE	REFERENCE	DETAILS	DATES	O.	C.	U.
<input type="checkbox"/> Low	New	#8 Expansion on OSINT Operation Pawn Storm: The Red in SEDNIT from Trend Micro	8	misp	ORCNAME	Observables TTPs	414 O. 10/23/14 03:00 C. 11/08/22 20:09 U. 11/08/22 20:10				
<input type="checkbox"/> Medium	New	#5 OSINT Watching Attackers Through Virustotal blog post by Brandon Dixon (9plus)	5	misp	ORCNAME	Observables TTPs	1817 O. 09/01/14 03:00 C. 11/08/22 20:01 U. 11/08/22 20:09				
<input type="checkbox"/> Medium	New	#4 OSINT Democracy in Hong Kong Under Attack blog post from Volexity (Steven Adair)	4	misp	ORCNAME	Observables TTPs	61 O. 10/09/14 03:00 C. 11/08/22 20:01 U. 11/08/22 20:01				

Source: <https://kifarunix.com/wp-content/uploads/2022/11/thehive-misp-event-alerts.png>

Figure 15.2: Alerts From MISP Server

15.4 Case Creation From MISP Template

We can add a new case from the predefined MISP case template where some configurations have already been applied. The details have been discussed in section Case-MISP-Template

X

Apply case template

* Select case template

MISP

Merge tags

hunting

Merge custom fields

Hits

Import tasks

Filter tasks...

Select all
Deselect all

default - Search for IOCs on Mail gateway logs Run queries in Mail gateway logs and look for IO...

default - Search for IOCs on Firewall logs Run queries in firewall logs and look for IOCs of type IP, ...

default - Search for IOCs on Web proxy logs Run queries in web proxy logs and look for IOCs of t...

Add description

Check if IOCs shared by the community have been seen on the network

Apply severity

SEV:MEDIUM

Apply TLP

Cancel
Confirm

Figure 15.3: Case Creation From MISP Template

Chapter 16

Platform Integration : Integration With Other Platforms

There are lots of other platforms which can be integrated with the Hive.

- Wazuh
- Webhook
- Mattermost
- MSTeams
- Slack
- Kafka
- Redis

Severity	Read	Title	Case	Type	Source	Reference	Observables	Dates	O.	C.	U.
<input type="checkbox"/>	M	Unread	Ossec server started.	None	wazuh_alert wazuh	b21655	0	O. 03/14/22 15:30 C. 03/14/22 15:30			
<input type="checkbox"/>	M	Unread	Listened ports status (netstat) changed (new port opened or closed).	None	wazuh_alert wazuh	08142f	3	O. 03/14/22 15:30 C. 03/14/22 15:30			

Figure 16.1: Alerts from Wazuh

To keep our documentation focused on The Hive and to keep it simple and precise, we will not discuss the integration mechanism for these tools. We have added some links in the references section.

Chapter 17

Conclusion

The Hive is a powerful and versatile SIRS that can be used by organizations of all sizes. It is constantly being updated with new features and improvements. Its flexible architecture, coupled with a user-friendly interface, offers security teams the tools they need to orchestrate incident response processes efficiently. The platform's automation capabilities, seamless integration with external security tools, and comprehensive reporting and analytics empower security professionals to streamline their incident response workflows. On the whole, as the threat landscape continues to evolve, The Hive remains a valuable asset in enhancing an organization's overall security posture, streamlining incident response processes and ensuring a proactive approach to cybersecurity.

Chapter 18

References

- <https://docs.strangebee.com/thehive>
- <https://www.tines.com/blog/getting-started-with-thehive-automation>
- <https://appmaster.io/blog/thehive-overview>
- <https://docs.strangebee.com/thehive/api-docs/>
- <https://kifarunix.com/how-to-integrate-thehive-with-misp>
- <https://wazuh.com/blog/using-wazuh-and-thehive-for-threat-protection-and-incident-response/>
- <https://docs.strangebee.com/thehive/user-guides/organisation/notifications/mattermost/>
- <https://docs.strangebee.com/thehive/user-guides/organisation/notifications/teams/>