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

Chapter 1

High Level Overview

The Hive is a free and open-source Security Incident Response Platform (SIRS) developed by StrangeBee. 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 secuity 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.

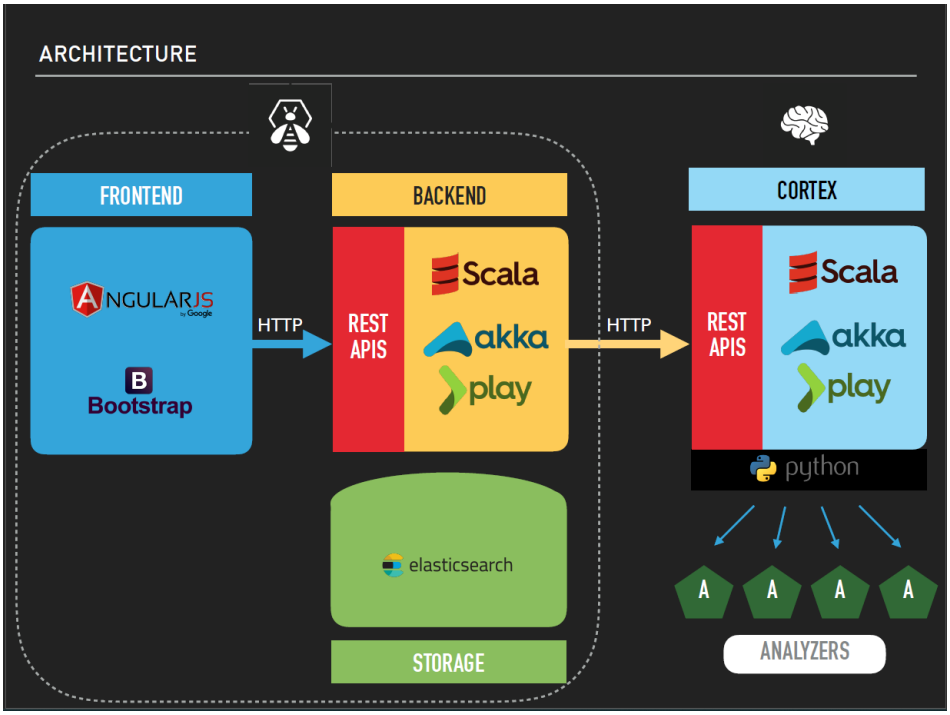
Overview of Features

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



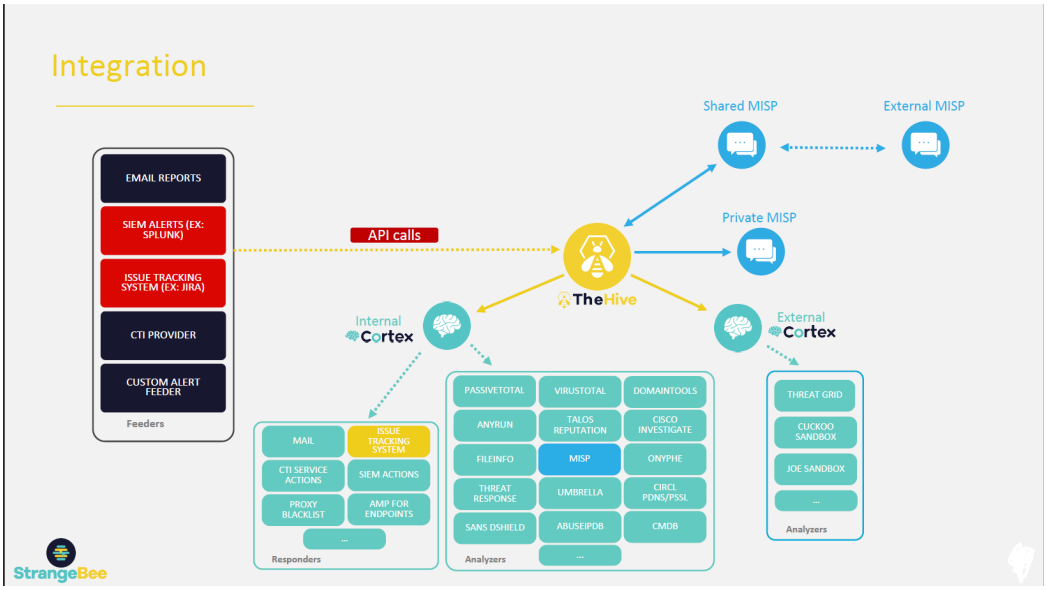
Source: https://chrissanders.org/wp-content/uploads/2017/03/hive_arch-1024x687.png

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_Adouani.pdf

Figure 2.2: The Hive Integration Architecture

The components of the integration architecture are labeled as follows:

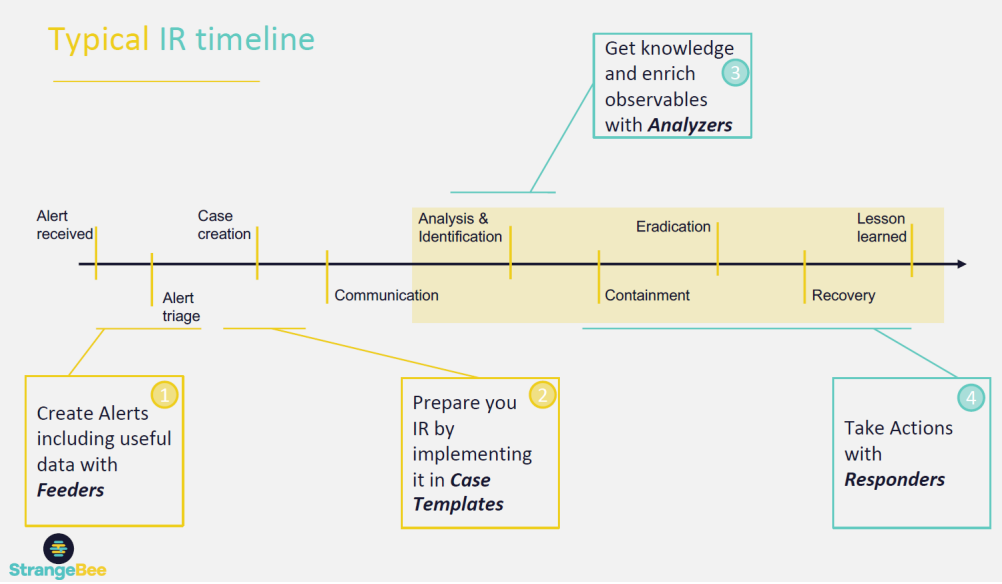
- **Integration:** This component is responsible for collecting data from various sources, such as SIEM alerts, email reports, and CTI providers.
- **Feeders:** This component is responsible for ingesting the data from the Integration component and storing it in the storage layer.
- **Analyzers:** This 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



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

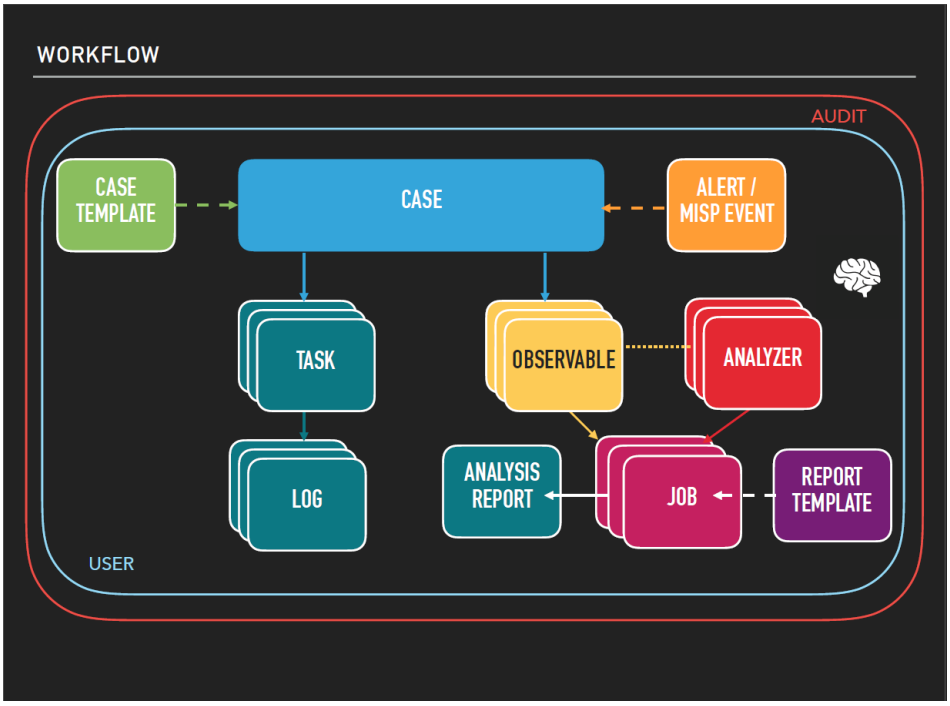
Figure 3.1: Typical Incident Response Timeline

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

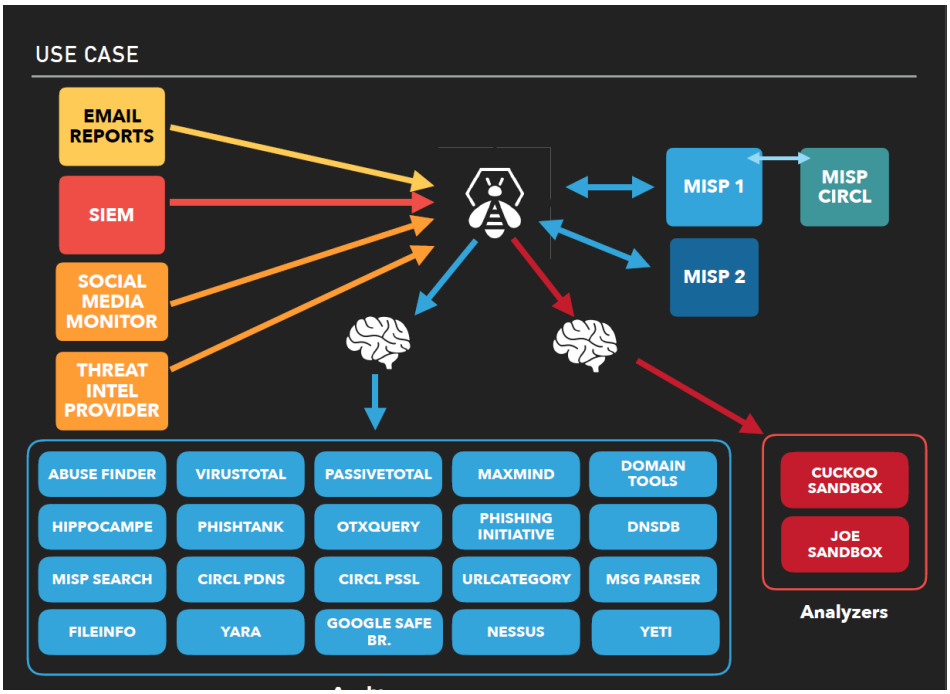
Figure 3.2: The Hive Workflow

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.

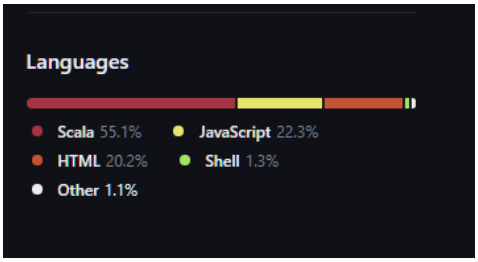


Figure 5.1: Languages Used in The Hive, From Github

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.

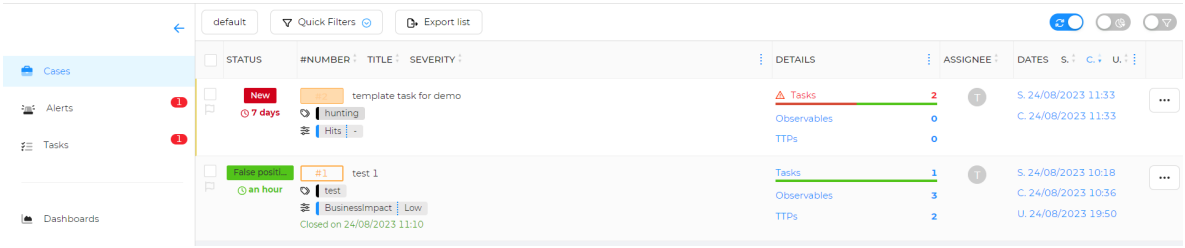


Figure 6.1: Example of Cases

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

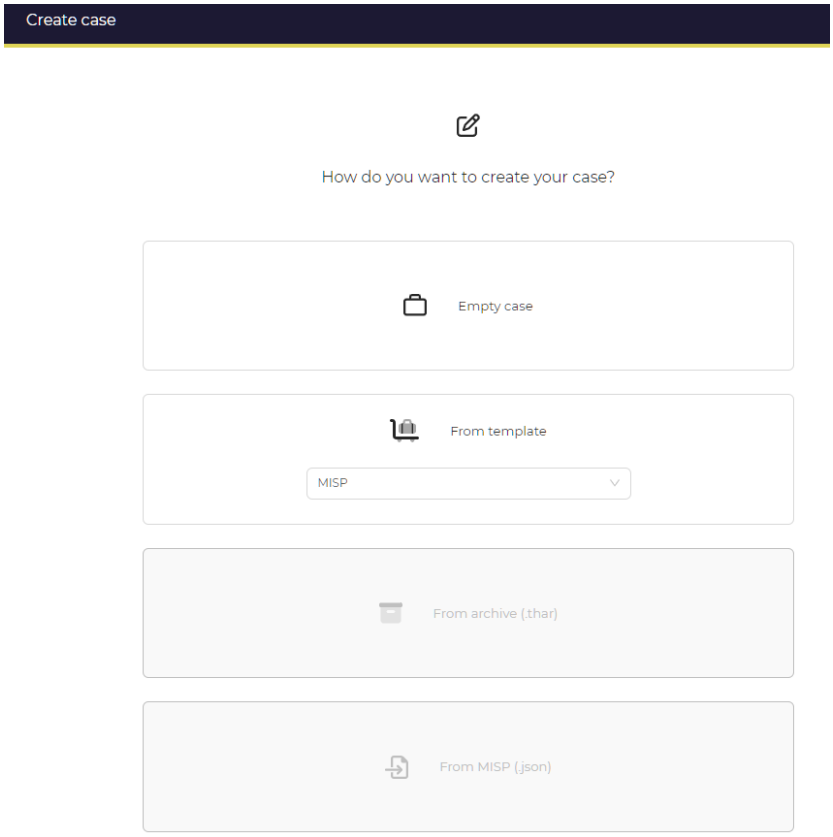


Figure 6.3: Create Case Tab View

6.2.1 Empty Case Creation

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

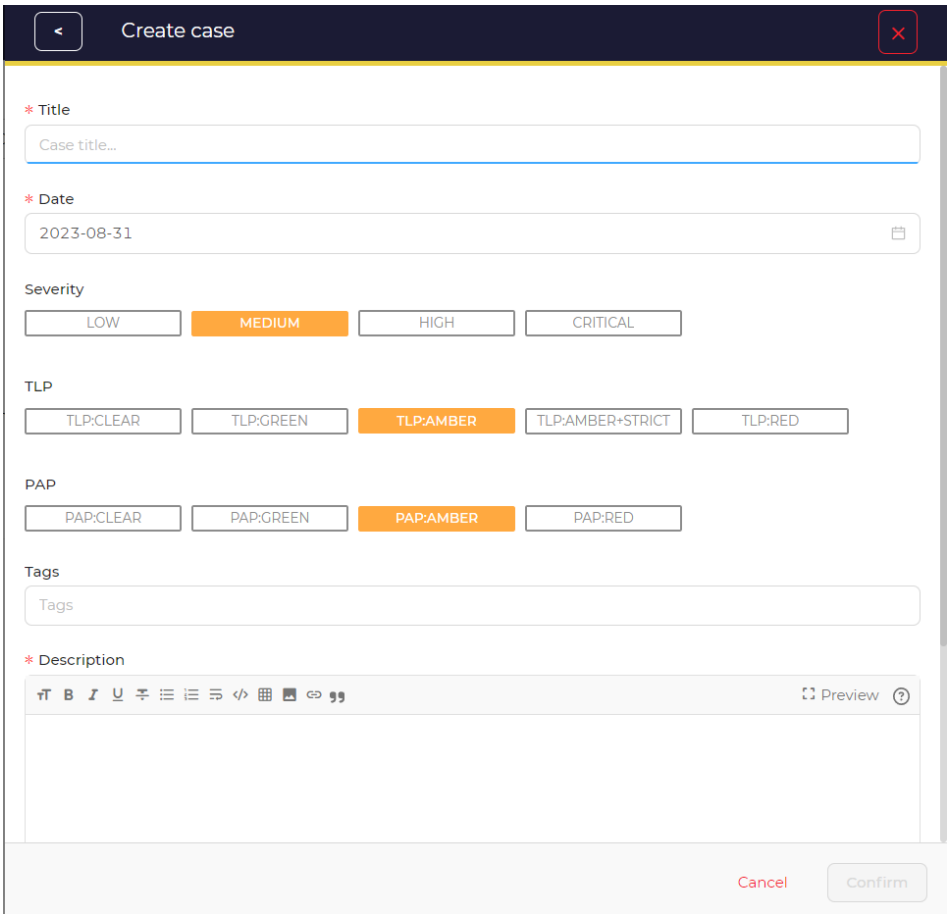


Figure 6.4: Create Empty Case

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.

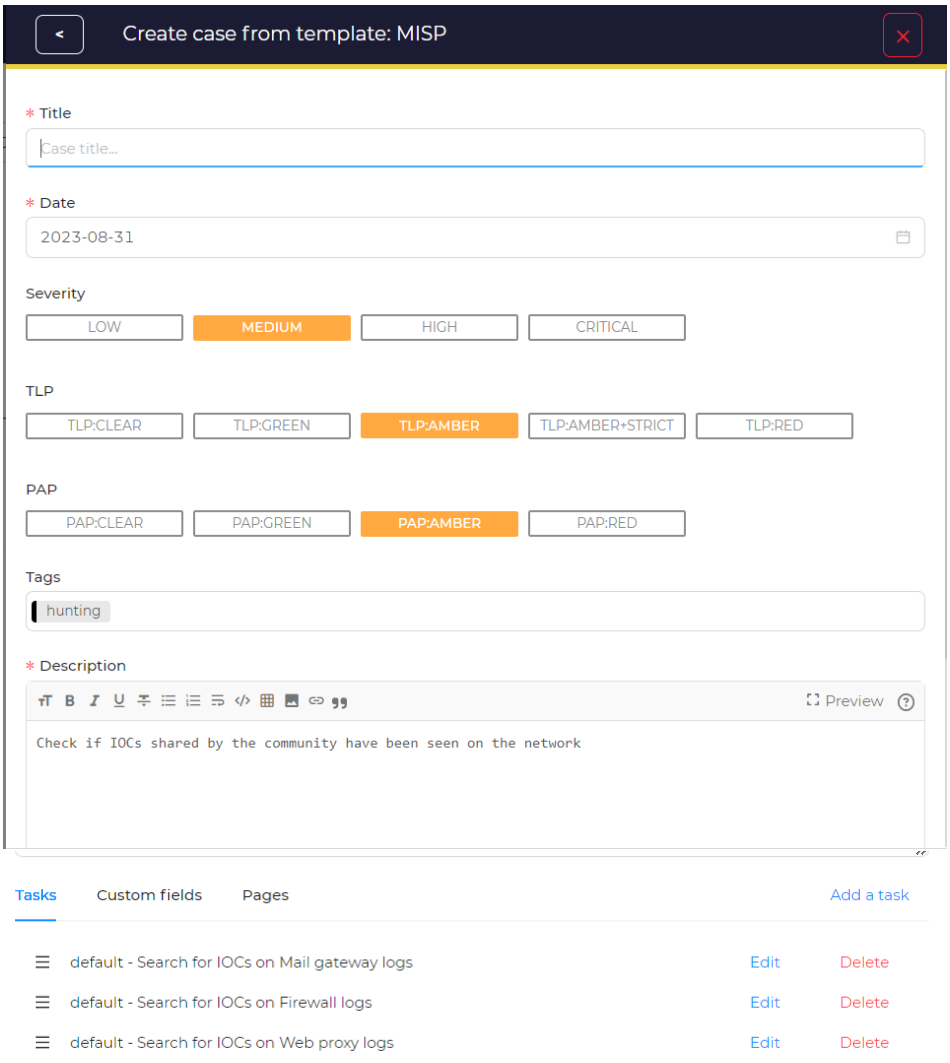


Figure 6.5: Create Case from MISP

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

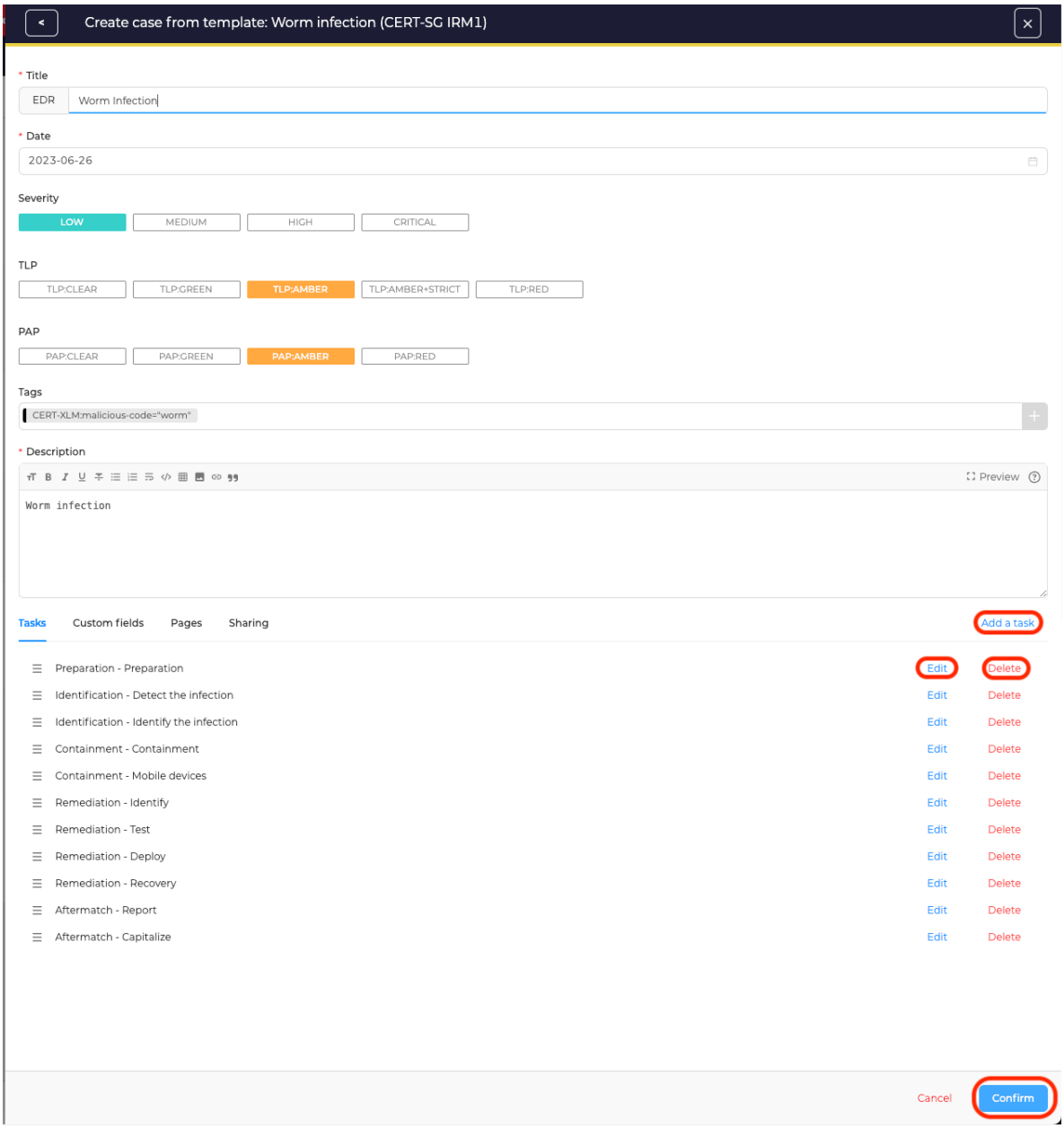


Figure 6.6: Create Case from EDR

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.

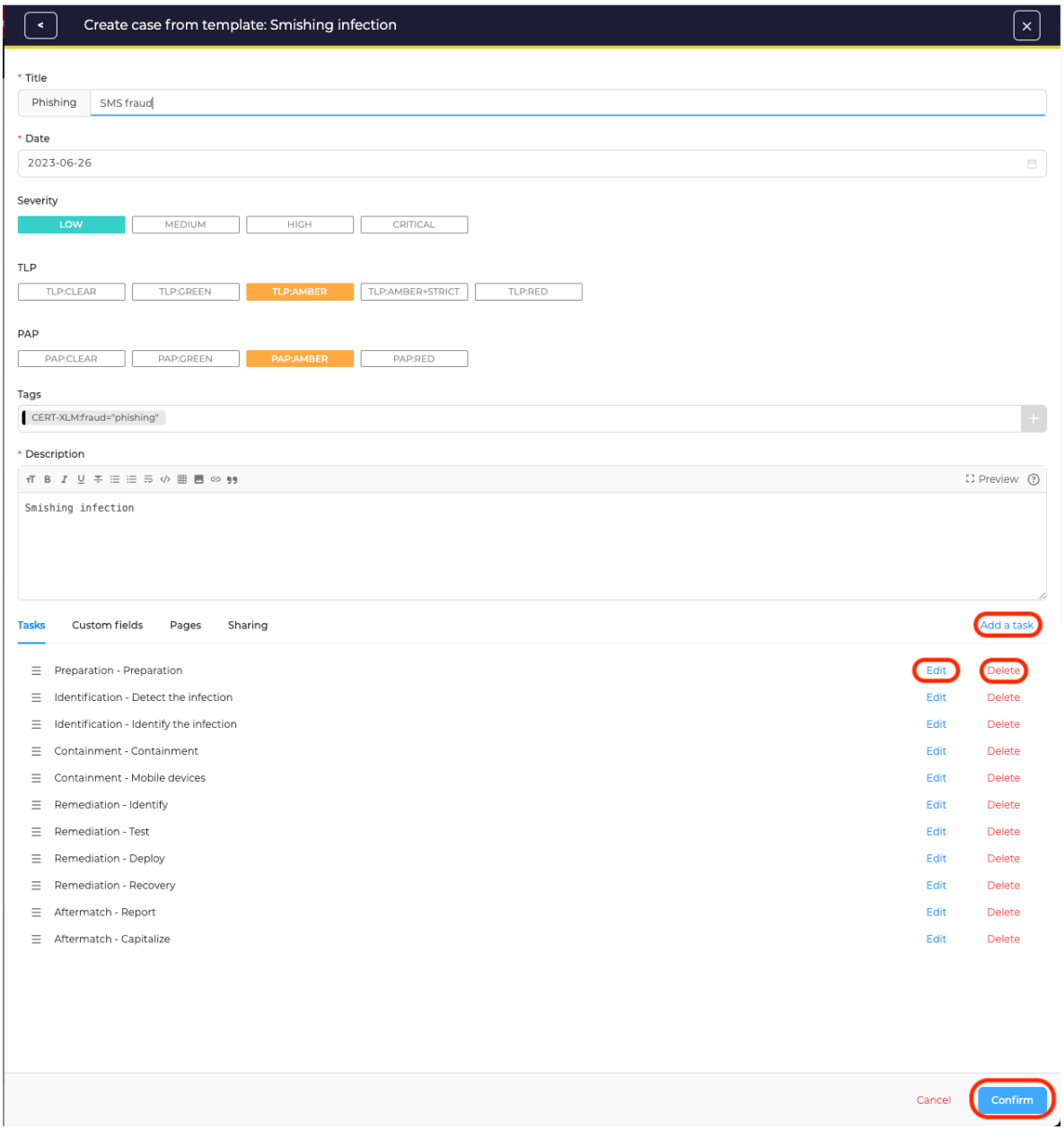


Figure 6.7: Create Case from Phishing Template

6.2.5 Apply Case template

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

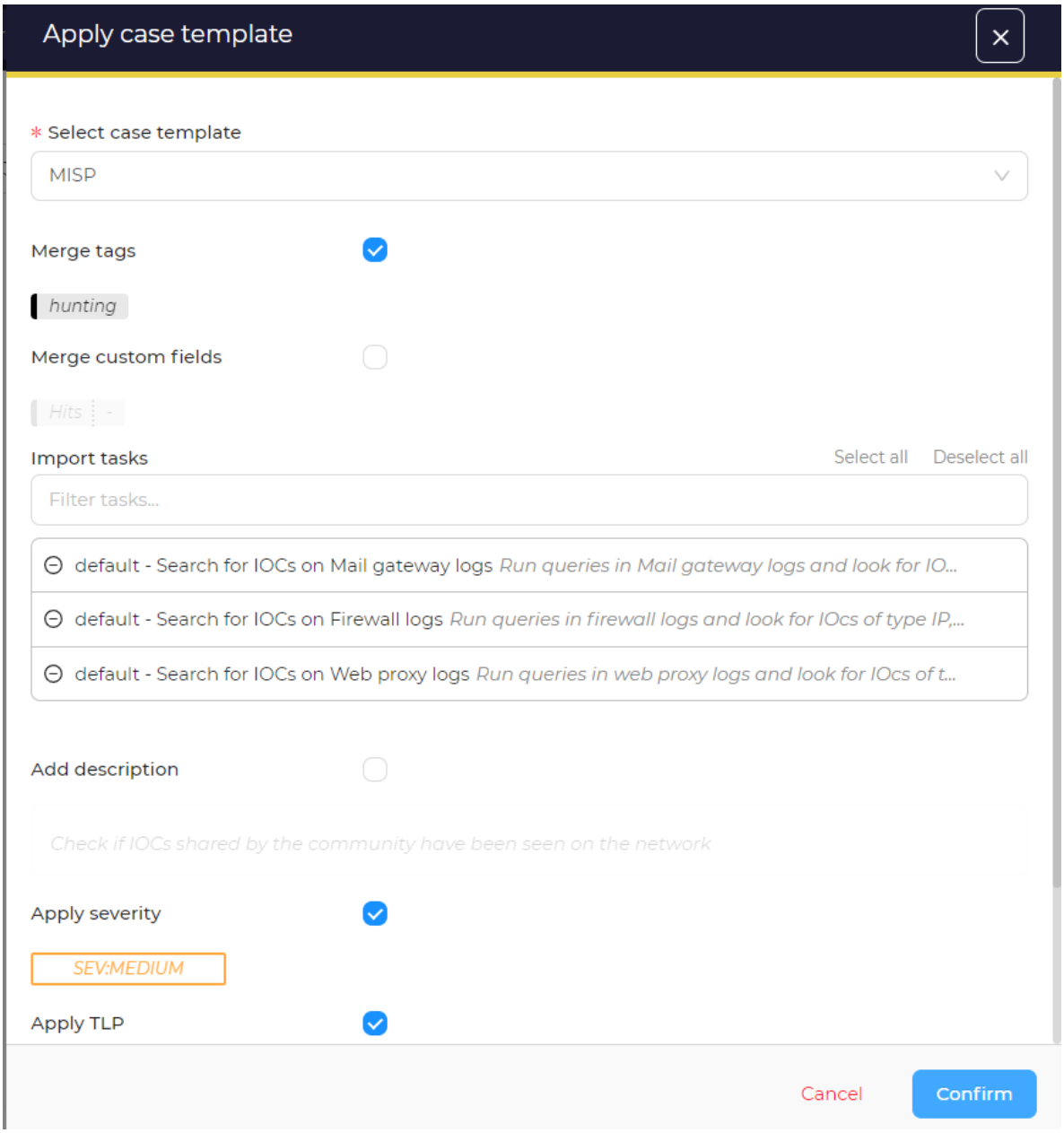


Figure 6.8: Apply template to case

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

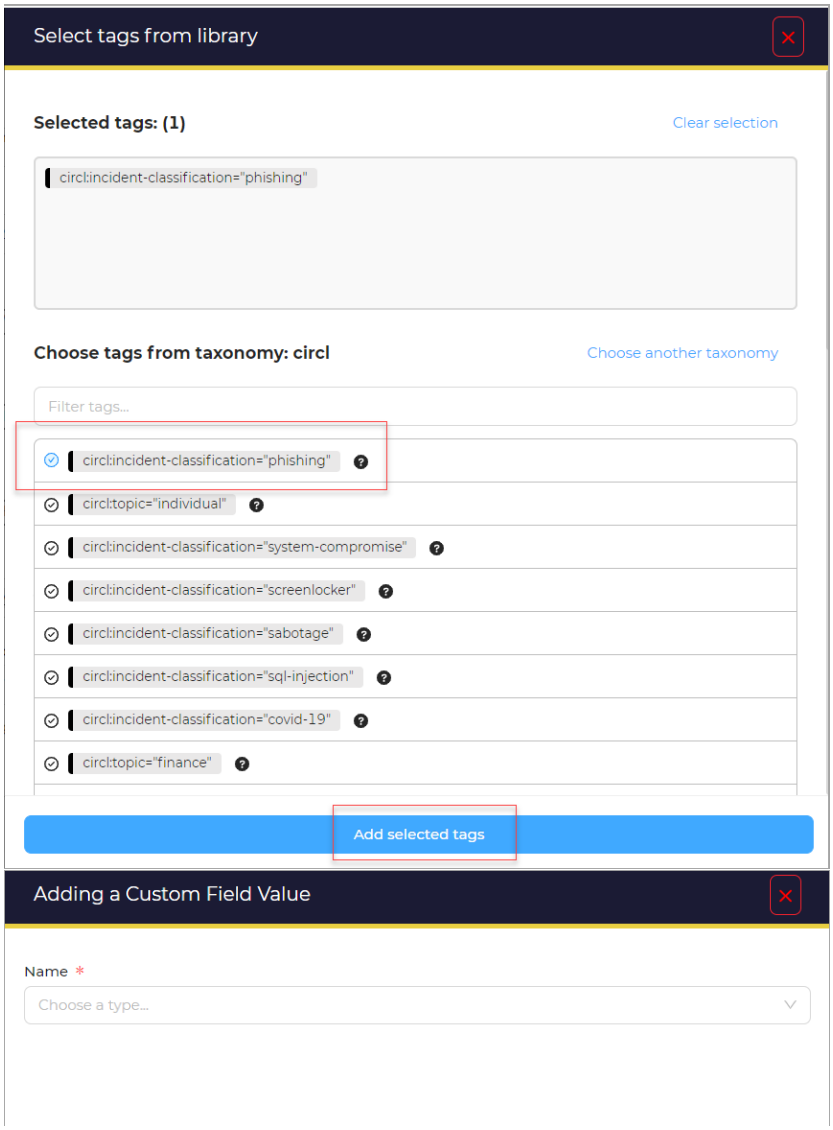


Figure 6.9: Addition of tags and custom field value on cases

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

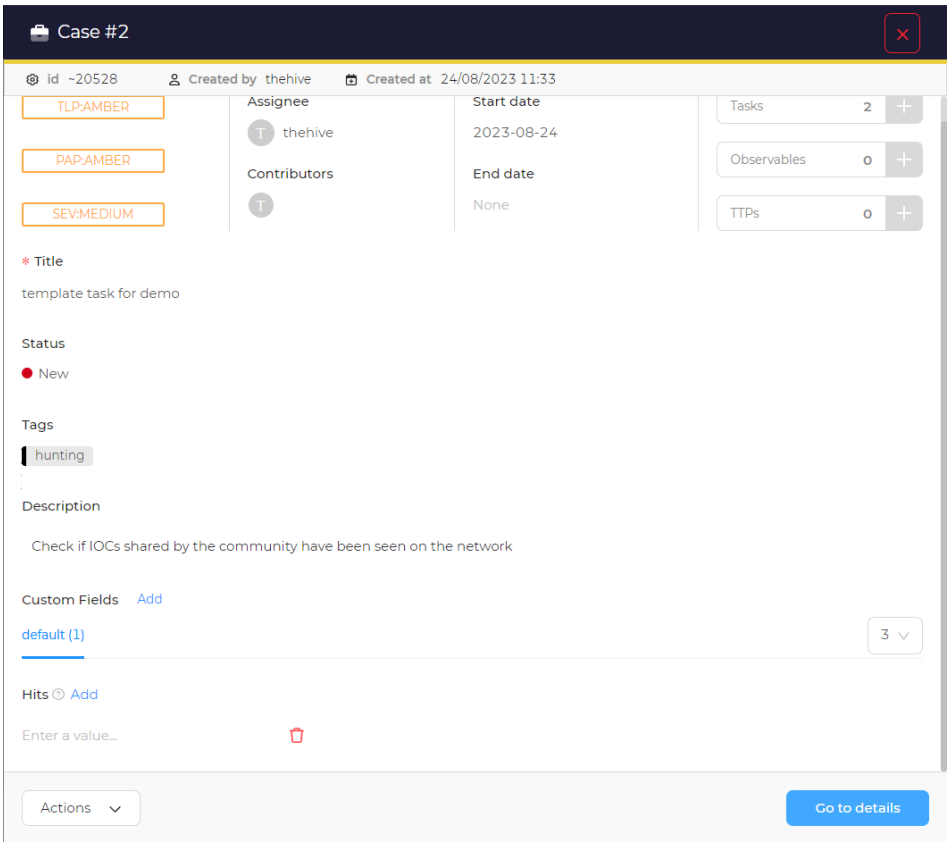


Figure 6.10: Case Preview

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.

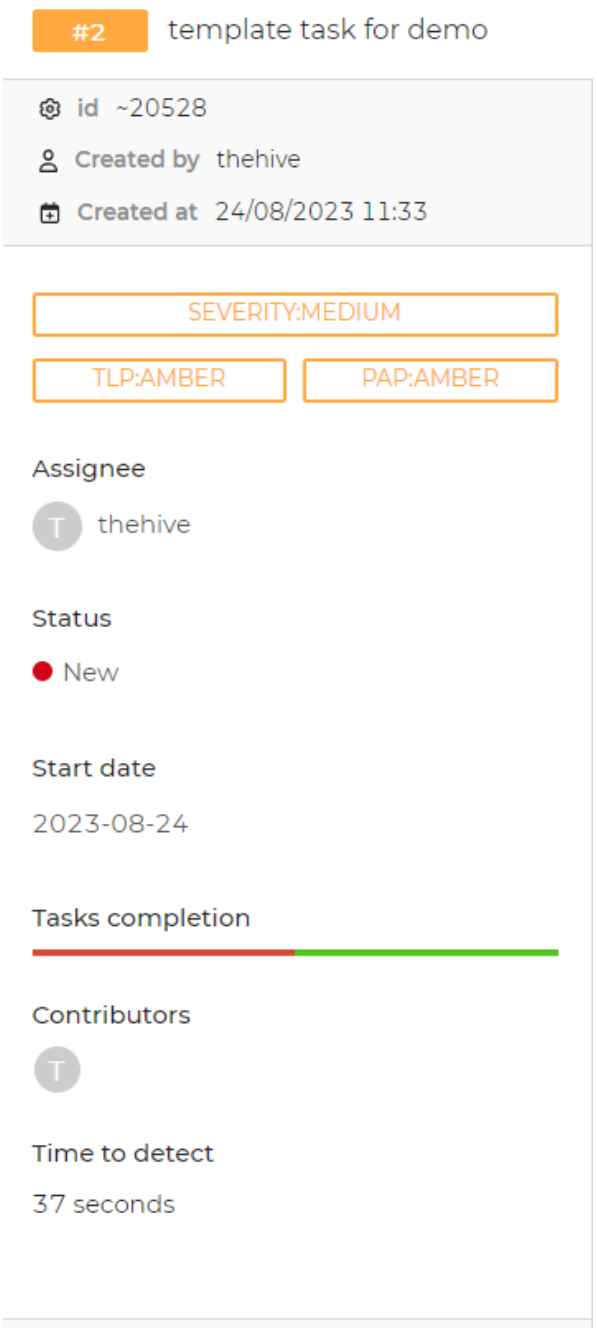


Figure 6.11: Left Side Pane of Case Details

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

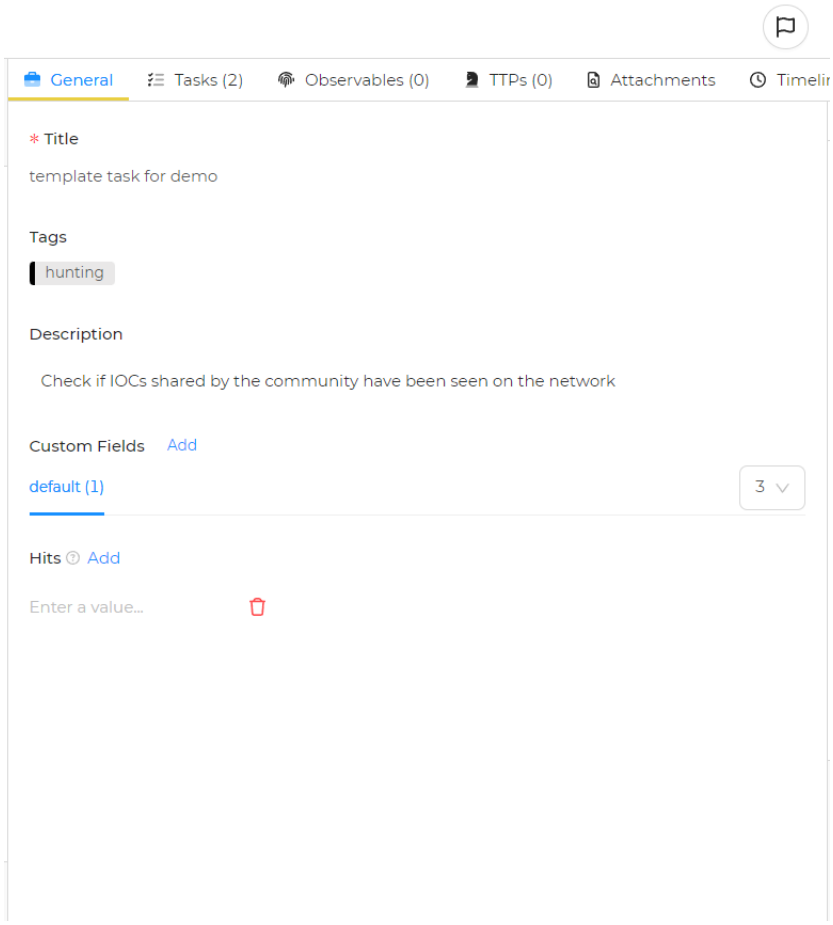


Figure 6.12: Case Details

6.4.4 Tasks Tab

The details of this section fully explained in Chapter Tasks

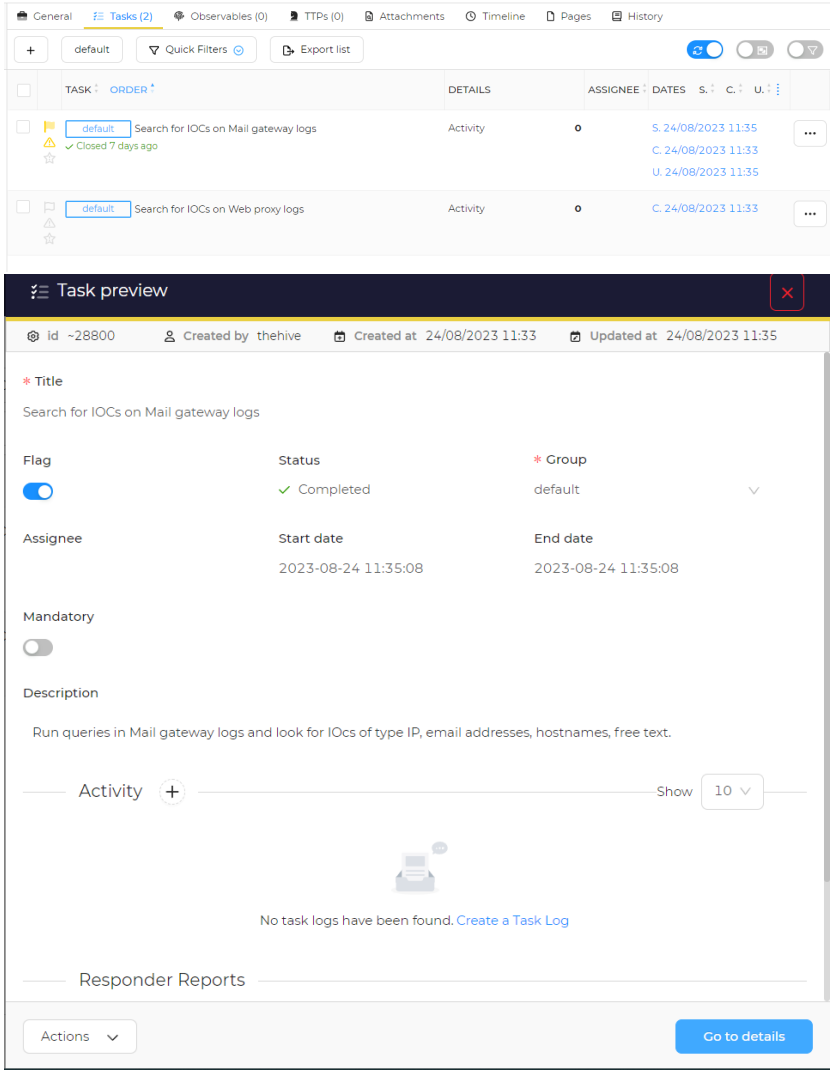


Figure 6.13: Task view on cases

6.4.5 Observables Tab

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

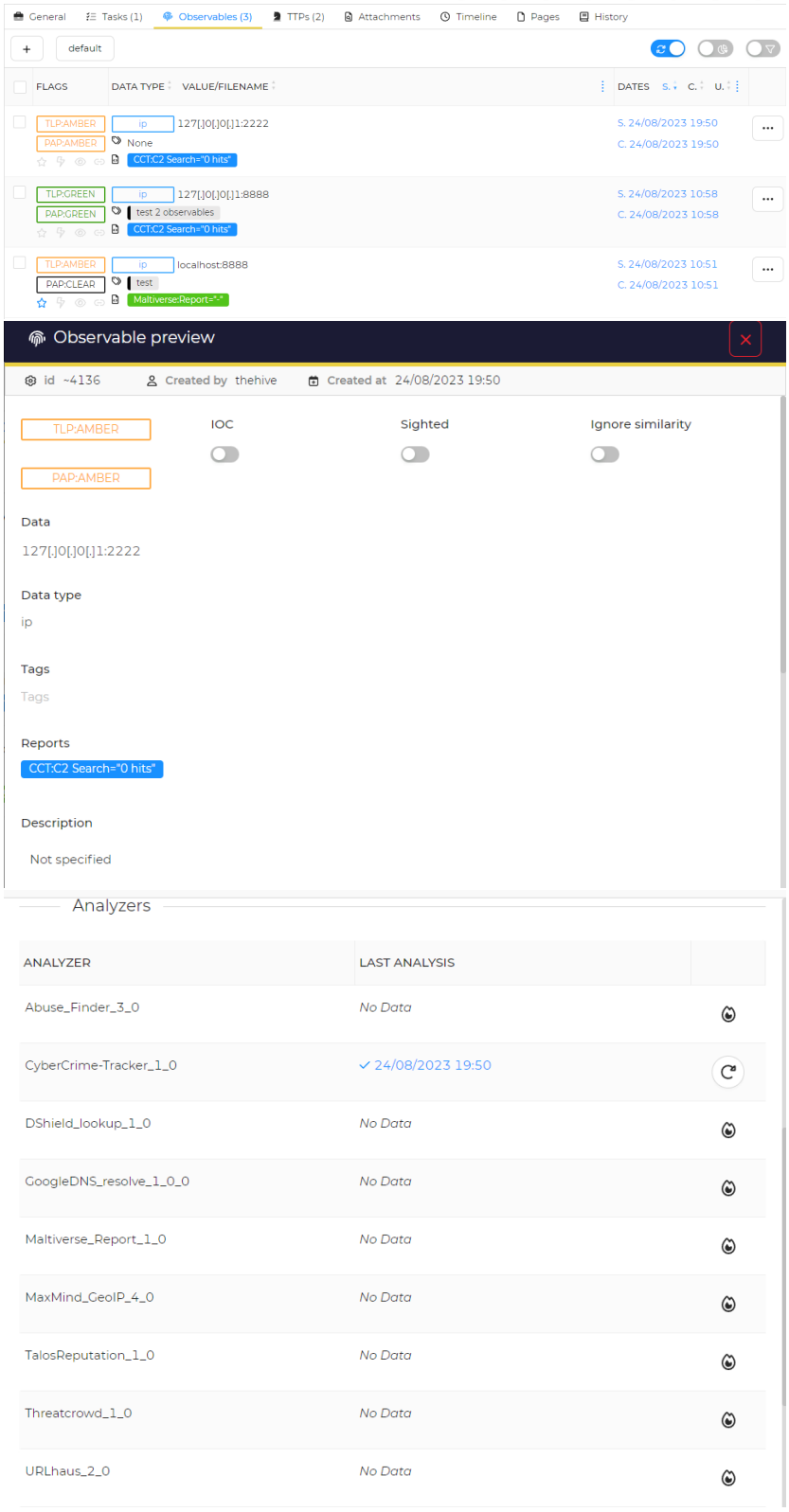


Figure 6.14: Observables and Analyzers view on cases

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.

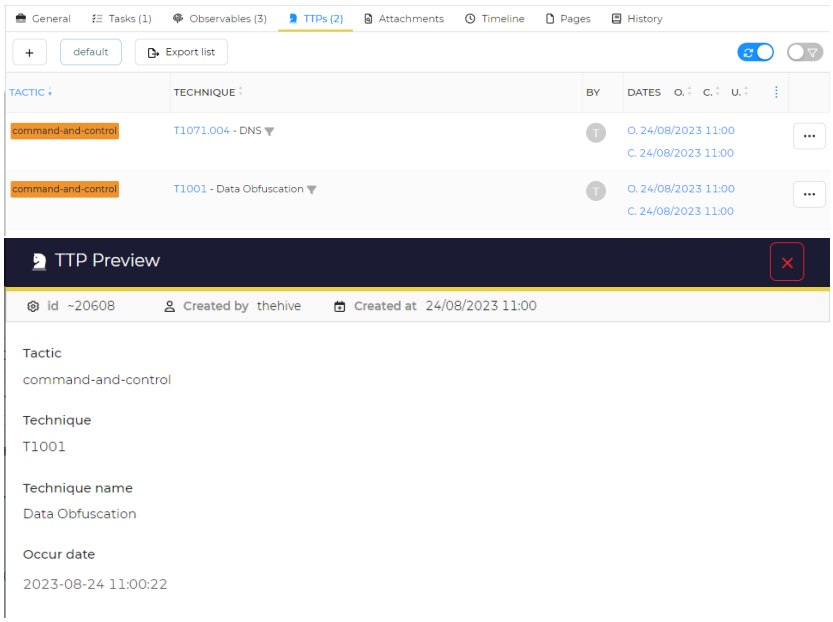


Figure 6.15: TTPs Preview and Details

Operations

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

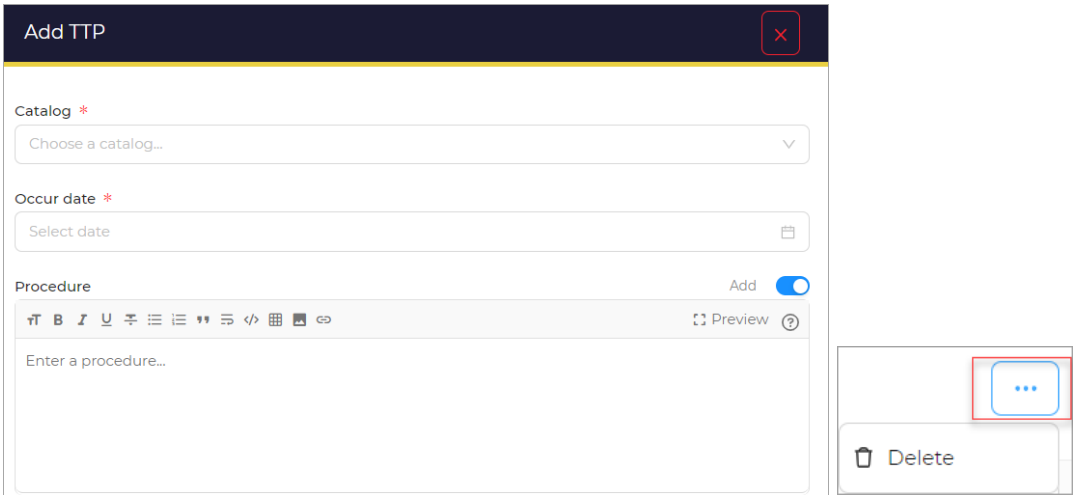


Figure 6.16: TTPs Addition and Deletion

6.4.7 Attachments Tab

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

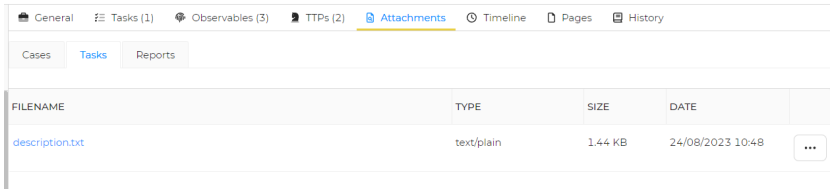


Figure 6.17: Attachment to cases

6.4.8 History

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

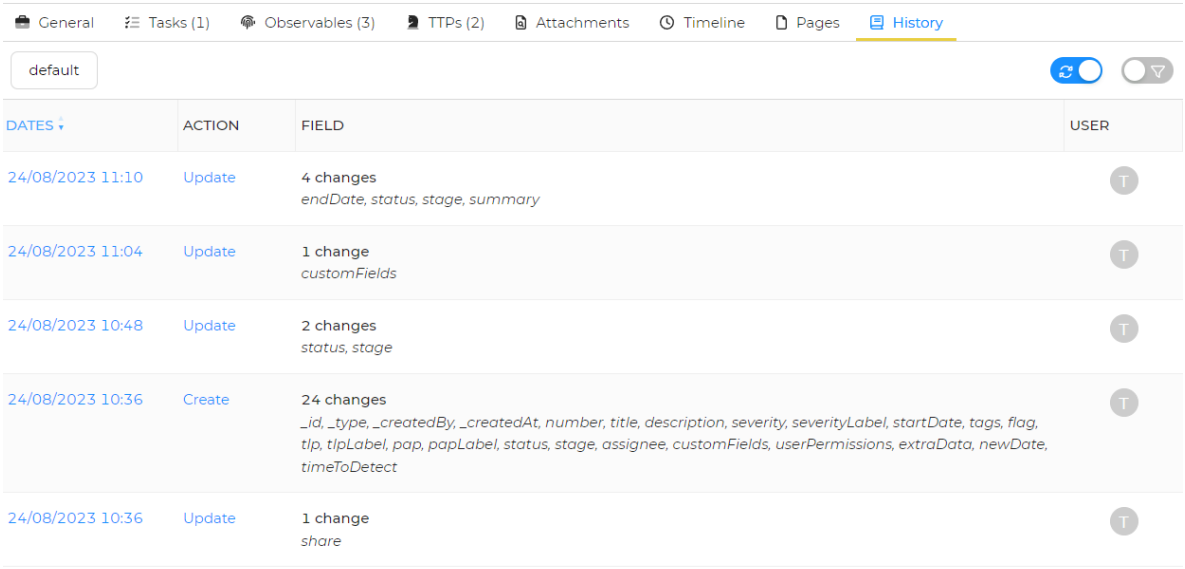


Figure 6.18: History of a case

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

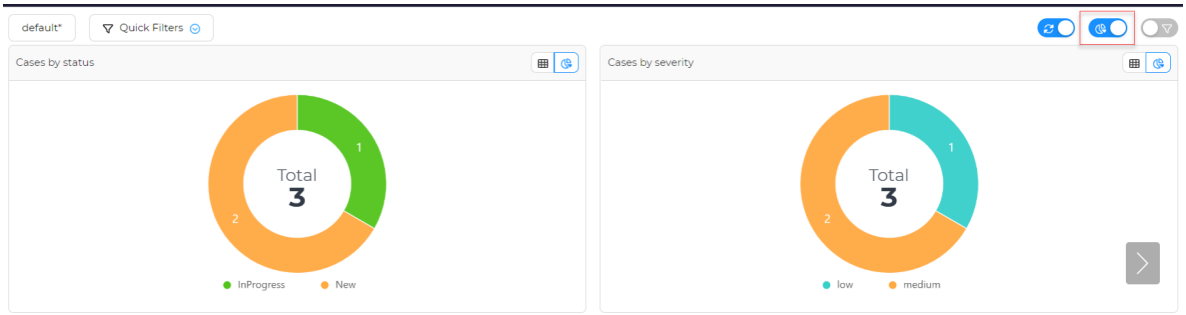


Figure 6.19: Case Statistics

6.5.2 Filtering and Sorting

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

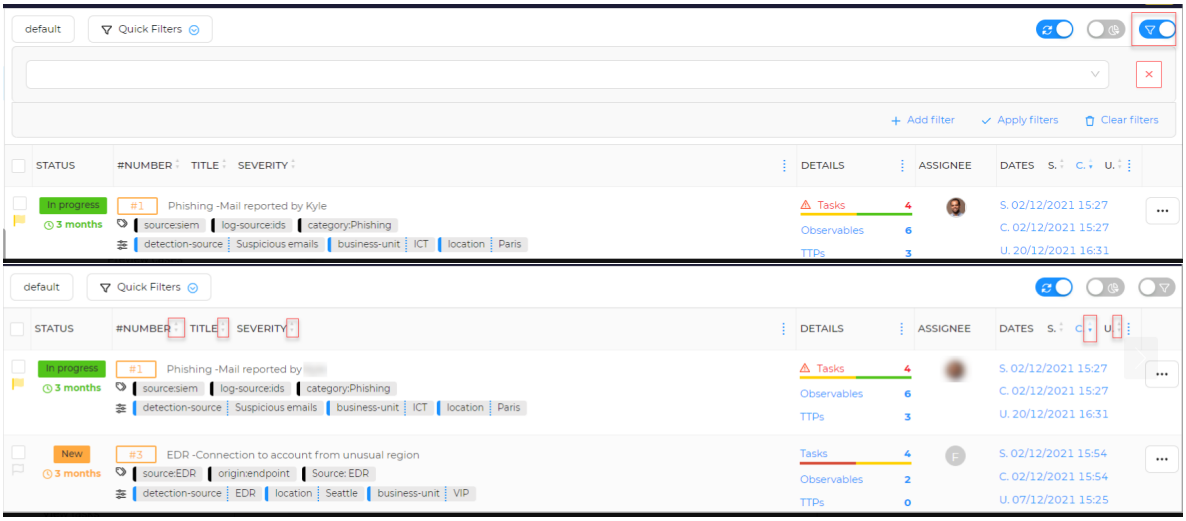


Figure 6.20: Case Filtering and Sorting

6.5.3 Flag a Case

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

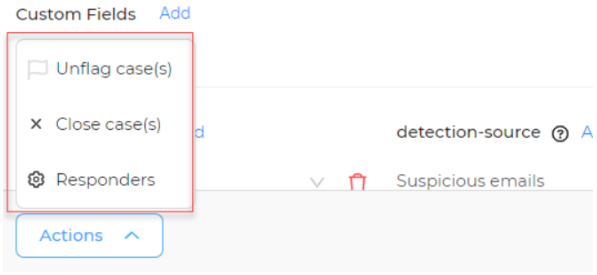


Figure 6.21: Case Flagging

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

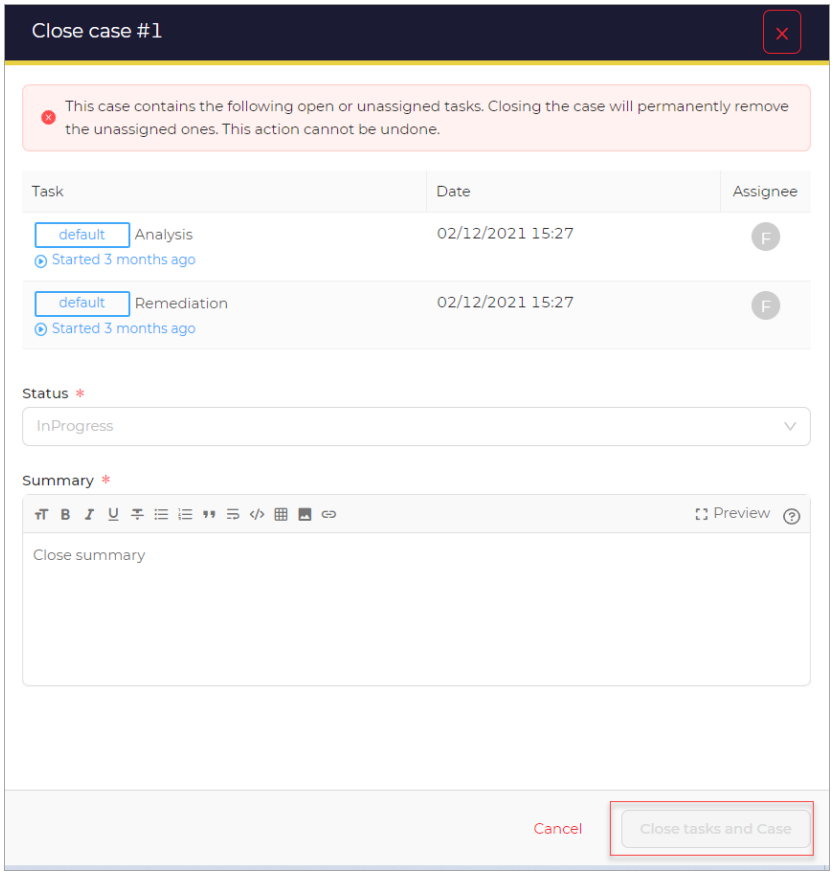


Figure 6.22: Closing cases

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.

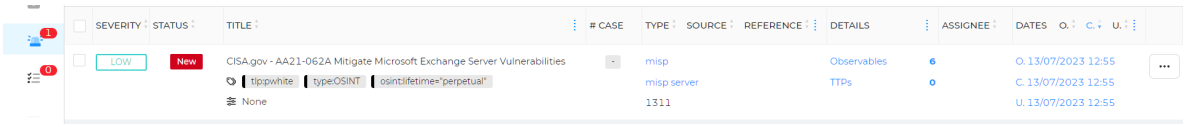


Figure 7.1: An Example of An Alert

7.2 Details of an alert

Clicking on an alert shows more details about it.

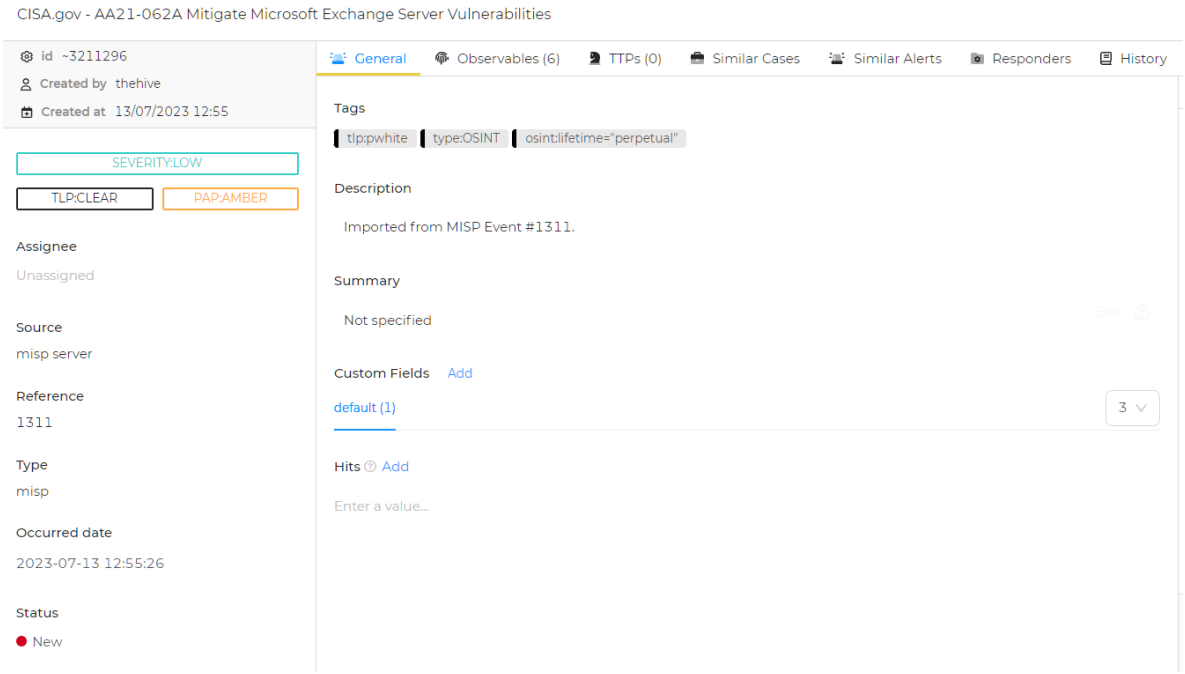
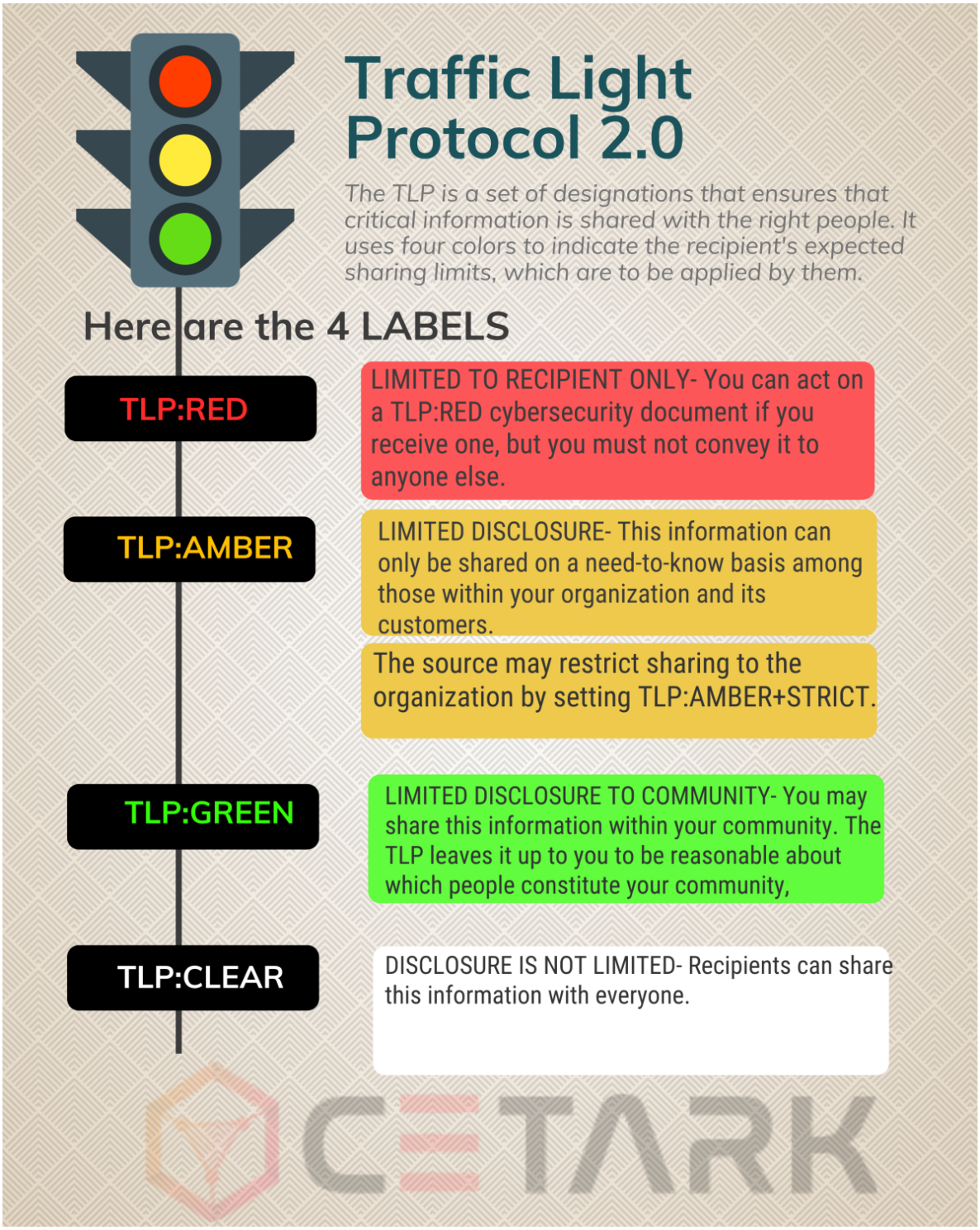


Figure 7.2: An Example of An Alert

7.2.1 Left Side View

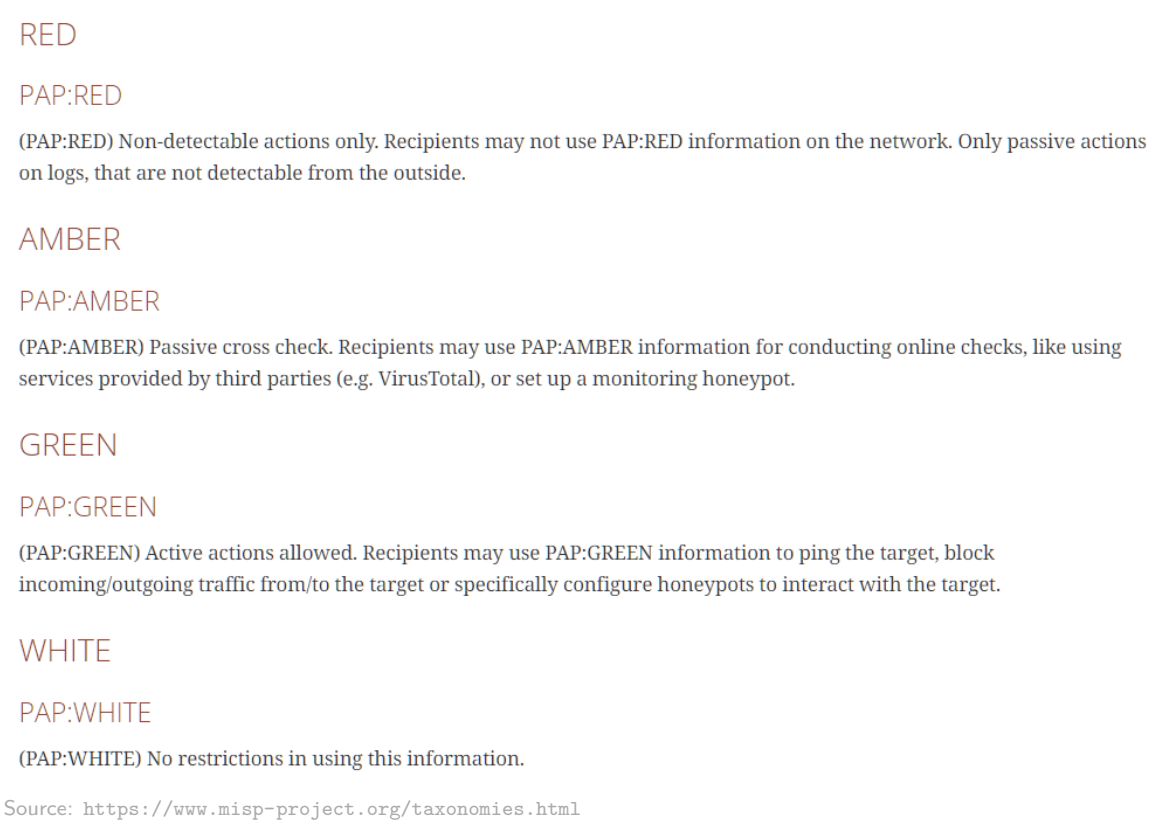
The left side pane shows general information about the alert. When it was created, its source, its severity, TLP (Traffic Light Protocol) and PAP(Permissible Actions Protocol). Details about TLP and PAP are given in the figure 7.4 and 7.5 respectively. It also contains a field called Assignee to assign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

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

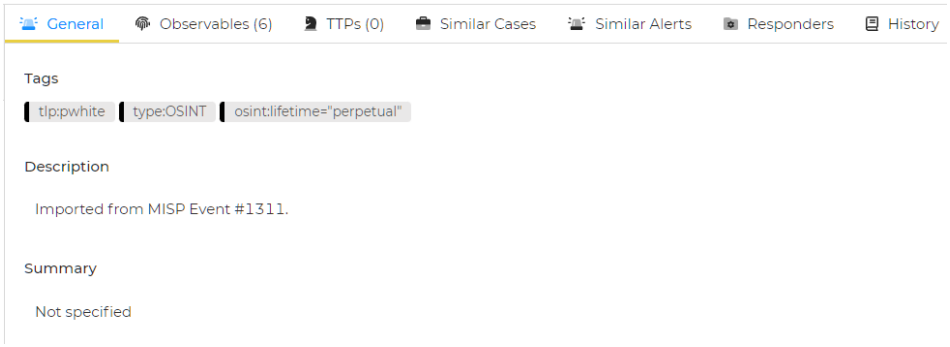


Figure 7.6: General Tab

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,

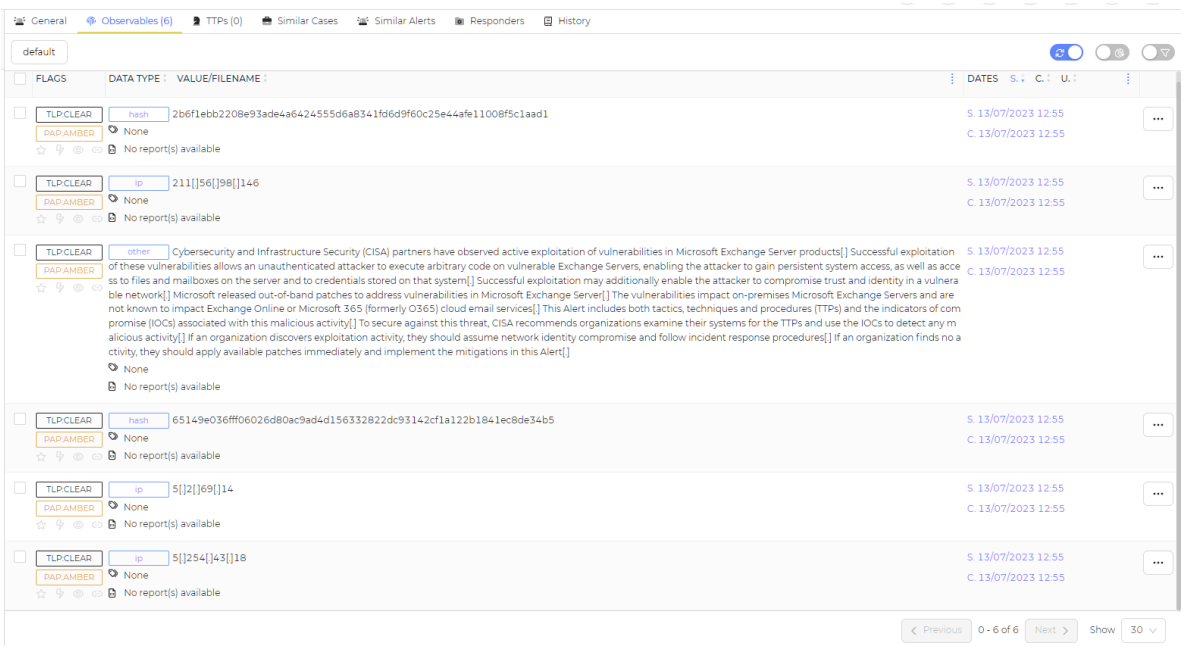


Figure 7.8: Observables Tab

We can click on an observable to view its details

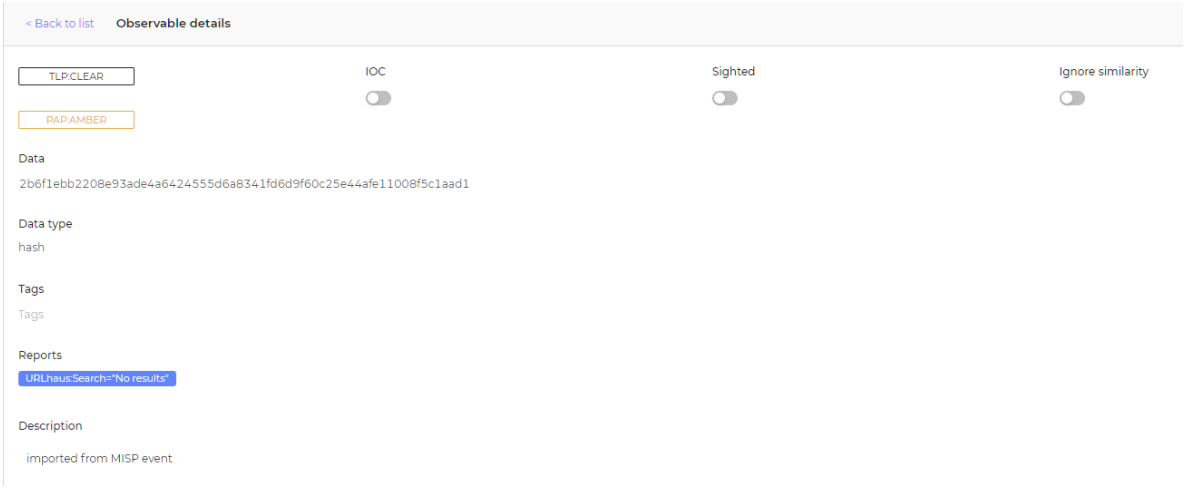


Figure 7.9: Details on an observable

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

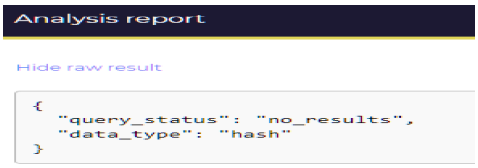


Figure 7.10: Report of an analysis

The continuation of figure 7.9 is shown in 7.11

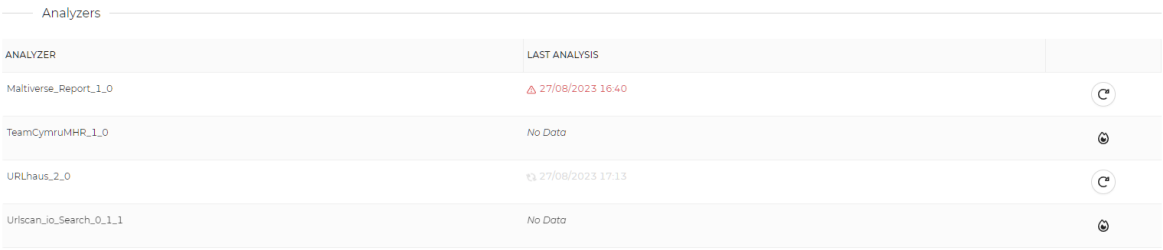


Figure 7.11: Run analyzer on observables

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.

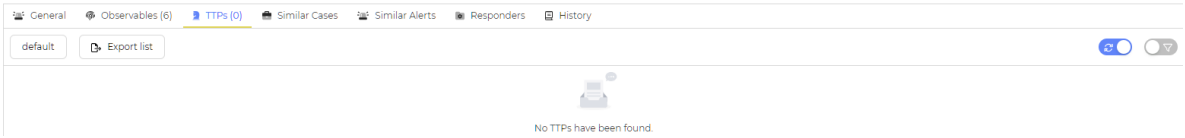


Figure 7.12: TTPs Tab

7.2.5 Similar Cases

This tab contains similar cases if any found

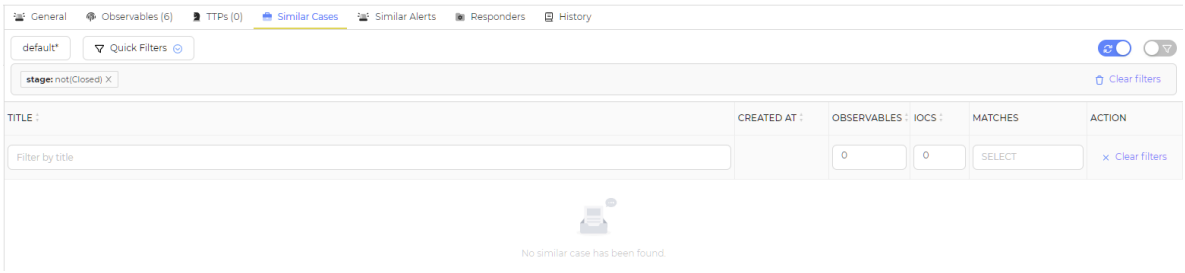


Figure 7.13: Similar Cases Tab

7.2.6 Similar Alerts

This tab contains similar alerts if any found

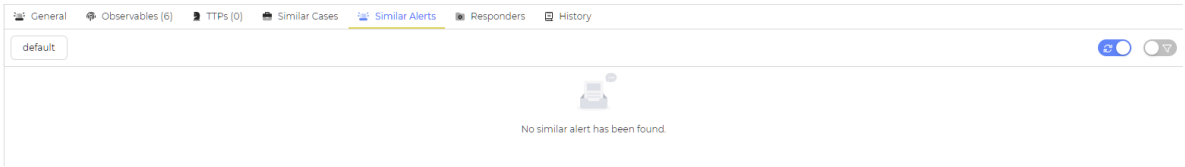


Figure 7.14: Similar Alerts Tab

7.2.7 Responders

This tab contains reports from responders if any available

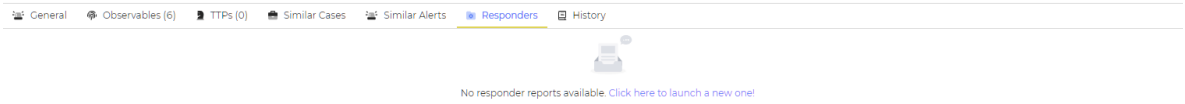


Figure 7.15: Responders Tab

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.

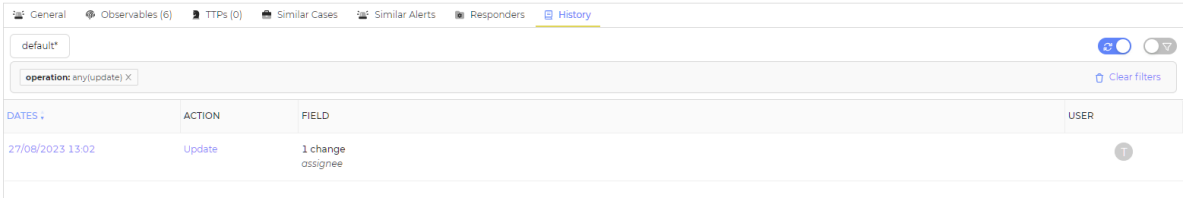


Figure 7.16: History Tab

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

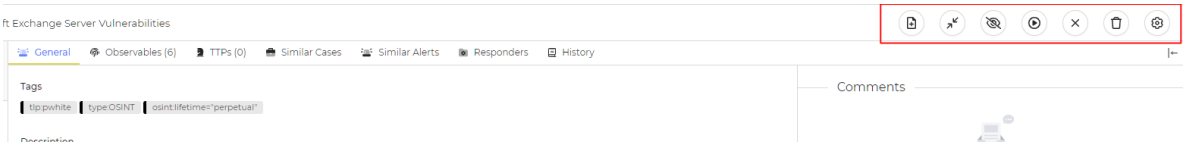


Figure 7.17: Actions Menu in Details View

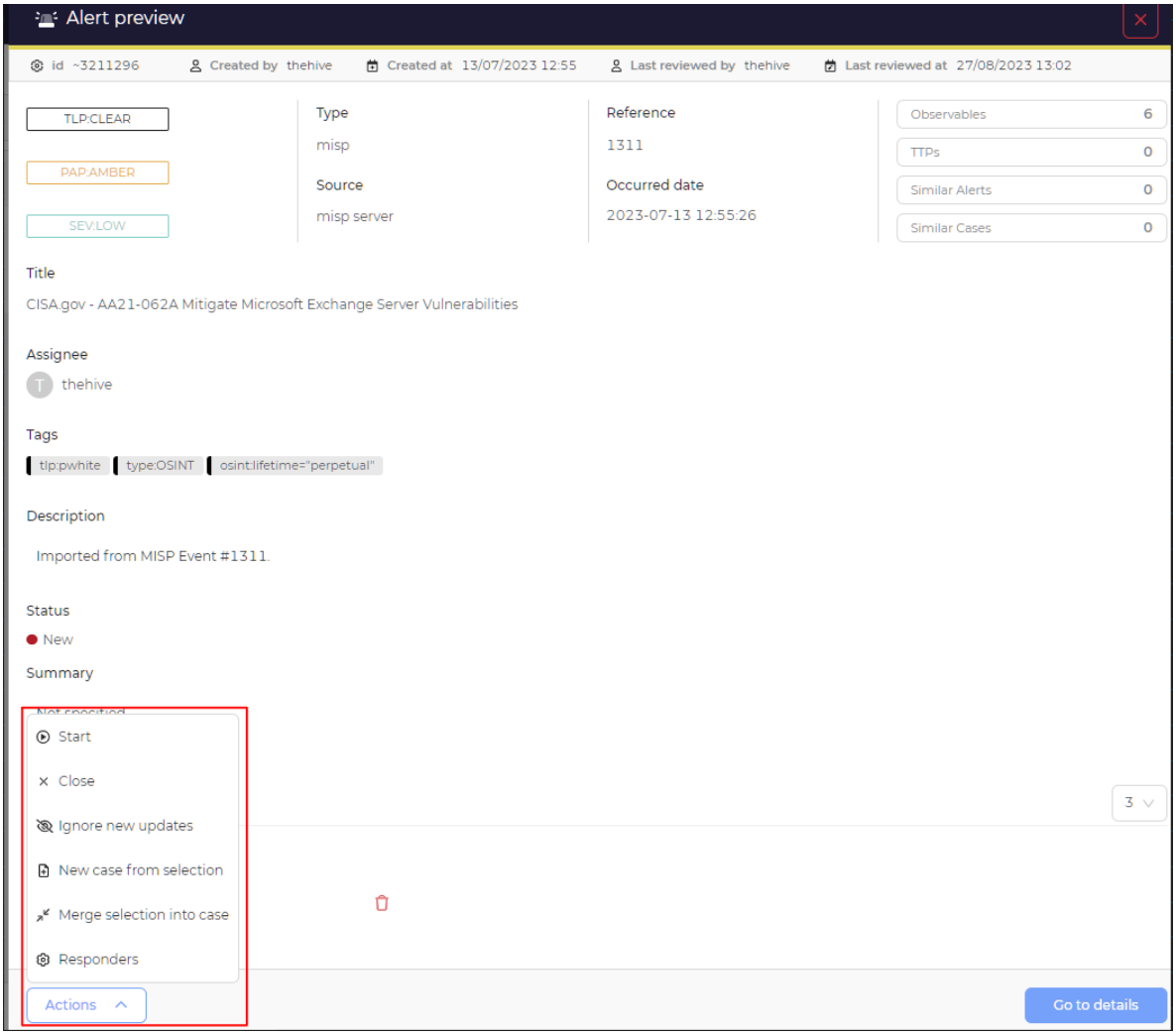


Figure 7.18: Actions Menu in Preview

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 assing users to this alert.

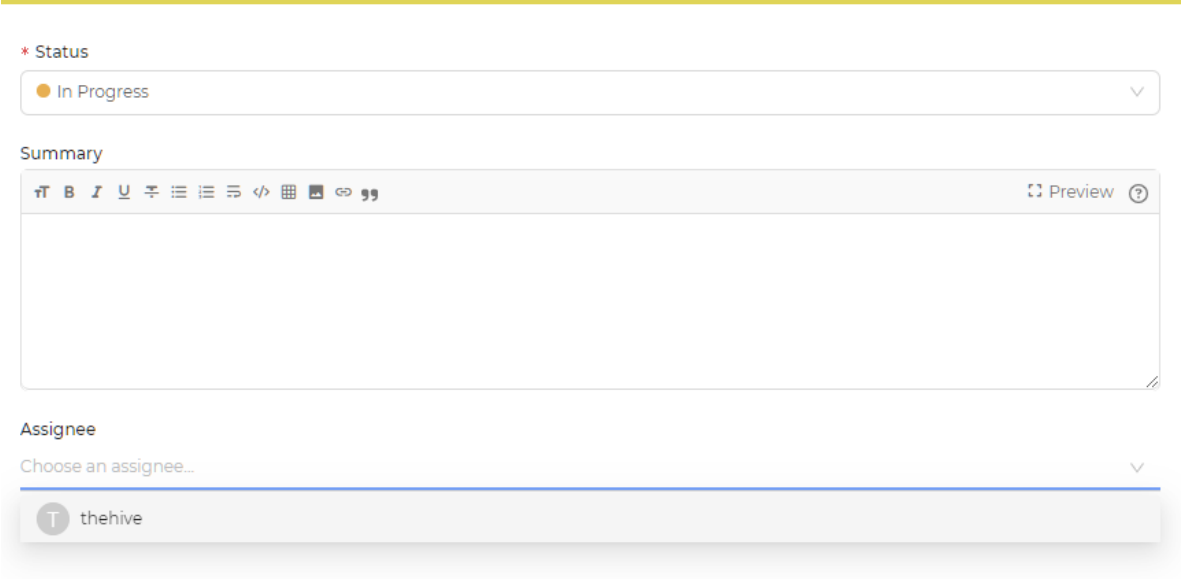


Figure 7.19: Start Alert

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.

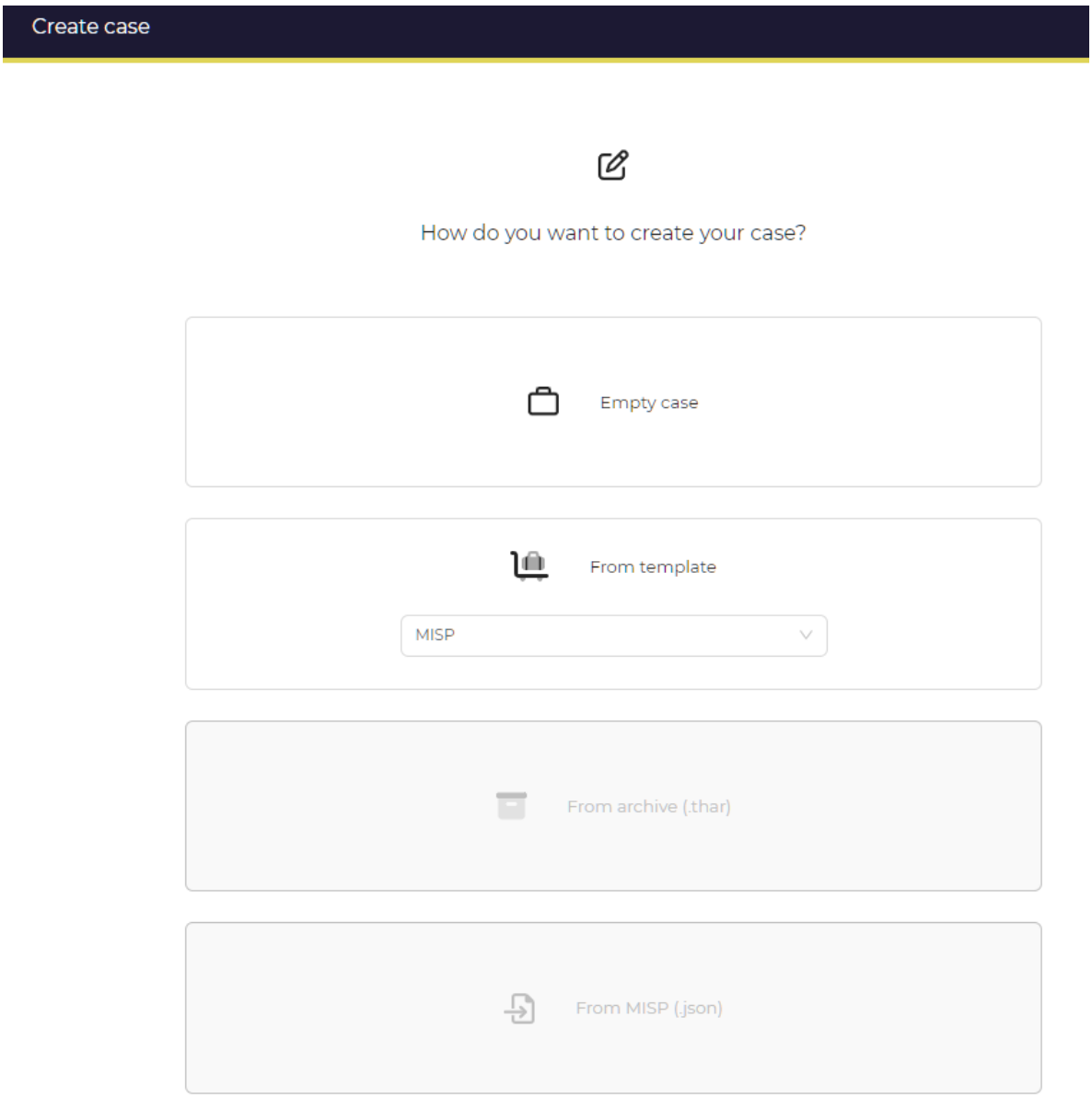


Figure 7.20: Create Case From Alert

Choosing empty case takes to 7.21

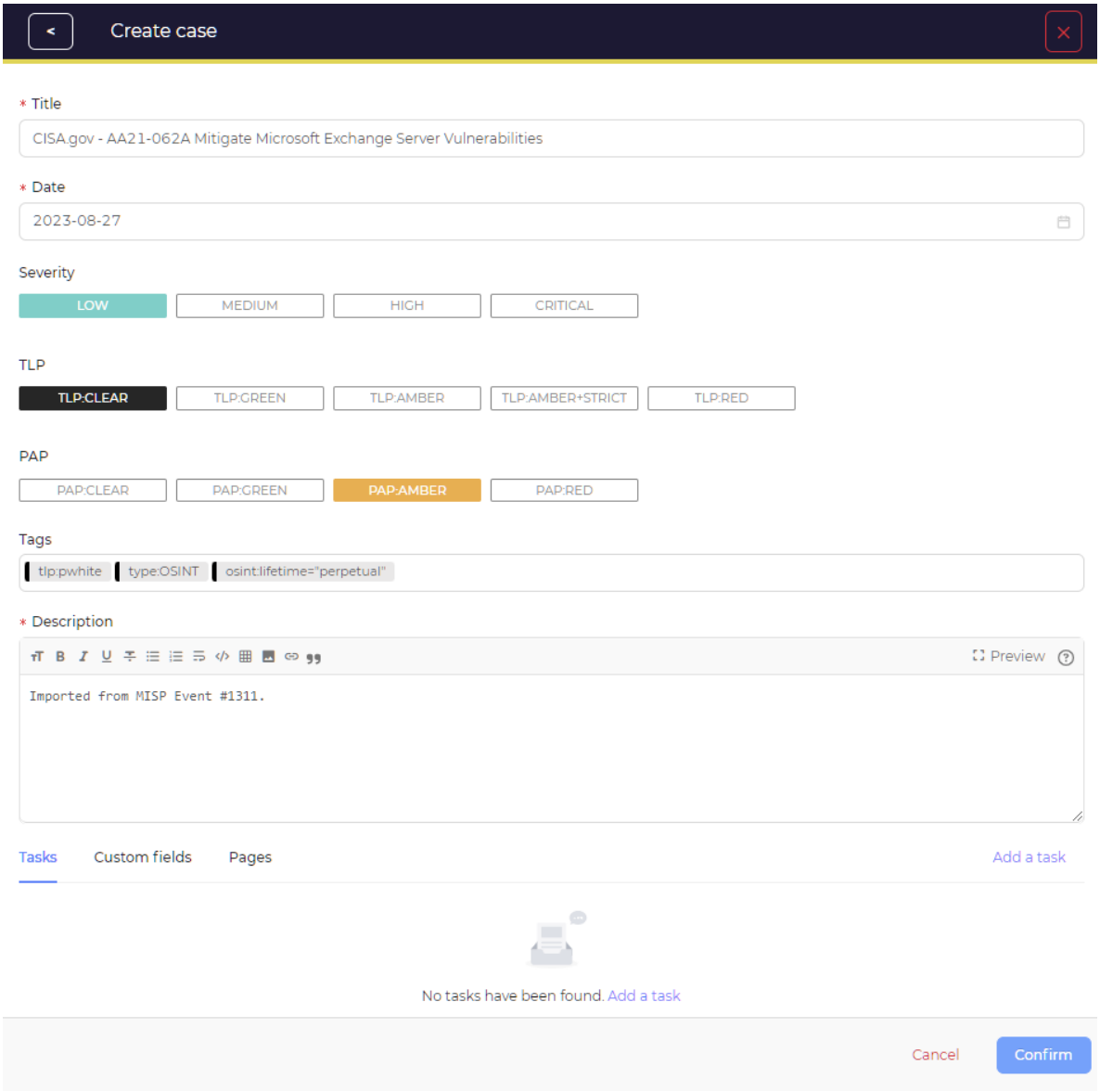


Figure 7.21: Create Empty Case From Alert

7.3.5 Merge selection into case

Merge alert into an exisiting 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.

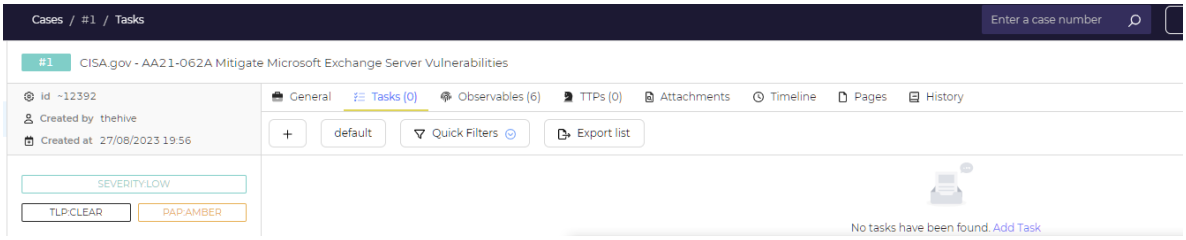


Figure 8.1: Creating Task

Clicking on the plus icon show 8.2 on the right.

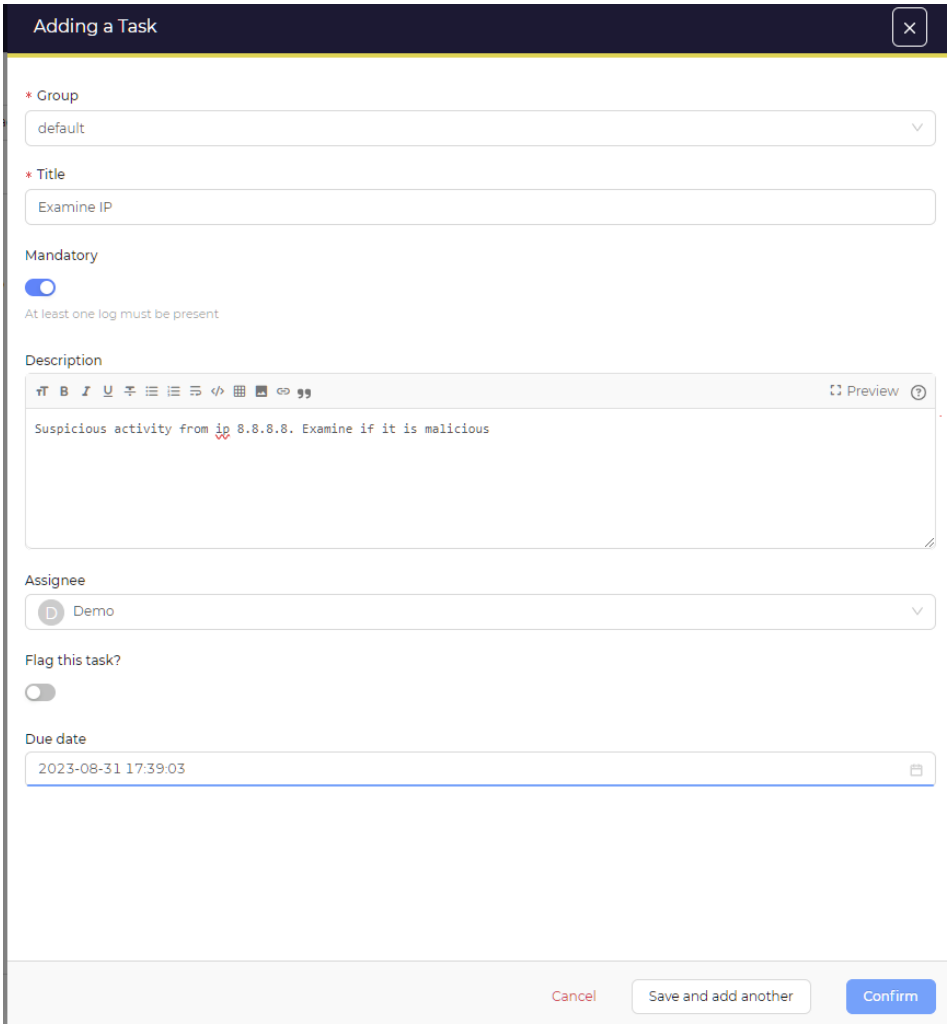


Figure 8.2: Creating Task

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.

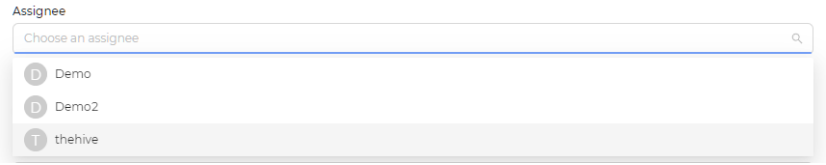


Figure 8.3: Creating Task

8.3 Viewing Tasks

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

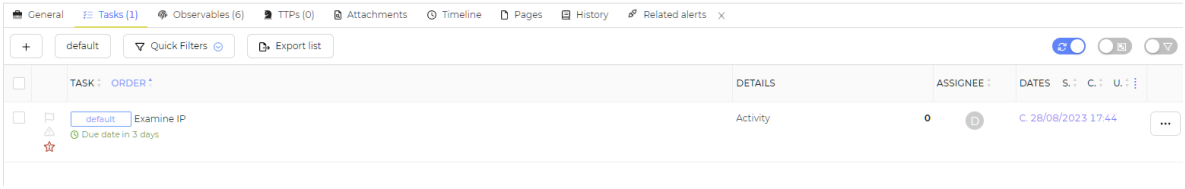


Figure 8.4: Task List

Clicking on a task shows its details

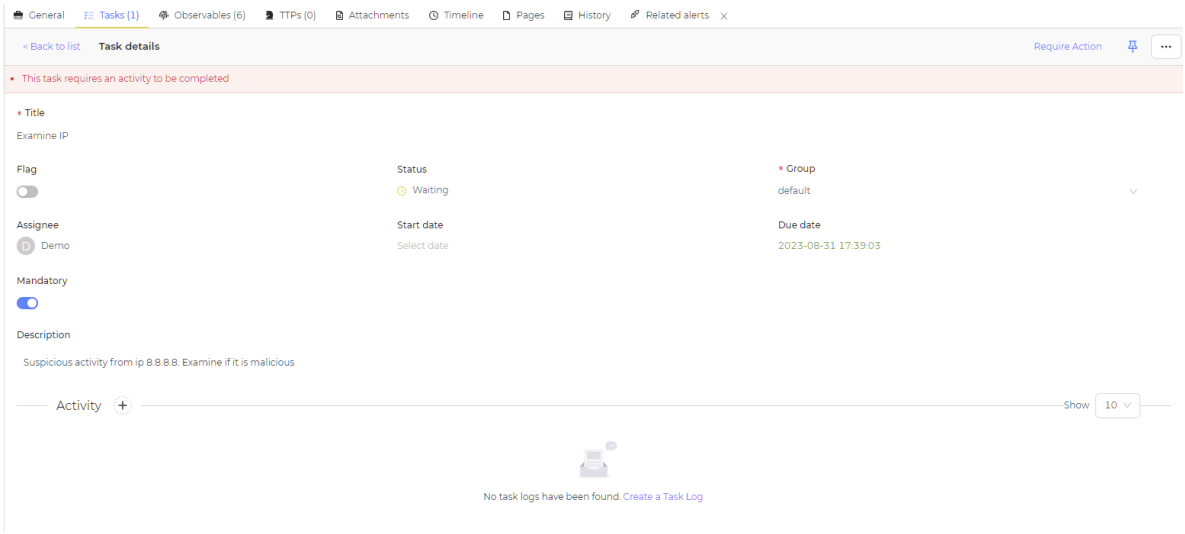


Figure 8.5: Details of a Task

8.4 Actions on a Task

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

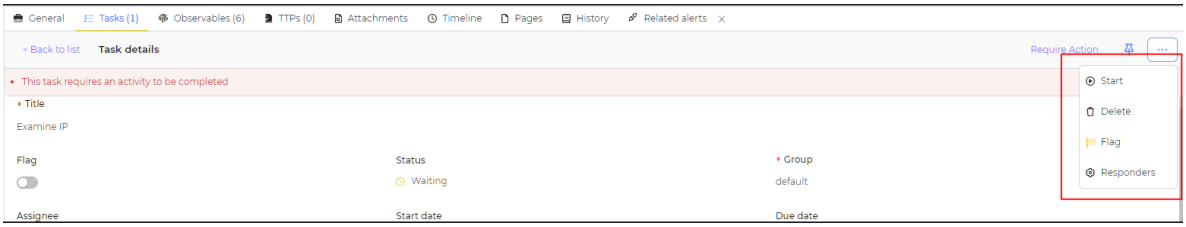


Figure 8.6: Actions Menu of Task (In task details)

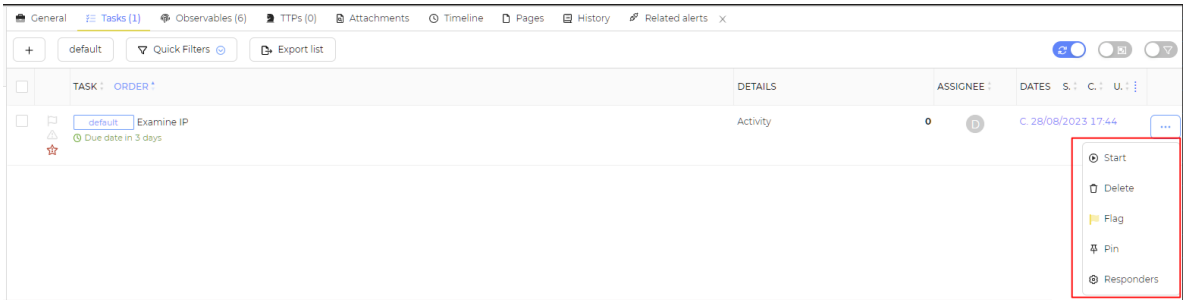


Figure 8.7: Actions Menu of Task (In task list)

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

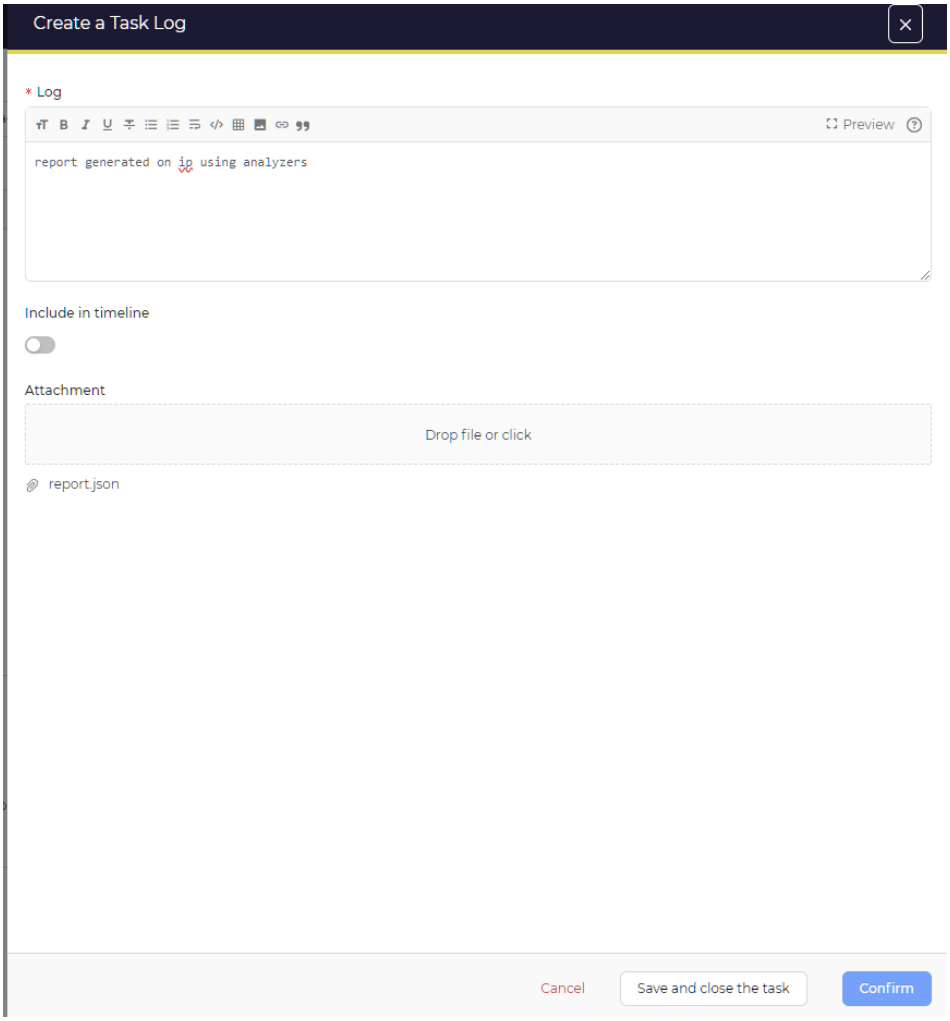


Figure 8.8: Adding Activity

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

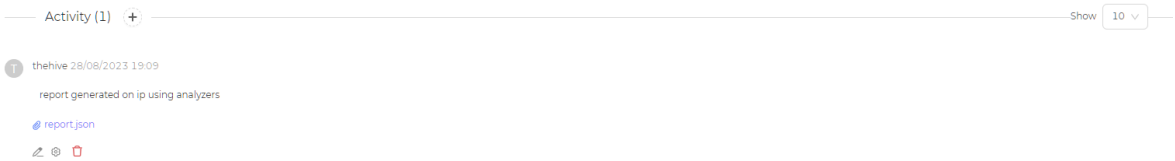


Figure 8.9: Activity List

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.

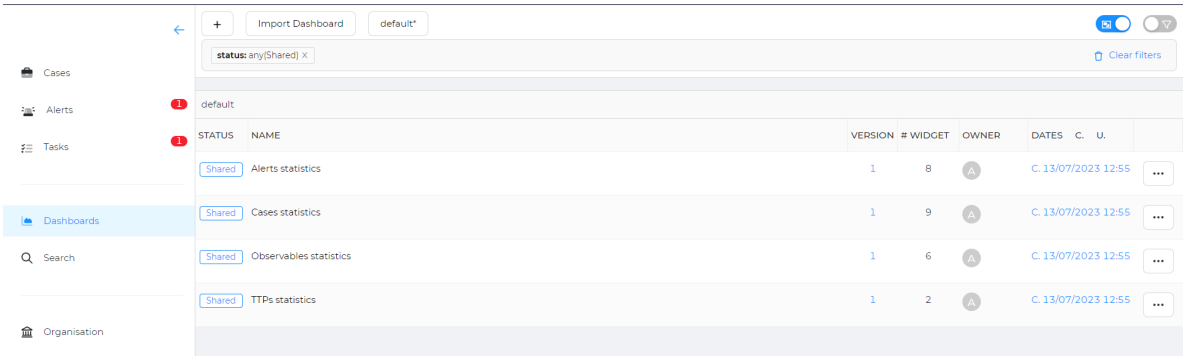


Figure 9.1: Dashboards

9.2 Add a Dashboard

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

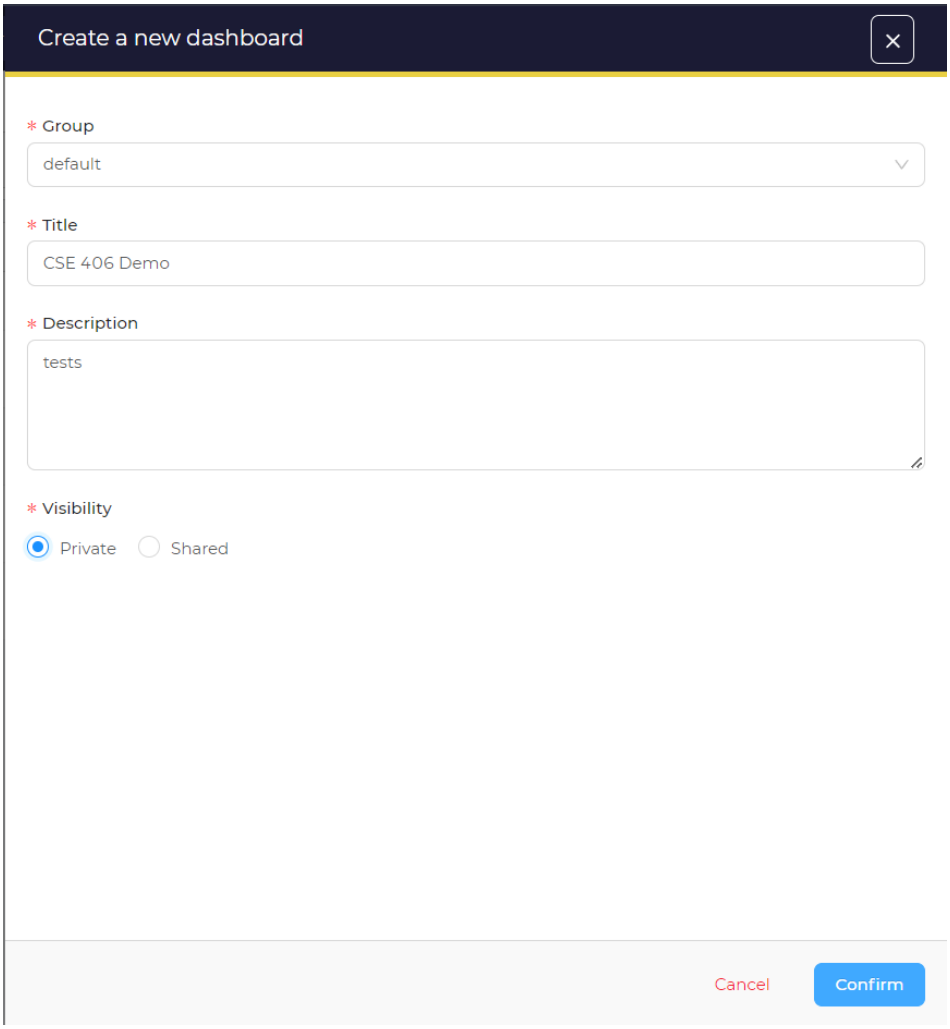


Figure 9.2: Add New Dashboard

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

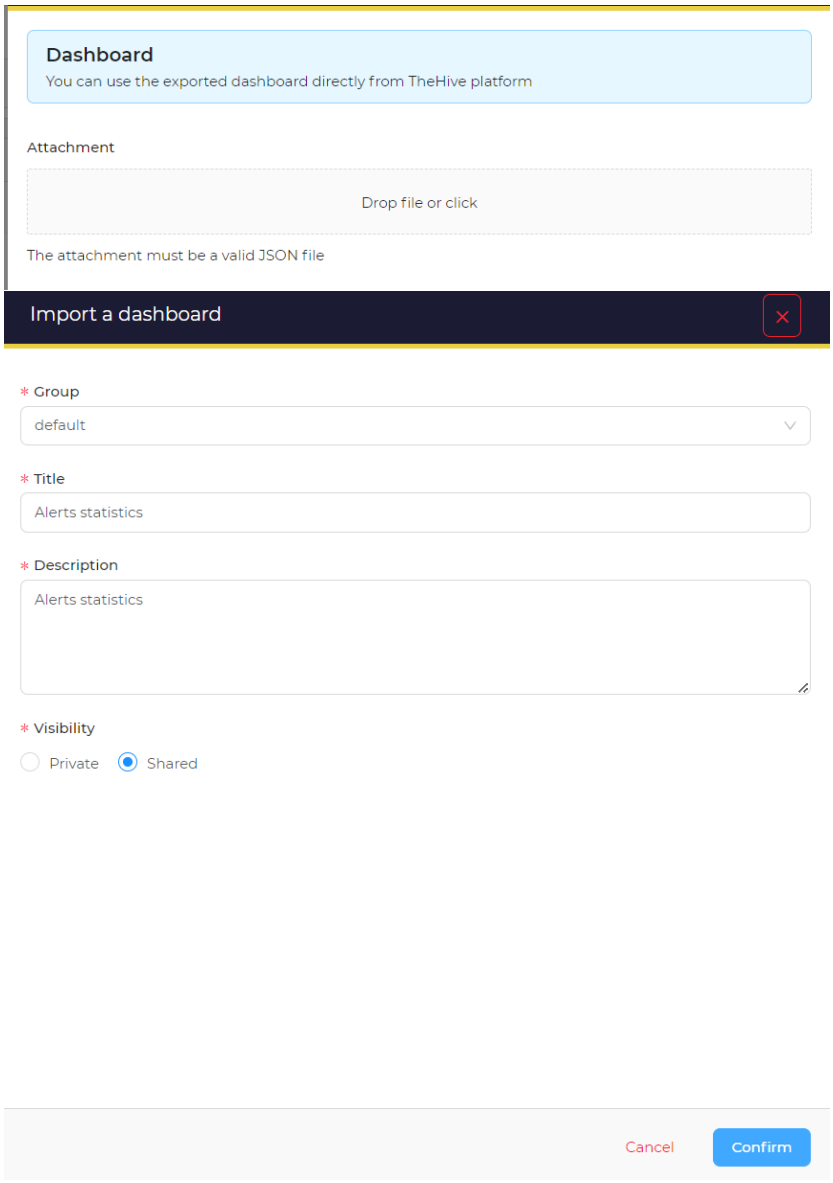


Figure 9.3: Import Dashboard

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

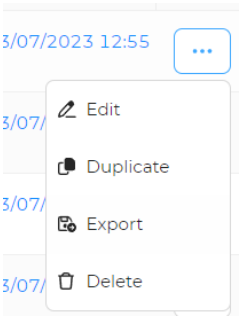


Figure 9.4: Dashboard Actions

9.4.2 Filtering and Sorting

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

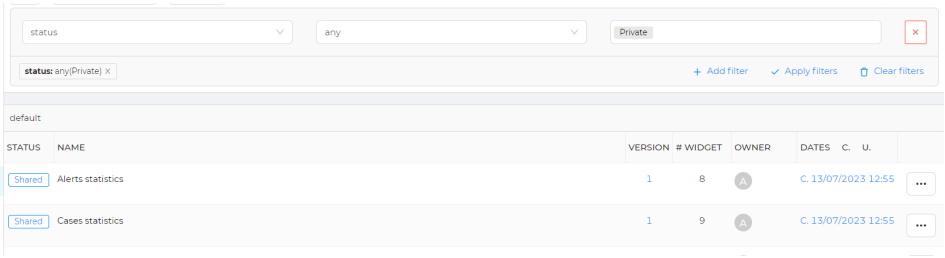


Figure 9.5: Dashboard Filtering and Sorting

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.

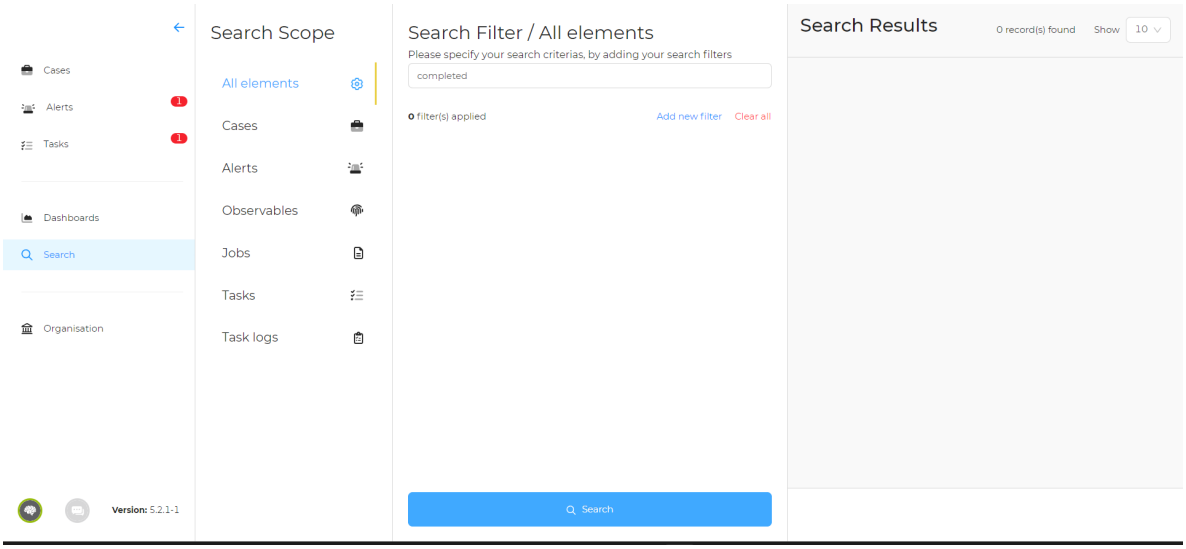


Figure 10.1: Search View

10.2 Search Alerts

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

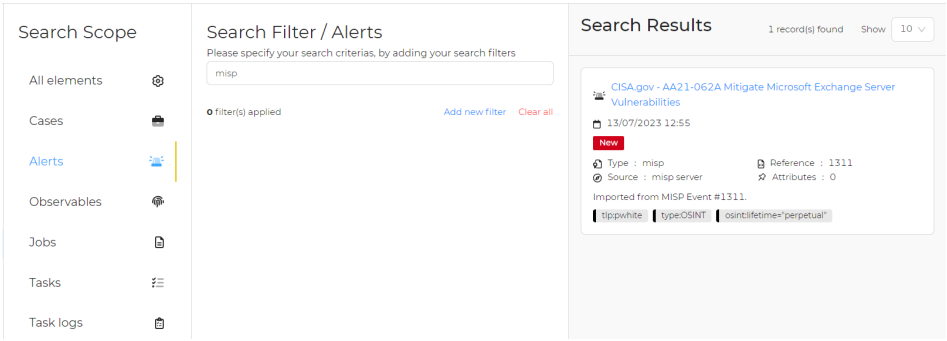


Figure 10.2: Search Alerts

10.3 Search Cases

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

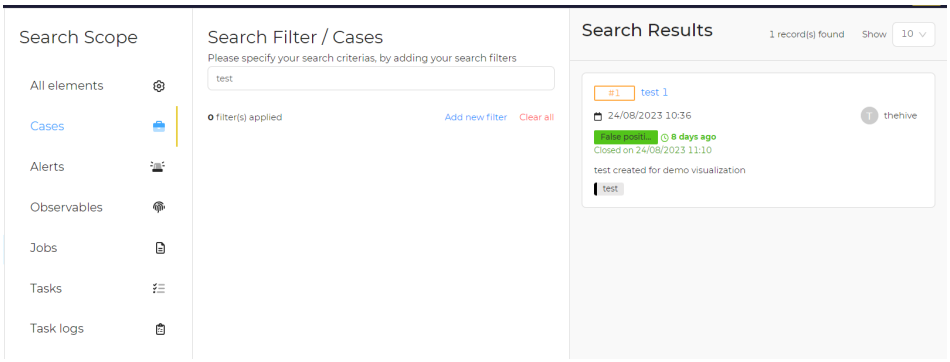


Figure 10.3: Search Cases

10.4 Search Observables

We can find observables from this criteria

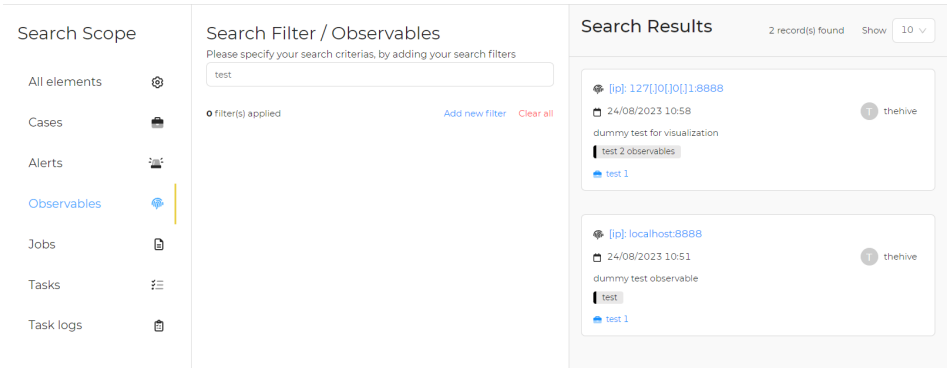


Figure 10.4: Search Observables

10.5 Search Tasks

We can also search the tasks to quickly view relevant tasks

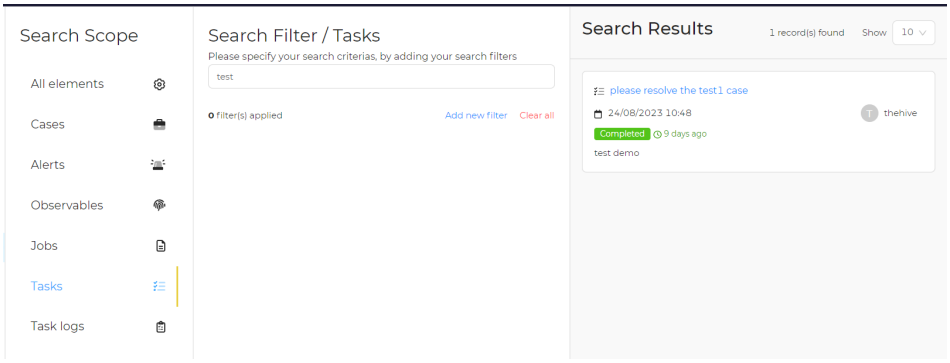


Figure 10.5: Search Tasks

Chapter 11

Admin Features : Organisations And Accounts Management

11.1 Manage Organisations

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

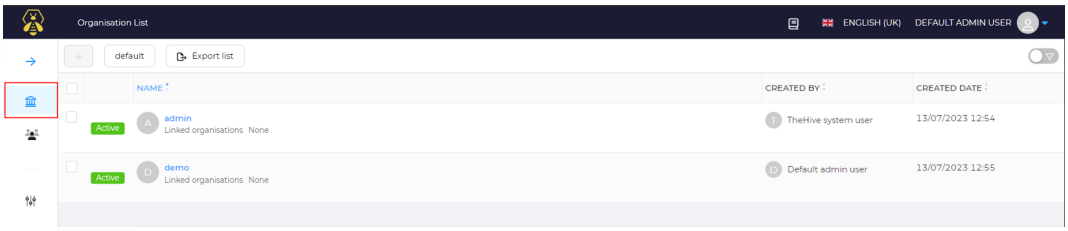


Figure 11.1: Organisations List

11.1.1 Create Organisation

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

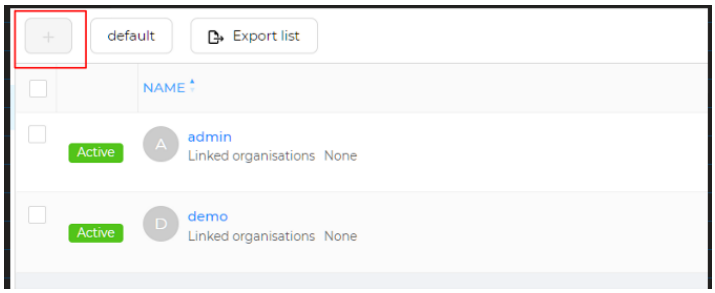


Figure 11.2: Add Organisation

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.

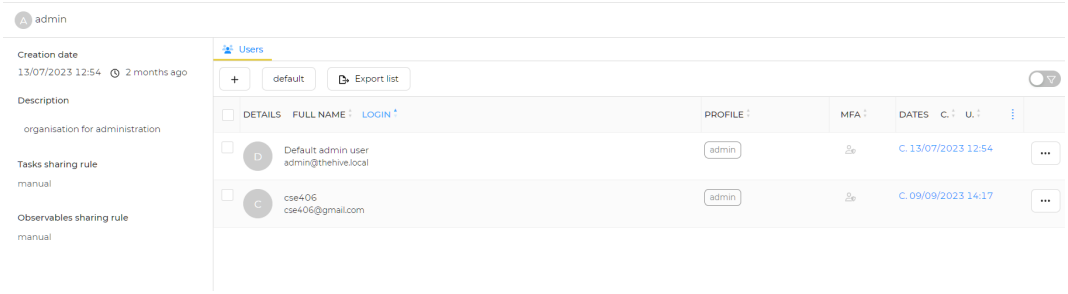


Figure 11.3: Details of An Organisation

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.

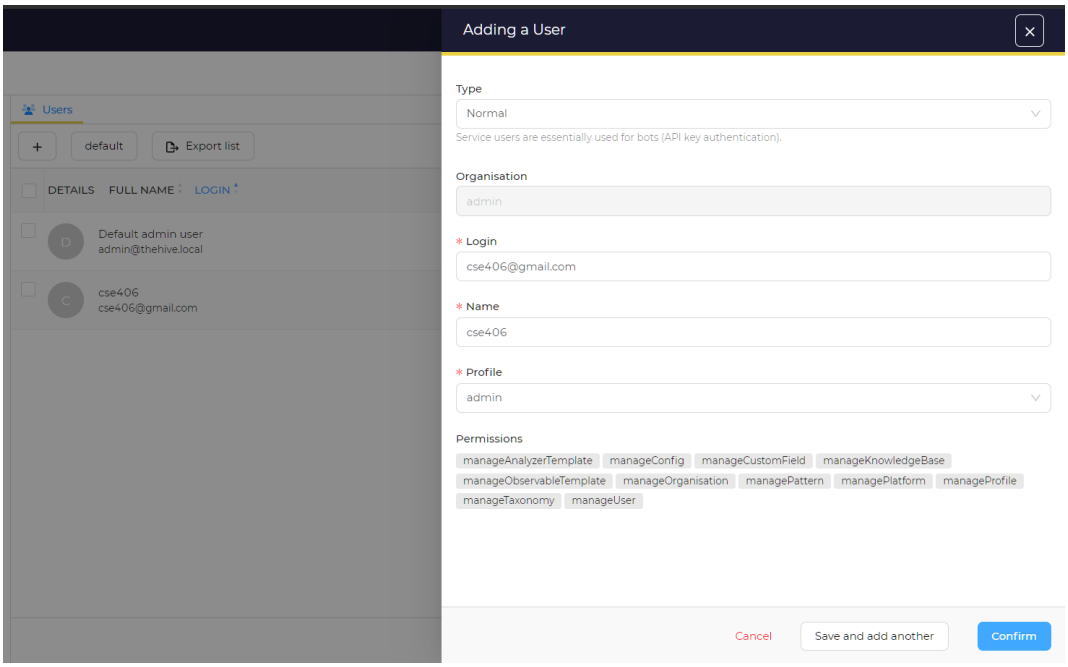


Figure 11.4: Add User to An Organisation

11.2 Manage Users

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

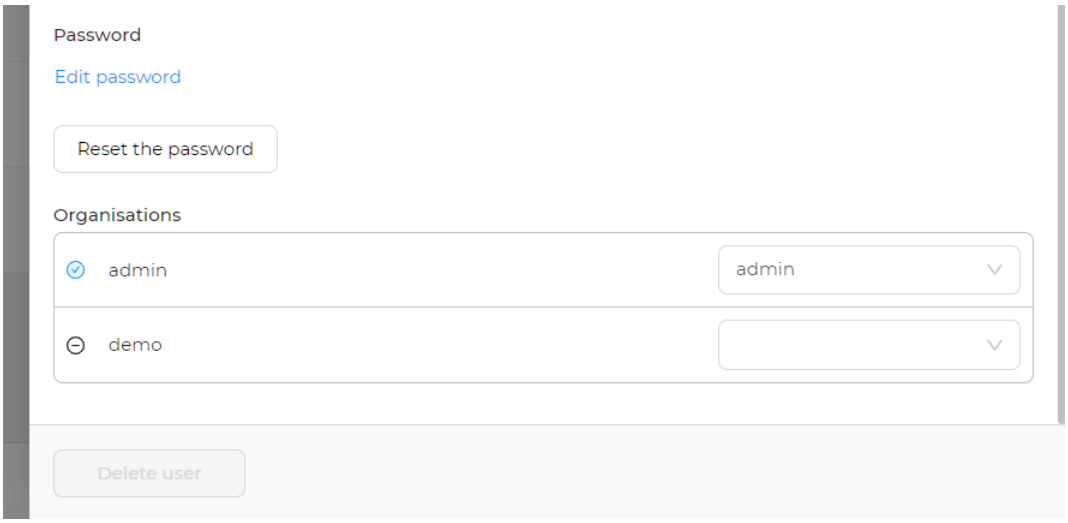


Figure 11.5: Users List

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.

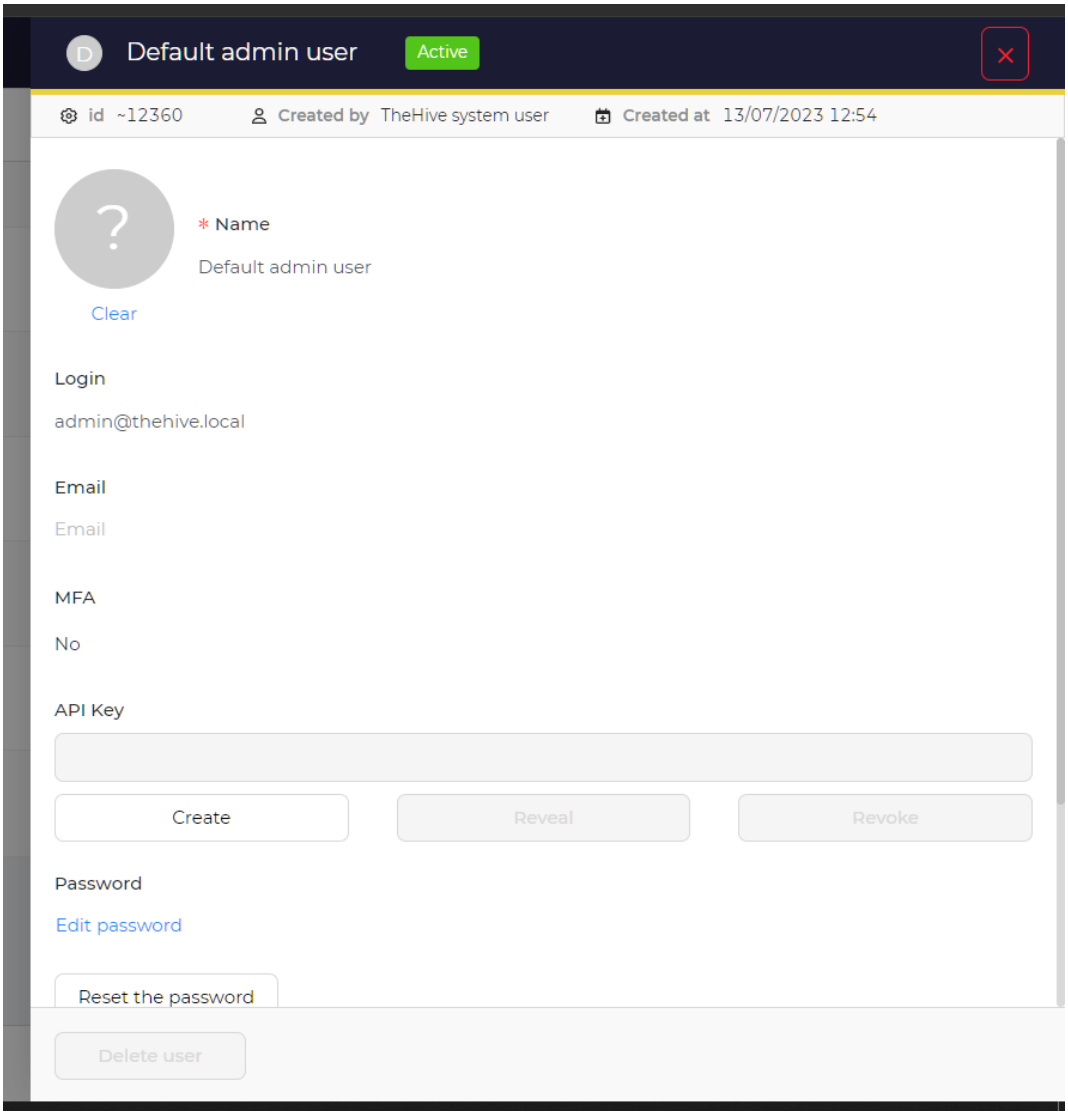


Figure 11.6: Preview of A User

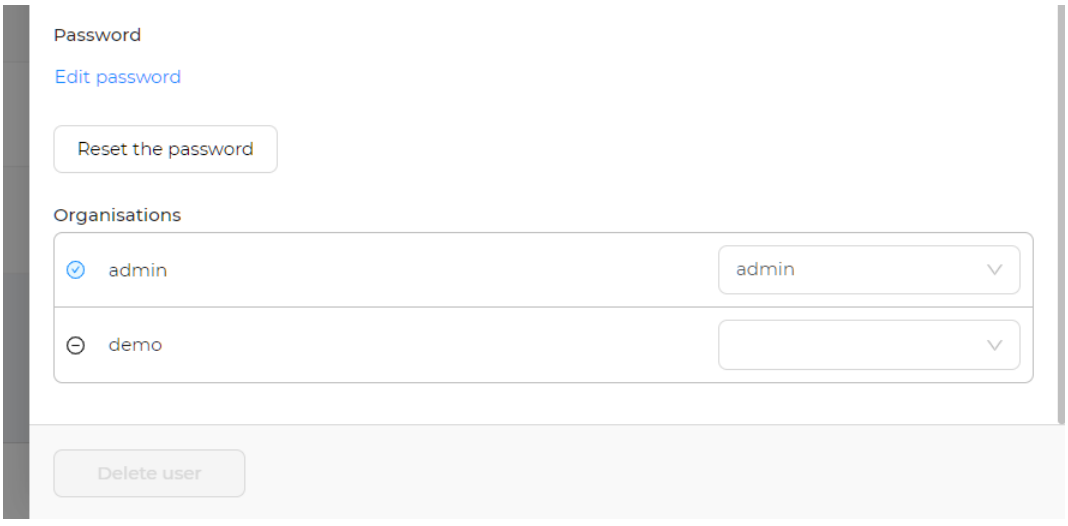


Figure 11.7: Preview of A User Continued

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.

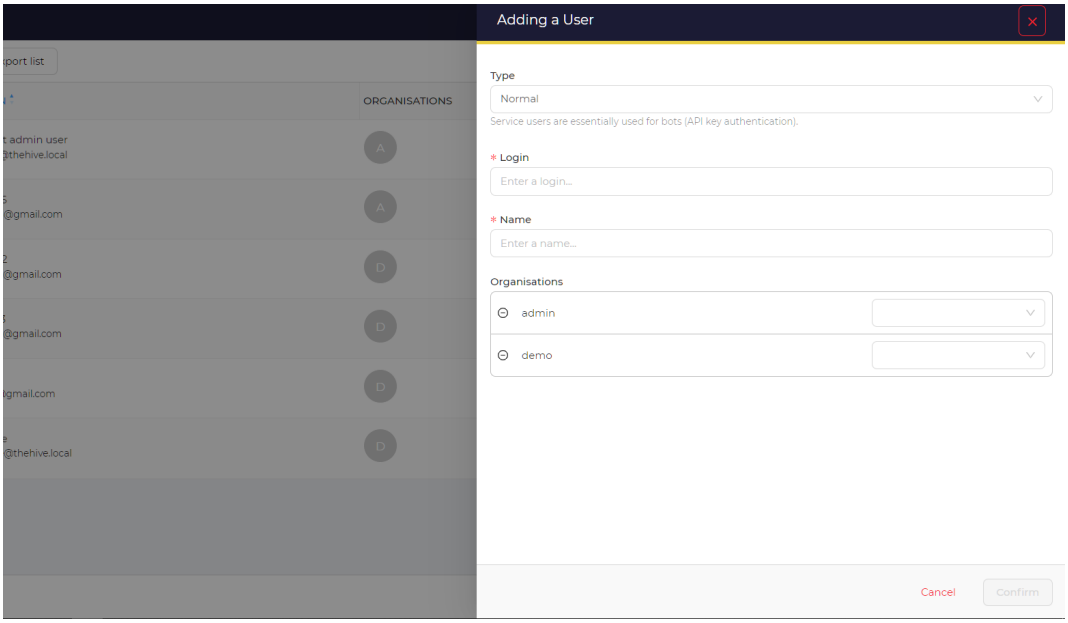


Figure 11.8: Create A User

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.

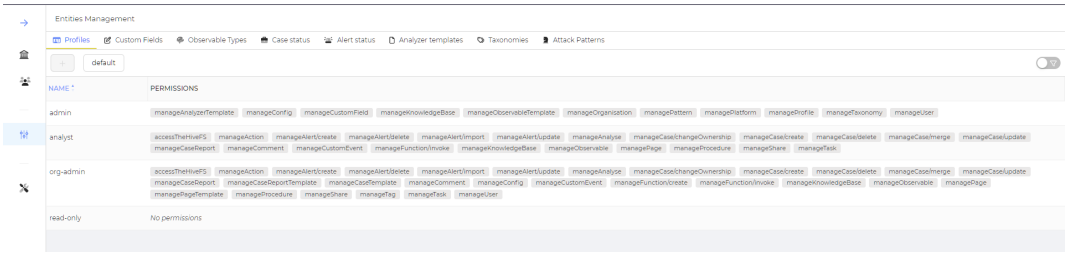


Figure 12.3: Profiles

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.

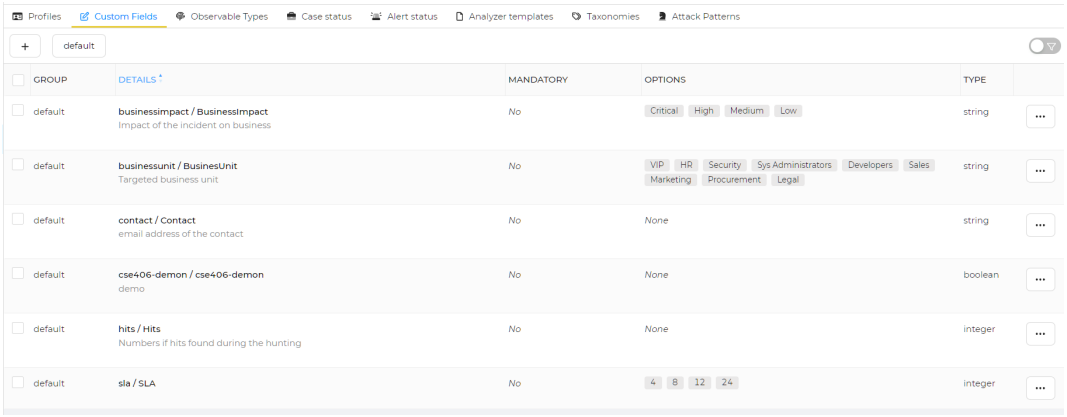


Figure 12.4: Custom Fields

12.3.1 Adding Custom Field

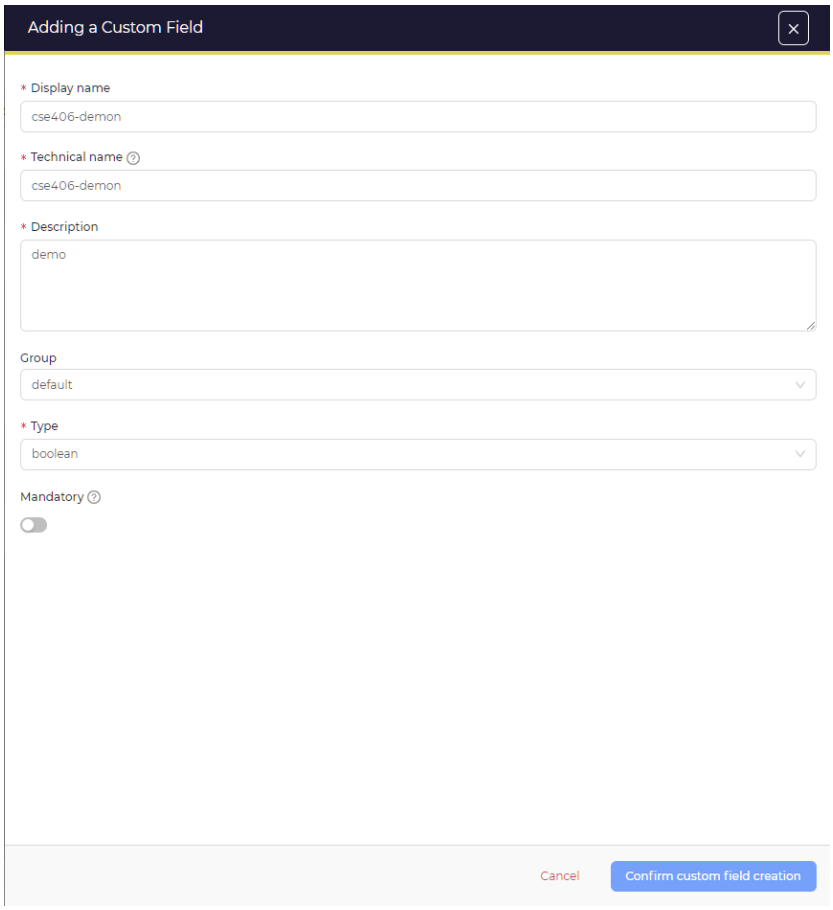


Figure 12.5: Add Custom Fields

12.3.2 Editing Custom Field

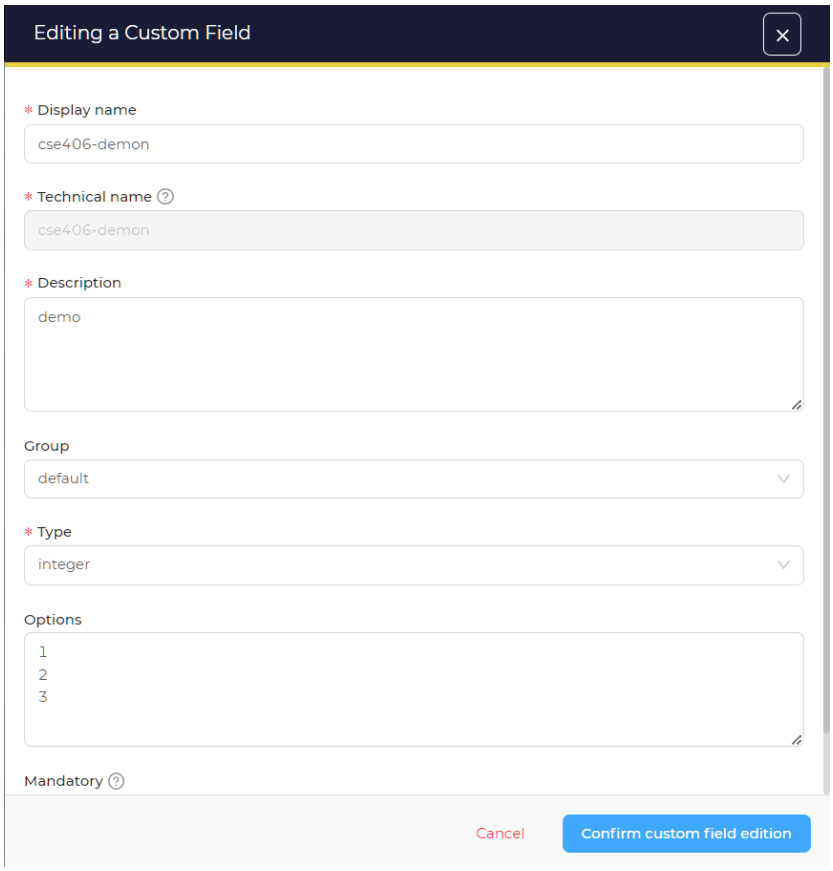


Figure 12.6: Edit Custom Field

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.

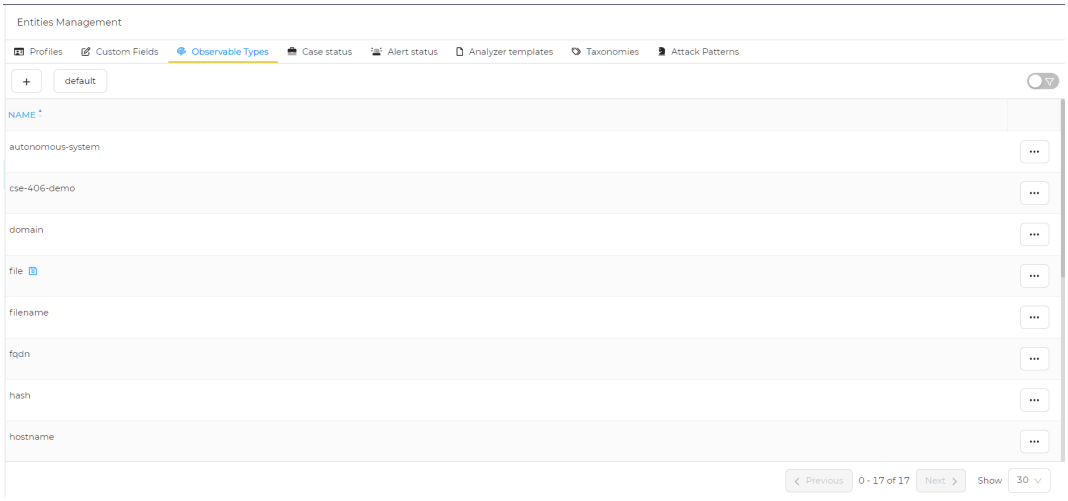


Figure 12.7: Observable Types

12.4.1 Adding Observable Type

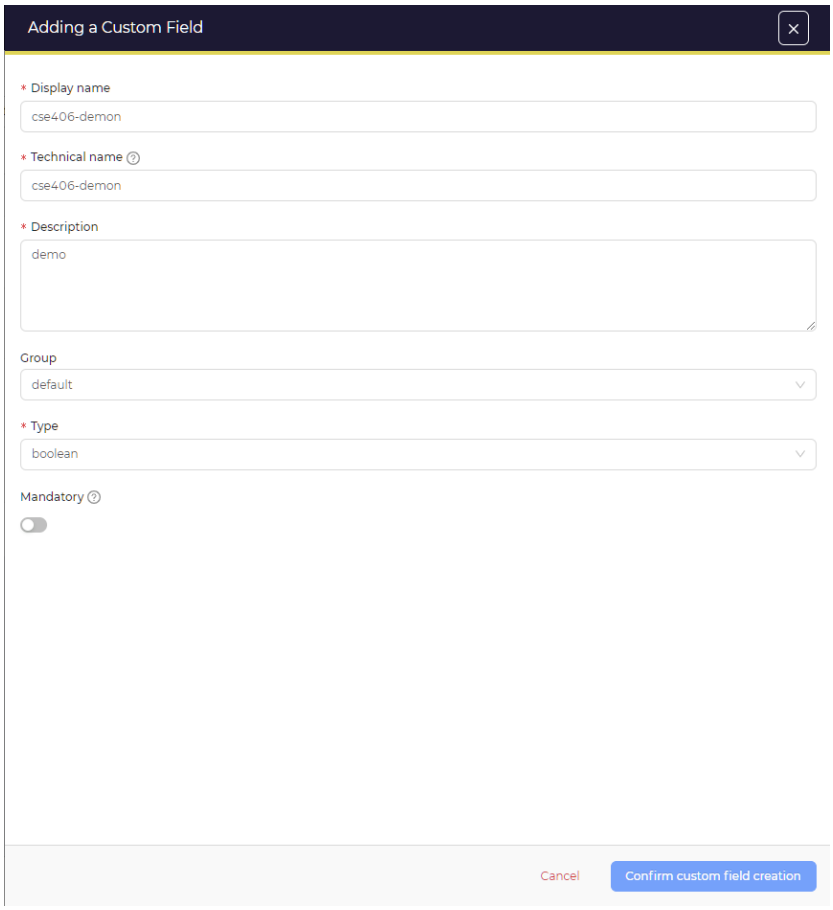


Figure 12.8: Add Observable Types

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.

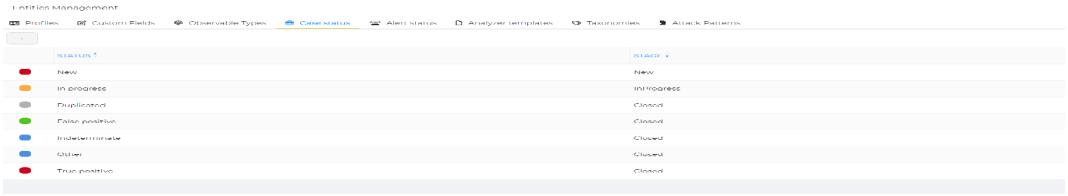


Figure 12.10: Case Status

12.6 Alert Status

Similar to case status.

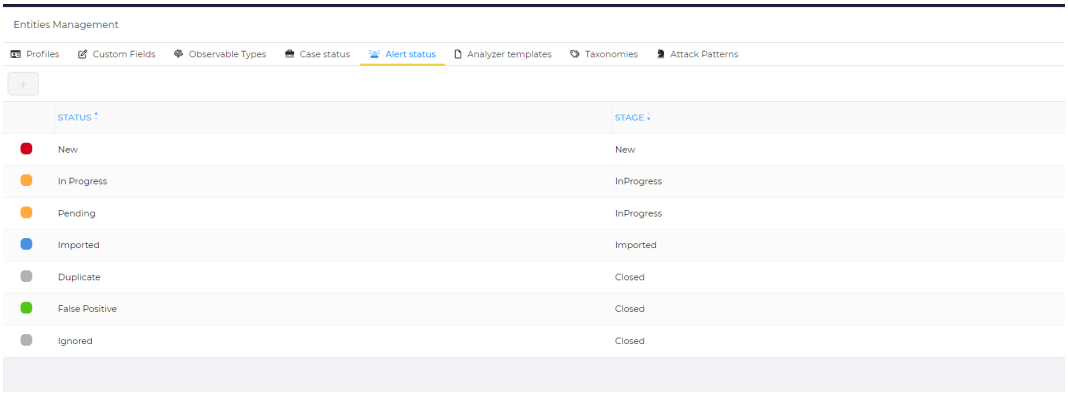


Figure 12.11: Alert Status

12.7 Analyzer Templates

Analyzers tamplates 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.

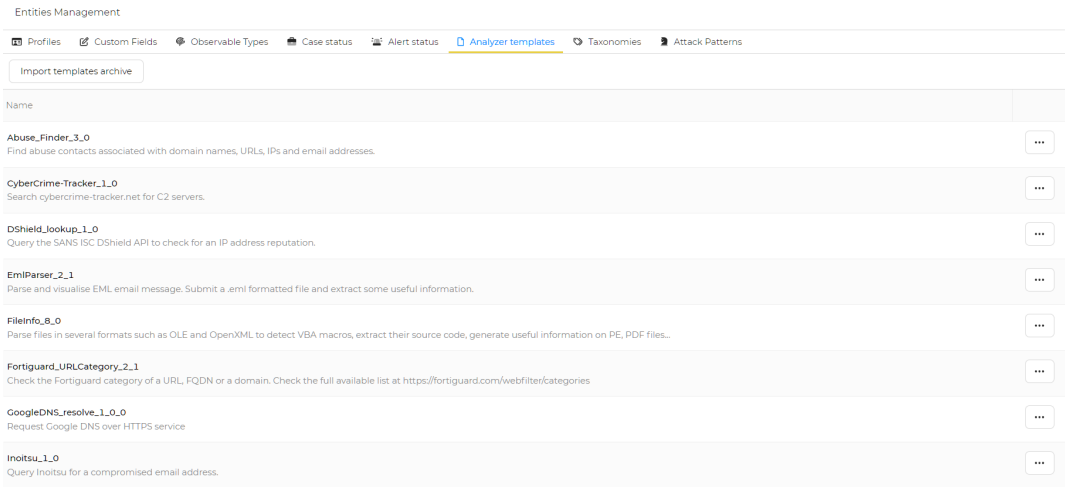


Figure 12.12: Analyzers Templates

12.7.1 Adding Template

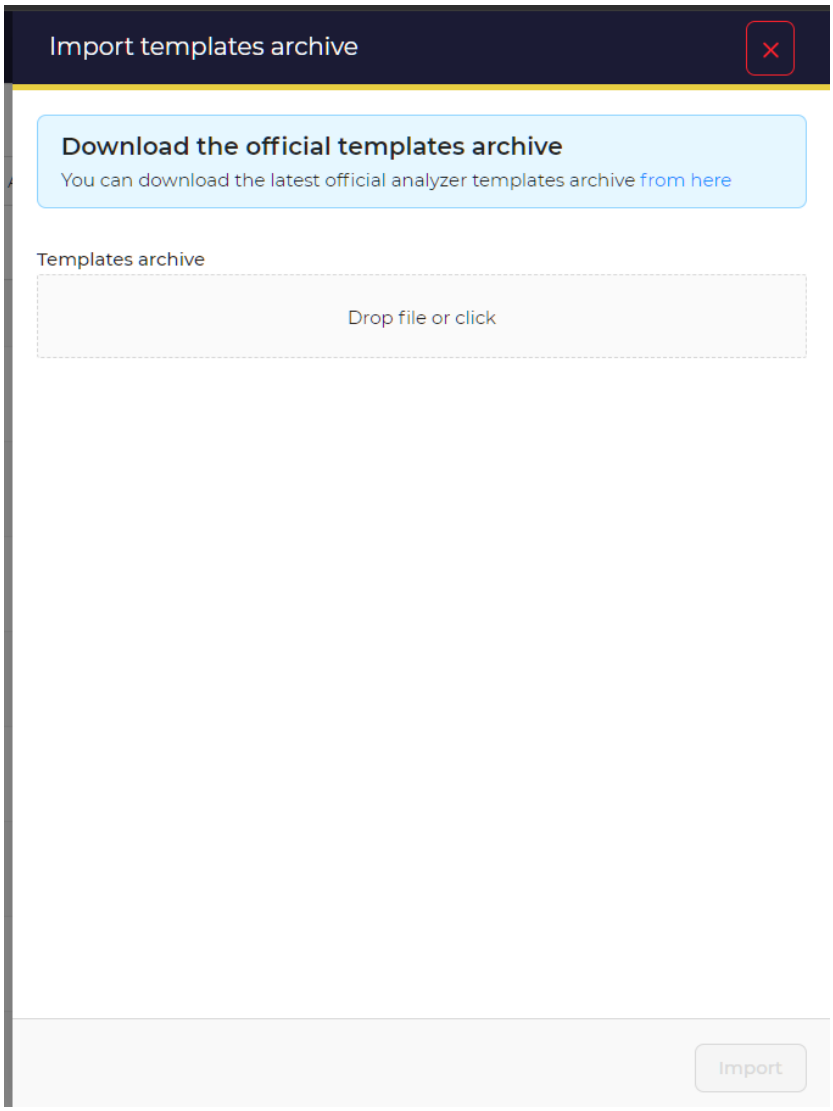


Figure 12.13: Add Analyzers Template

12.7.2 Modifying Template

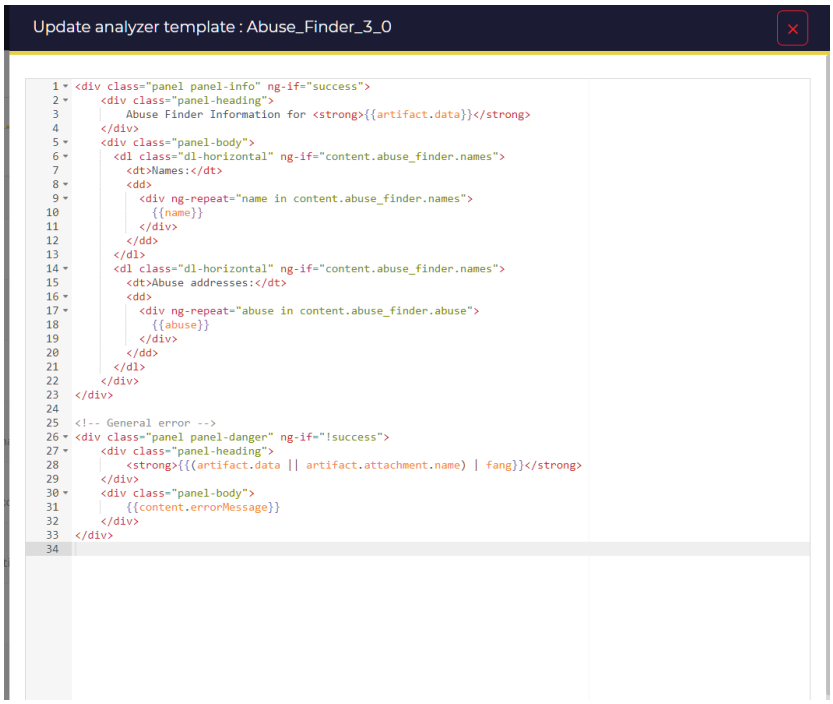


Figure 12.14: Edit Analyzers Template

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.

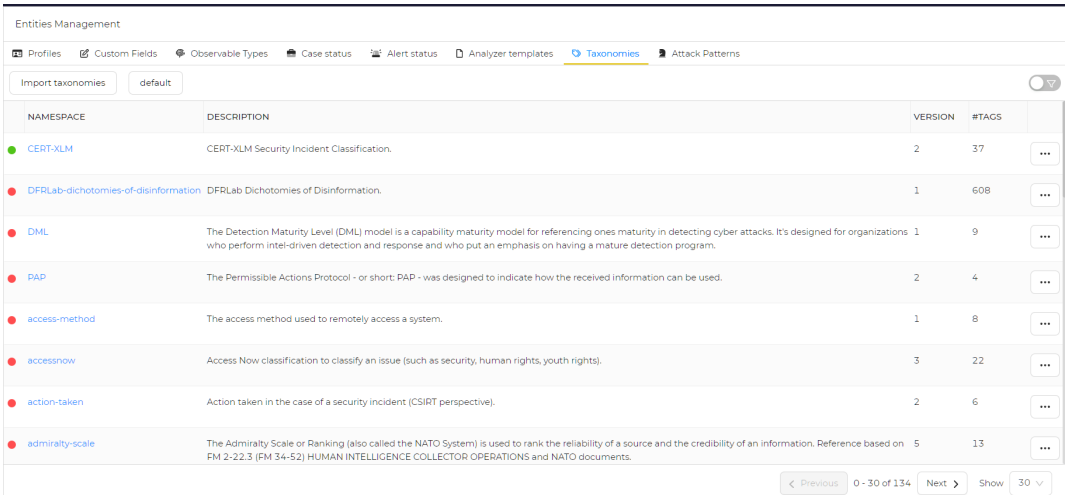


Figure 12.15: Taxonomies

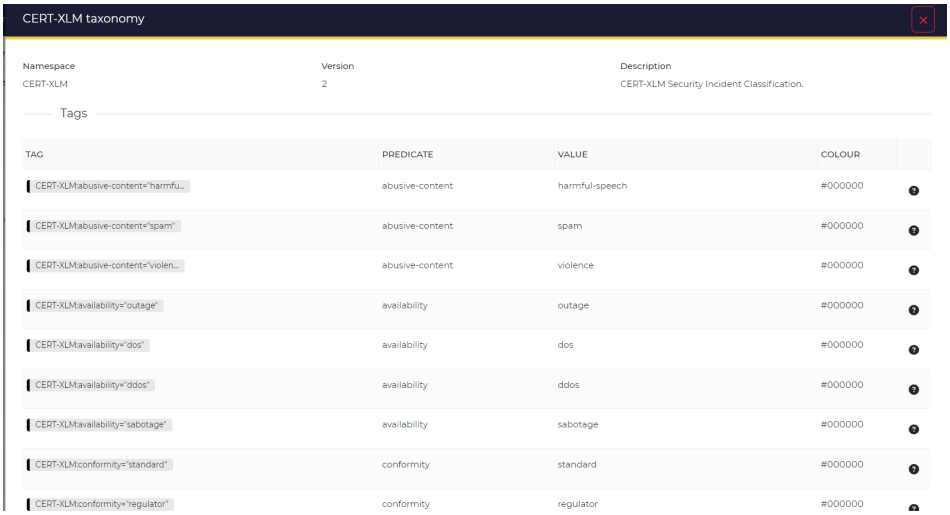


Figure 12.16: Cert Taxonomy

12.8.1 Adding Taxonomy

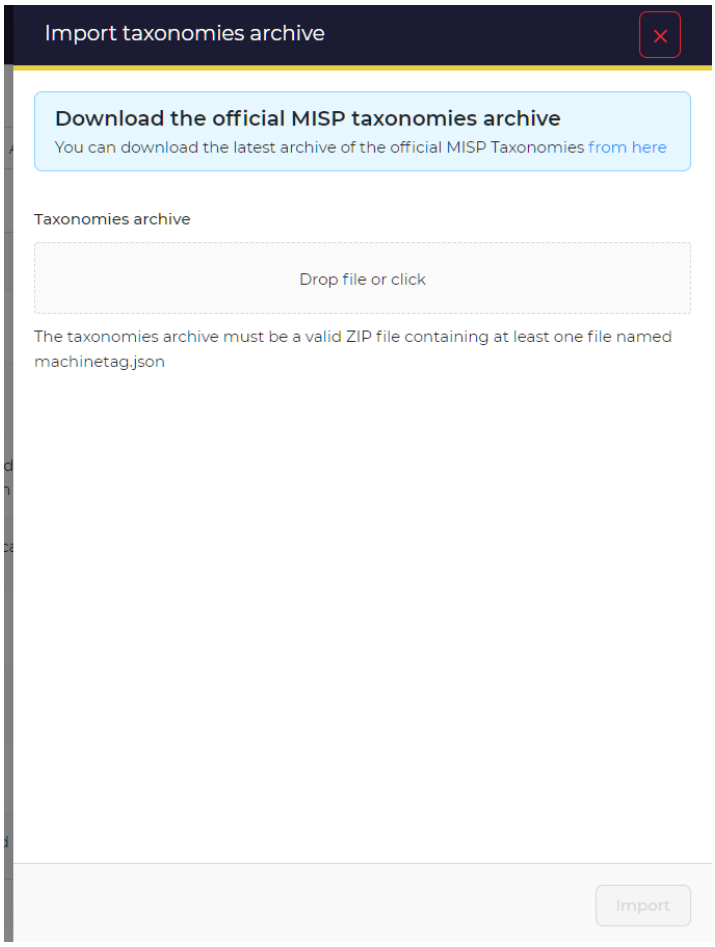


Figure 12.17: Add Taxonomies

12.8.2 Activating Taxonomy

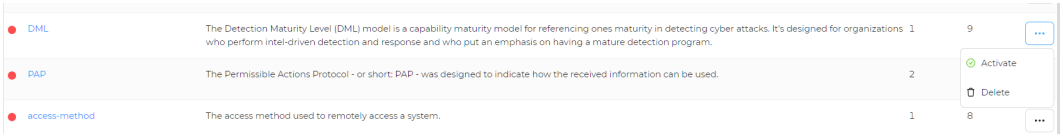


Figure 12.18: Activate Taxonomies

12.9 Attack Patterns

This section contains details of various attack patterns.

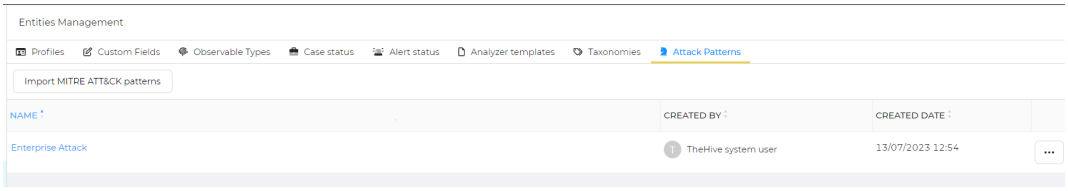


Figure 12.19: Attack Pattern

12.9.1 Details of An Attack Pattern

Clicking on an attack pattern shows its details.

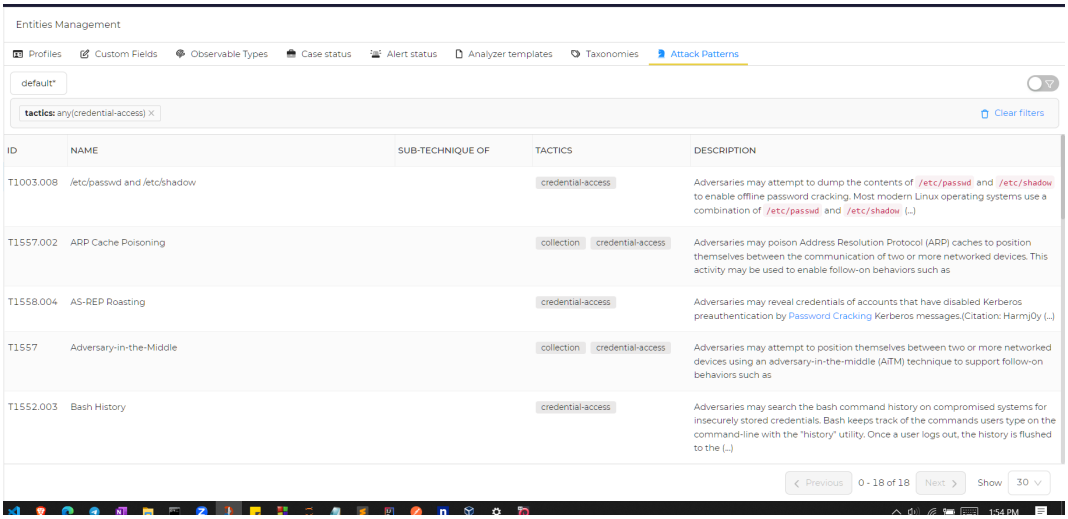


Figure 12.20: Attack Pattern Details

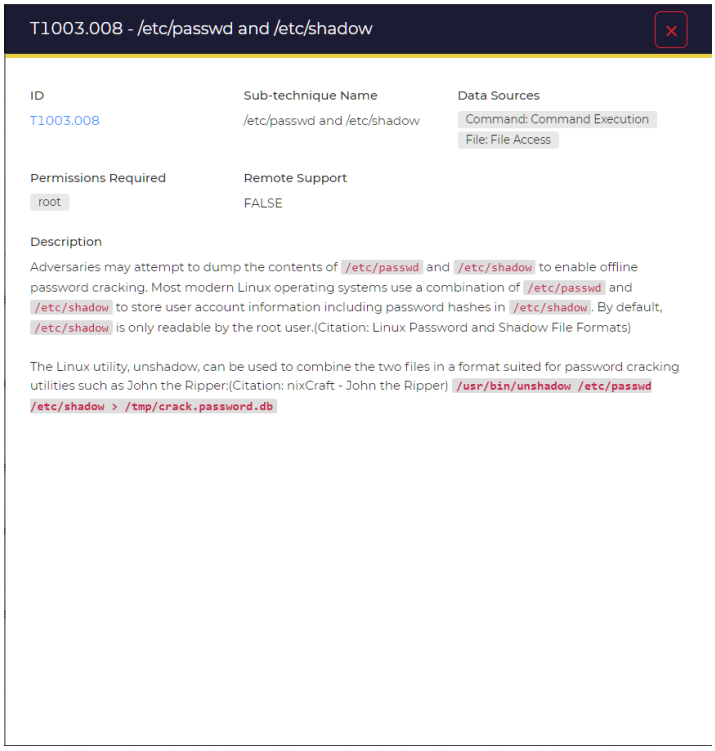


Figure 12.21: Attack Pattern Details

12.9.2 Adding Attack Pattern

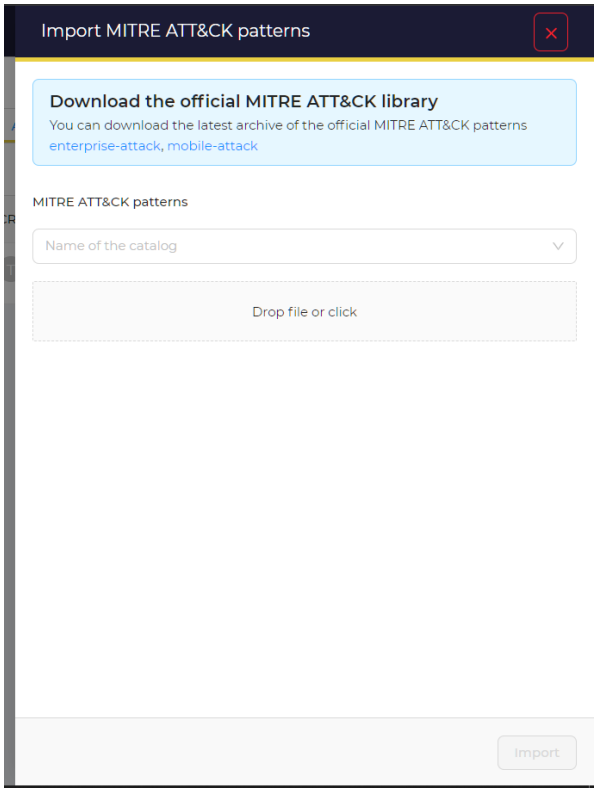


Figure 12.22: Add Attack Pattern

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.

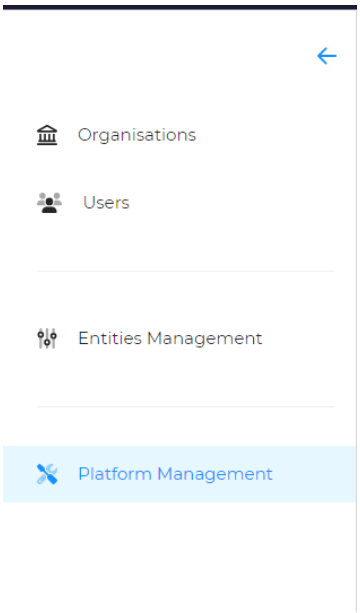


Figure 13.1: Admin view Taskbar

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

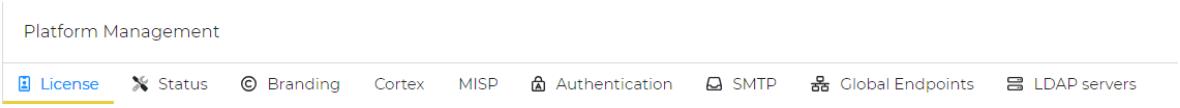


Figure 13.2: Options In Platform Management

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

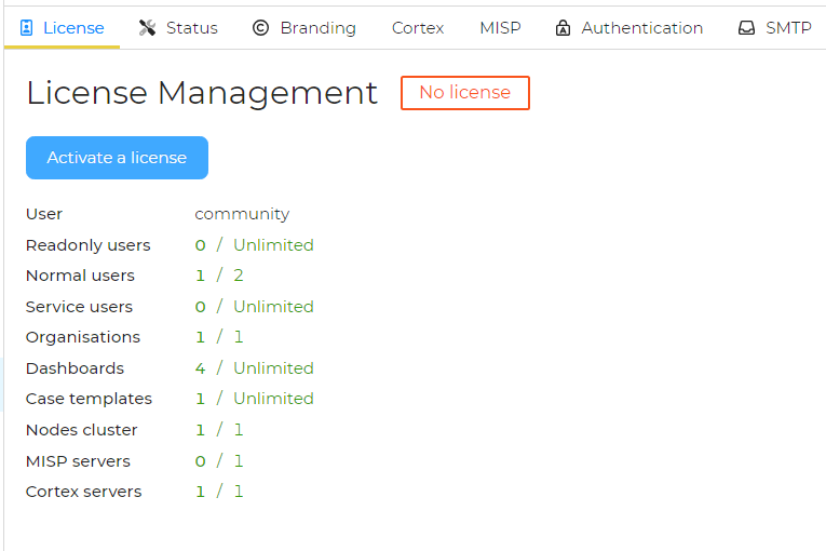


Figure 13.3: Community License

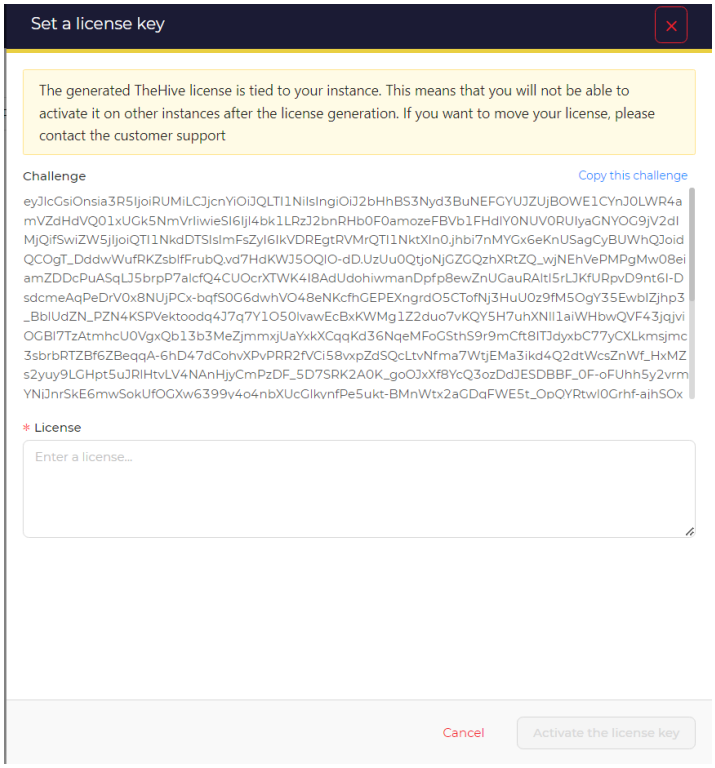


Figure 13.4: Add New License (if key available)

13.3 Platform Status

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

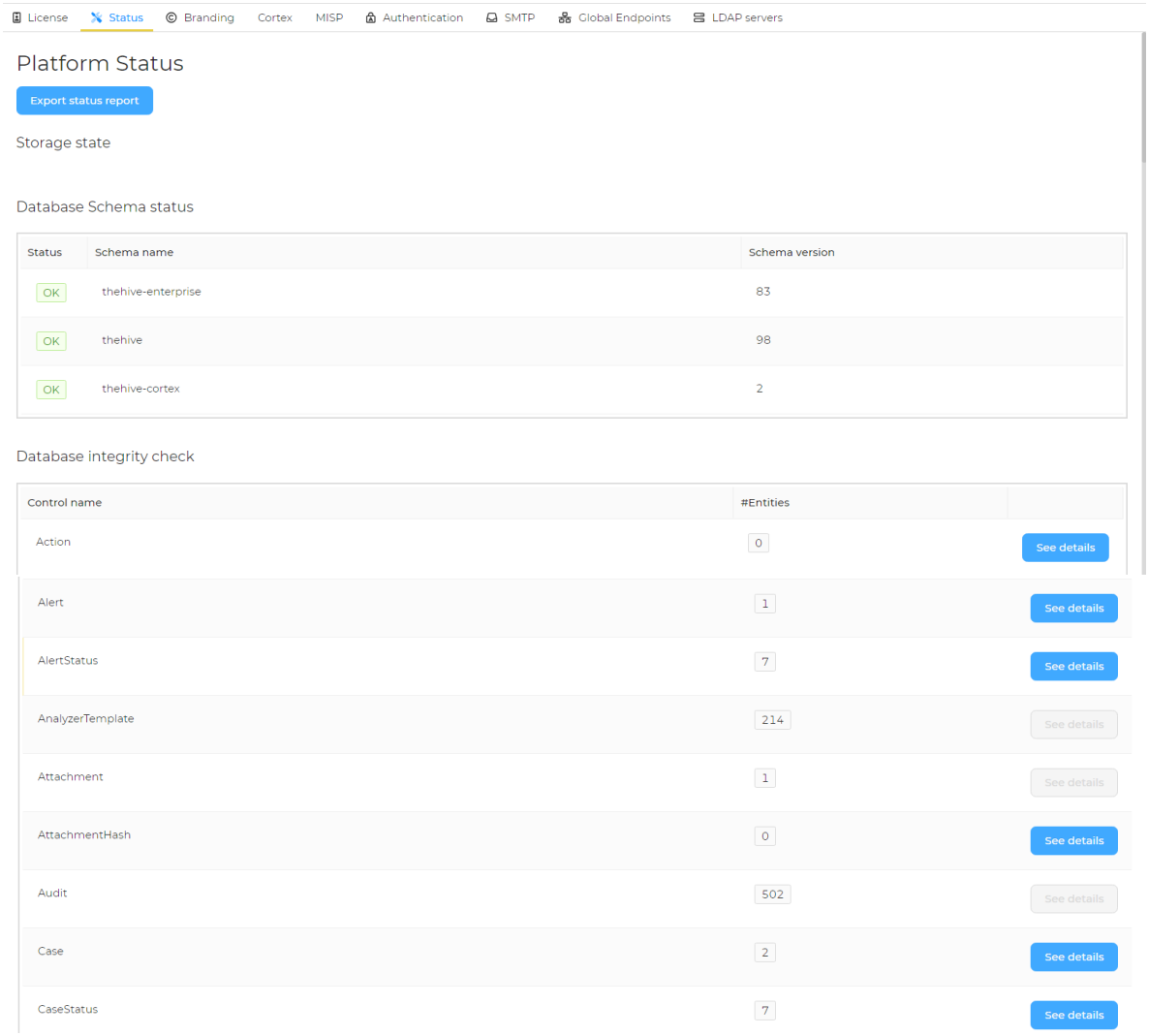


Figure 13.5: Plaform Status

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.

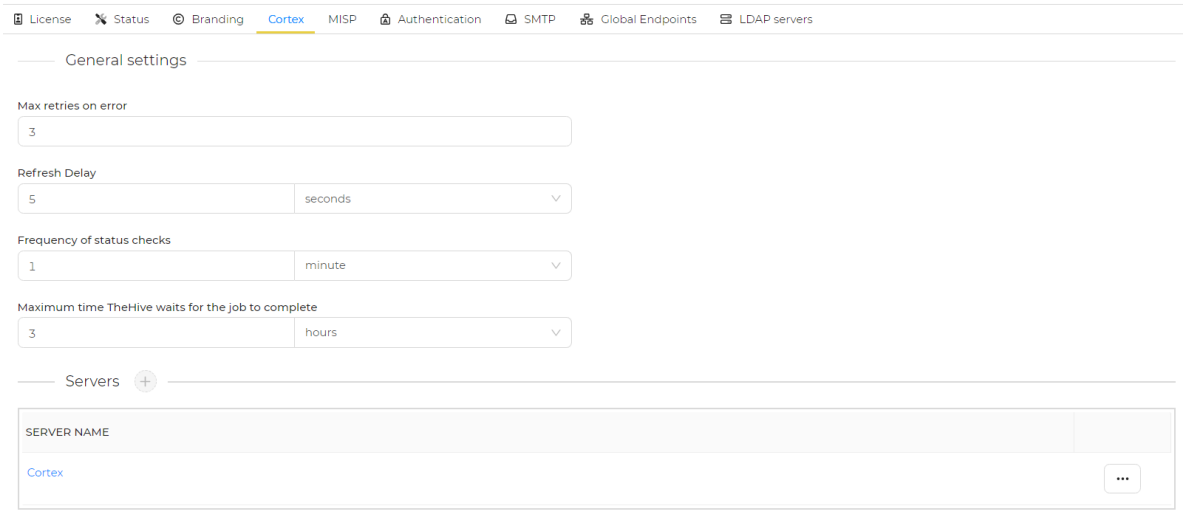


Figure 13.6: Cortex Tab View

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.

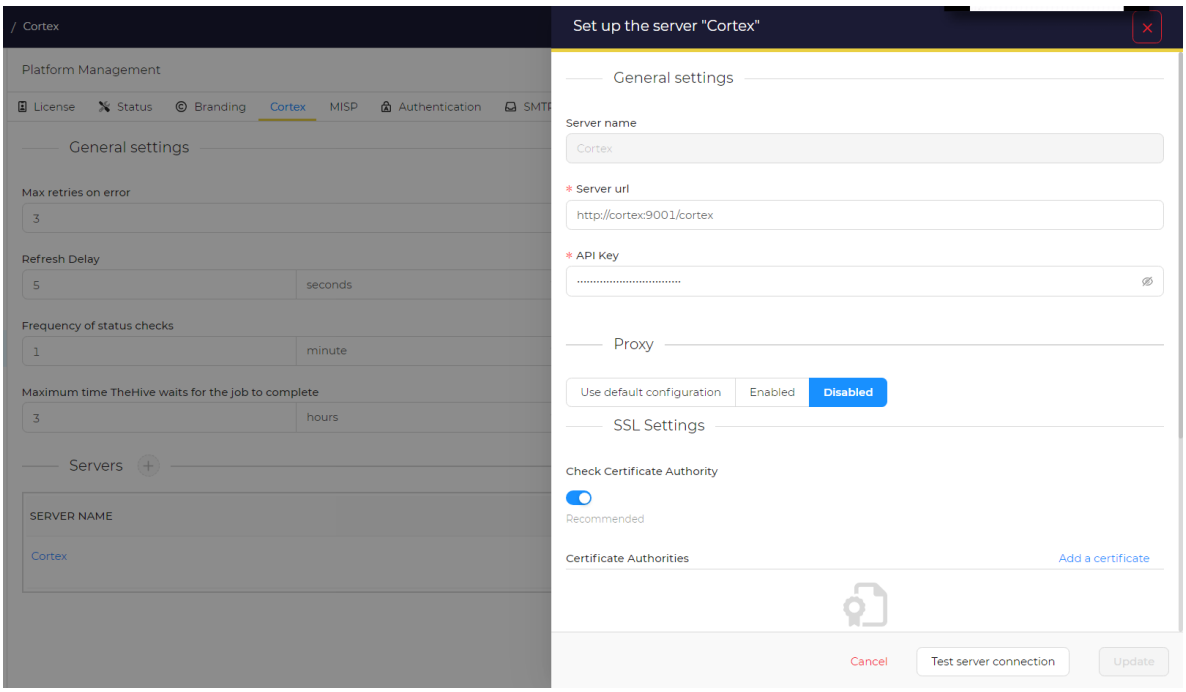


Figure 13.7: Add Cortex Server

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 facilititates 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.

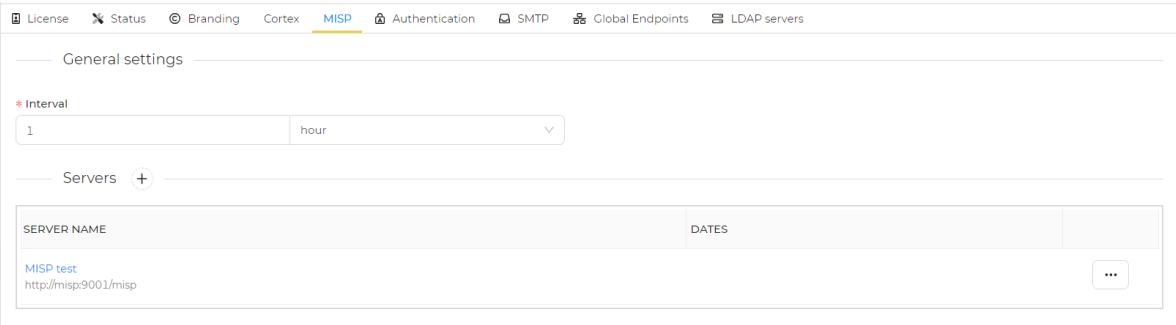


Figure 13.9: MISP Tab View

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.

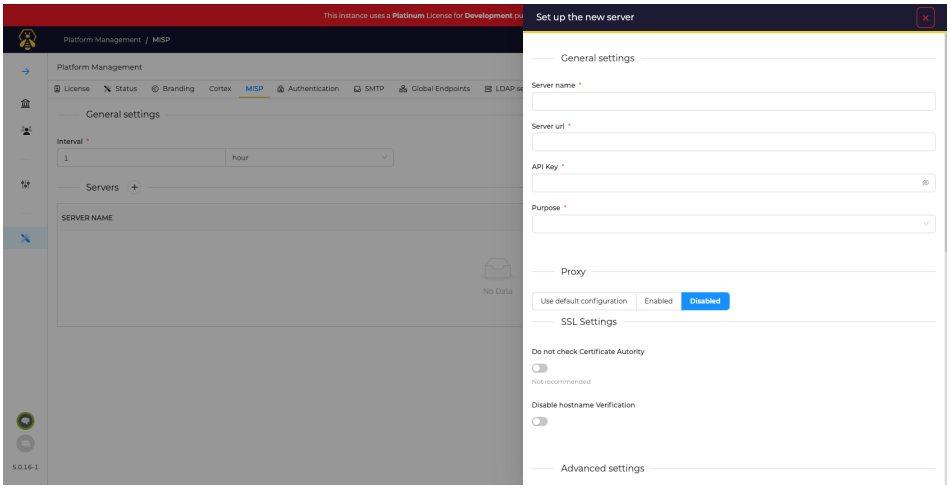


Figure 13.10: Add MISP Server

13.5.2 Configure MISP Server Settings

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

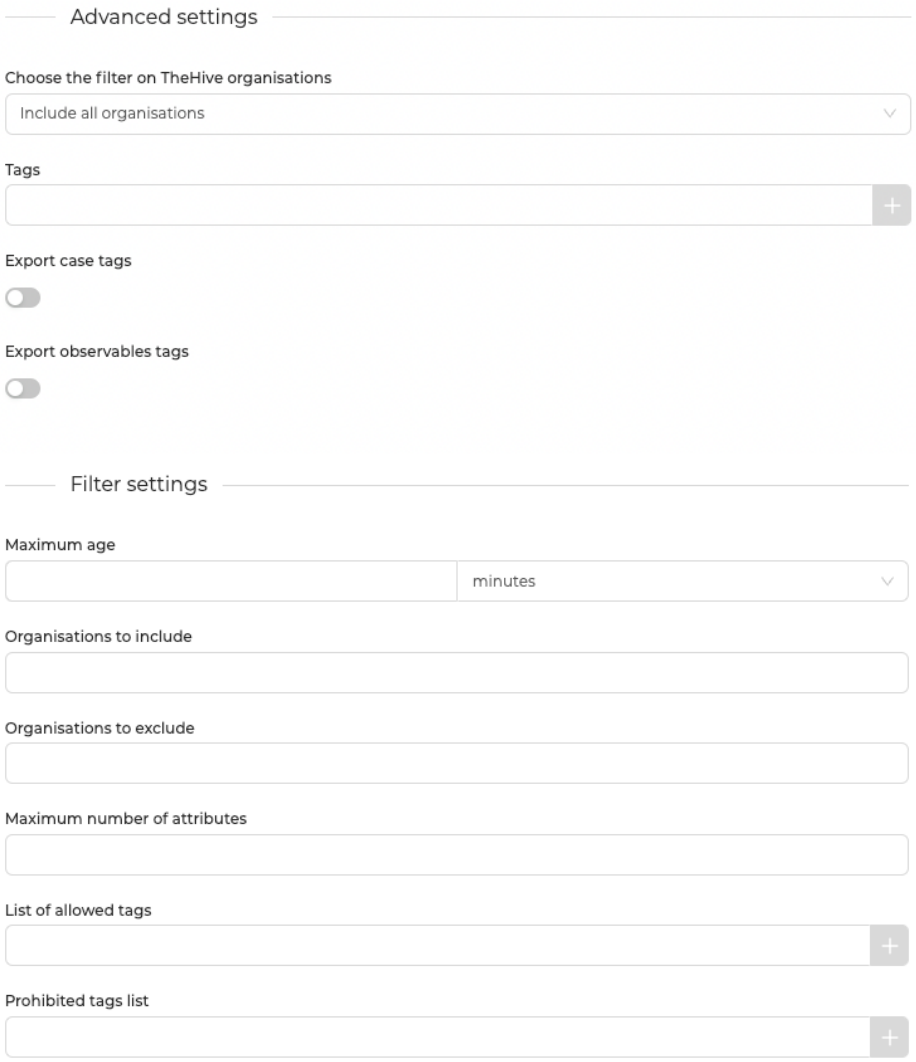


Figure 13.11: MISP Server Settings

13.5.3 Delete MISP Server

We may also delete any existing MISP server.

Figure 13.12: Delete MISP Server

13.6 Authentication

Admin can modify the authentication settings from authentication tab

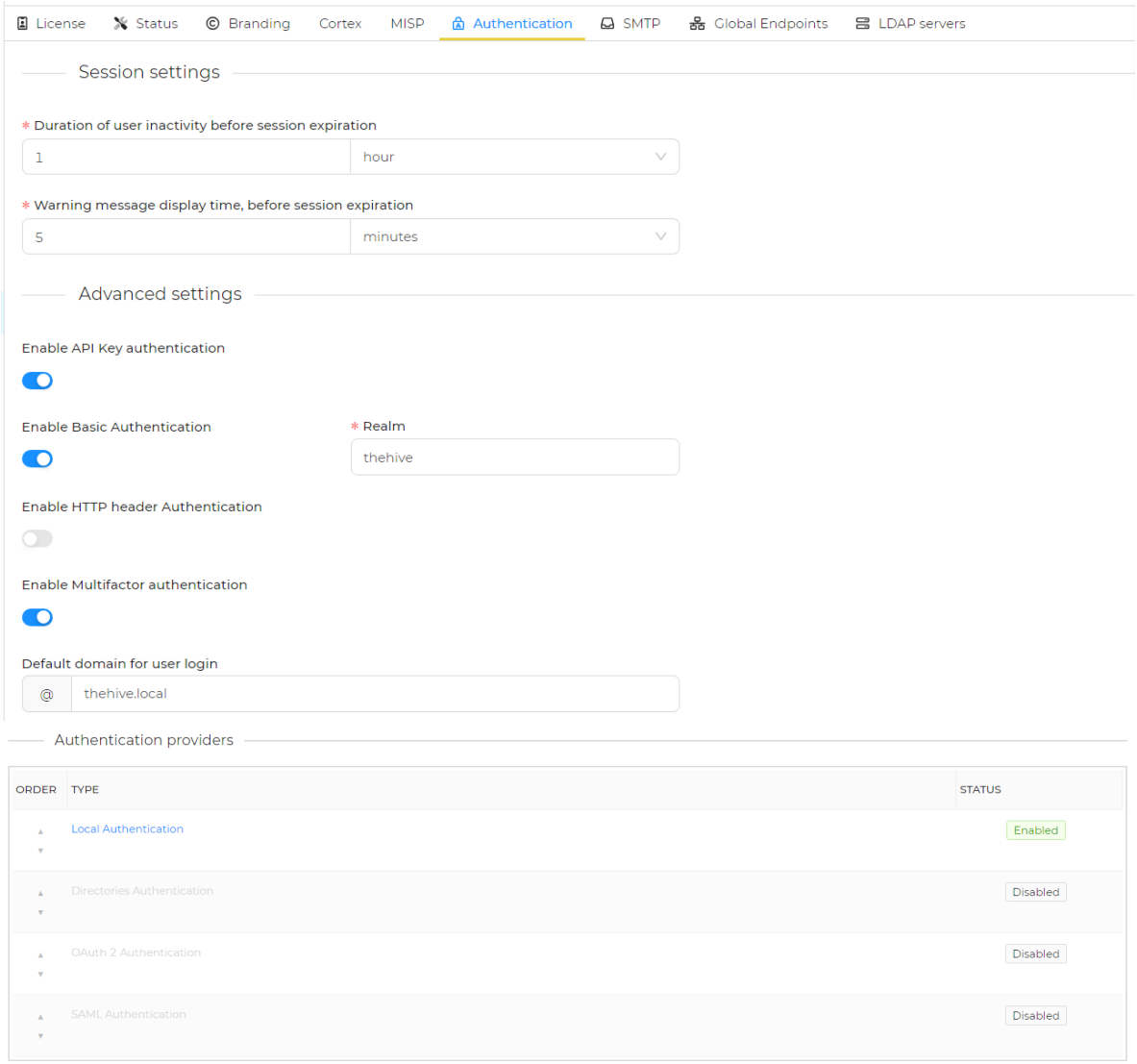


Figure 13.13: Authentication Tab

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

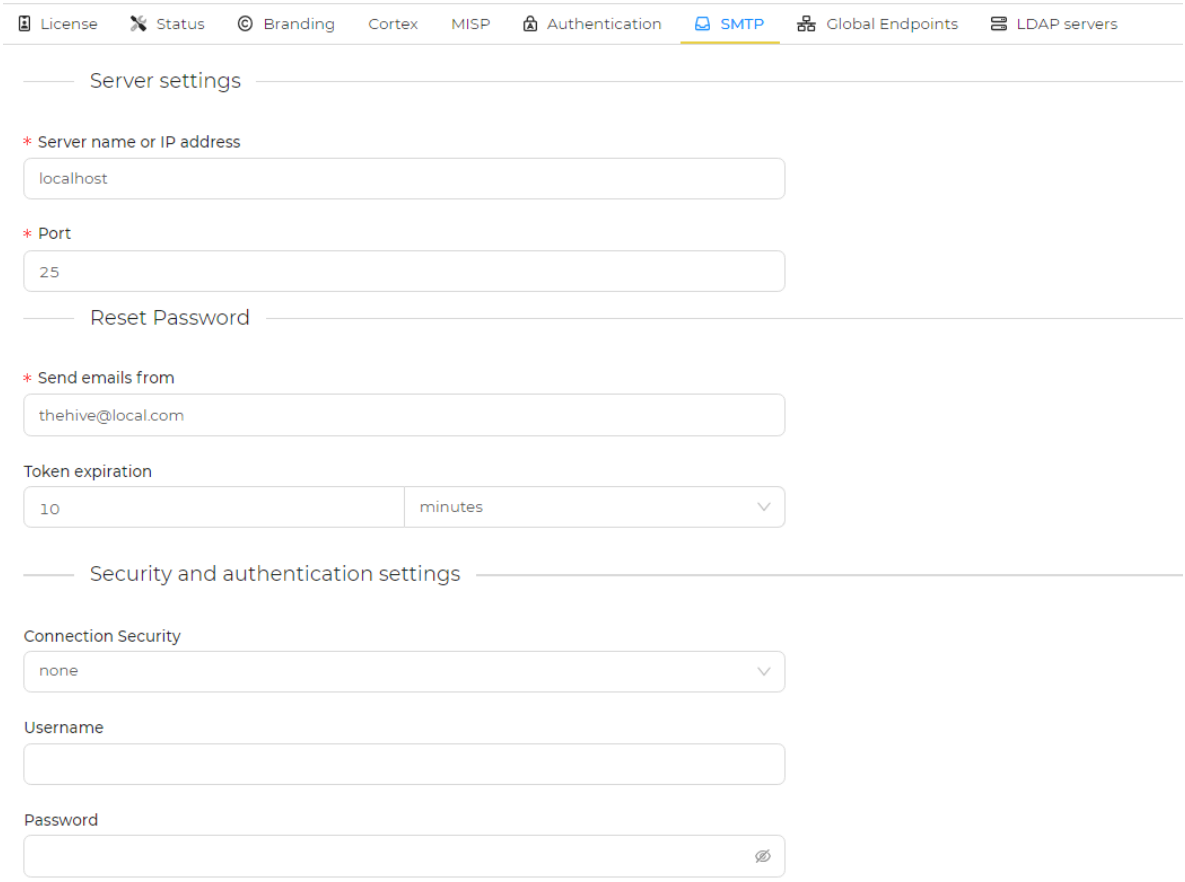


Figure 13.14: SMTP Tab

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.

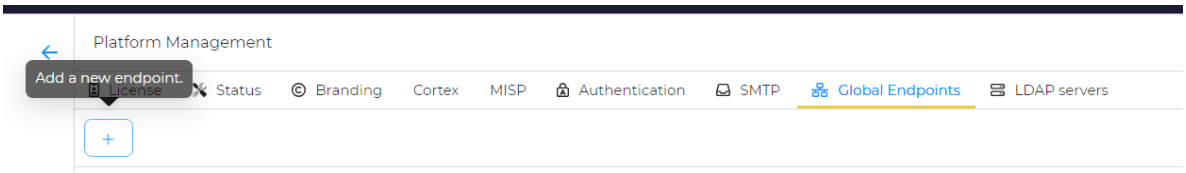


Figure 13.15: Add Global Endpoint

Add New Endpoint

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

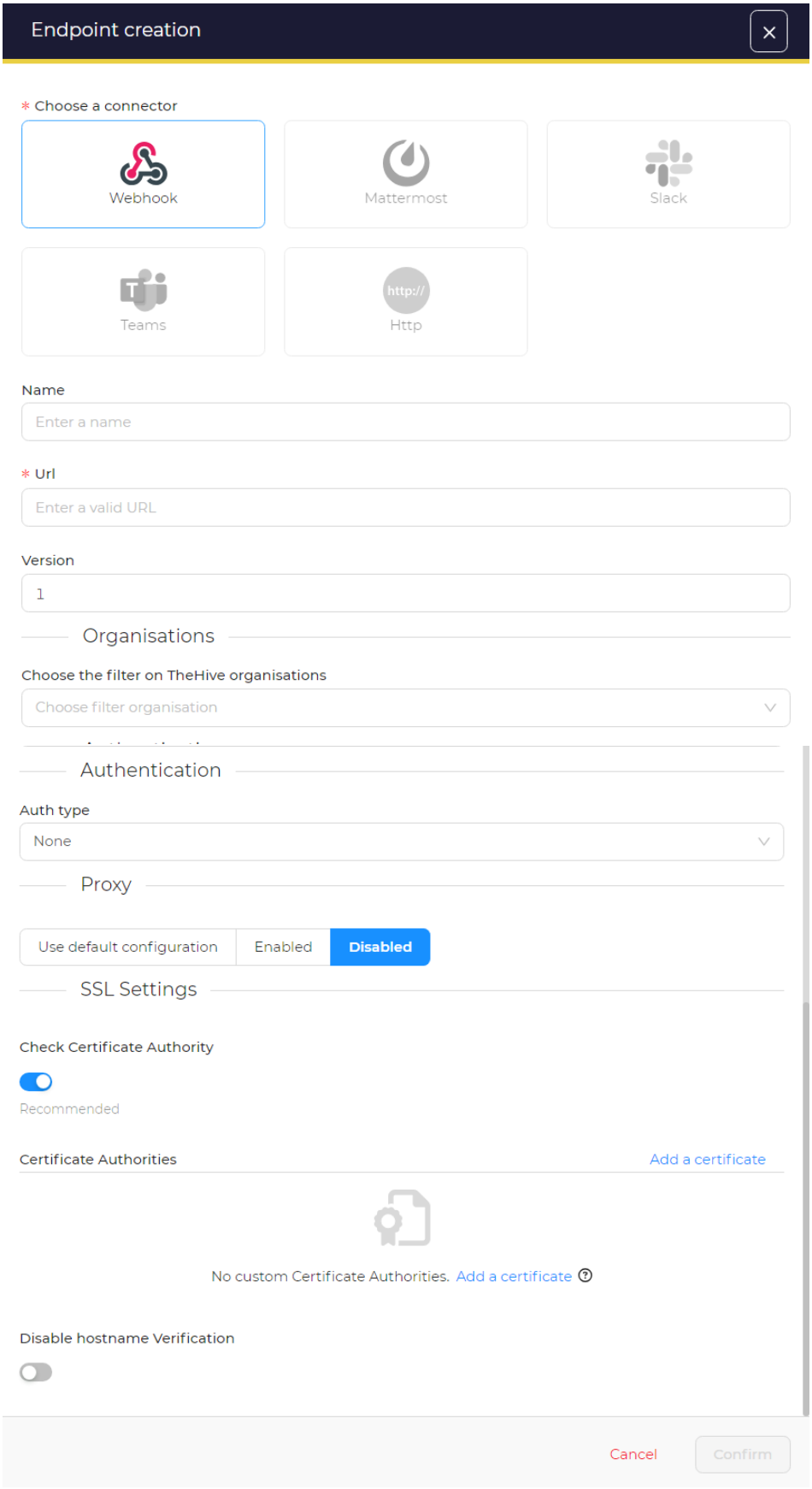


Figure 13.16: Endpoint Creation

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 unmanagable 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 take 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.

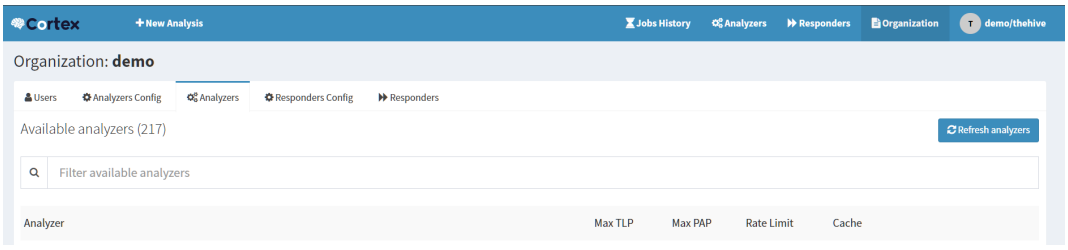


Figure 14.1: Available Analyzers In Cortex

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.

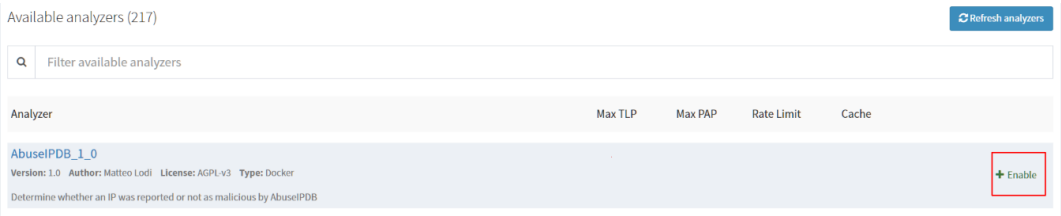


Figure 14.2: Enabling An Analyzer In Cortex

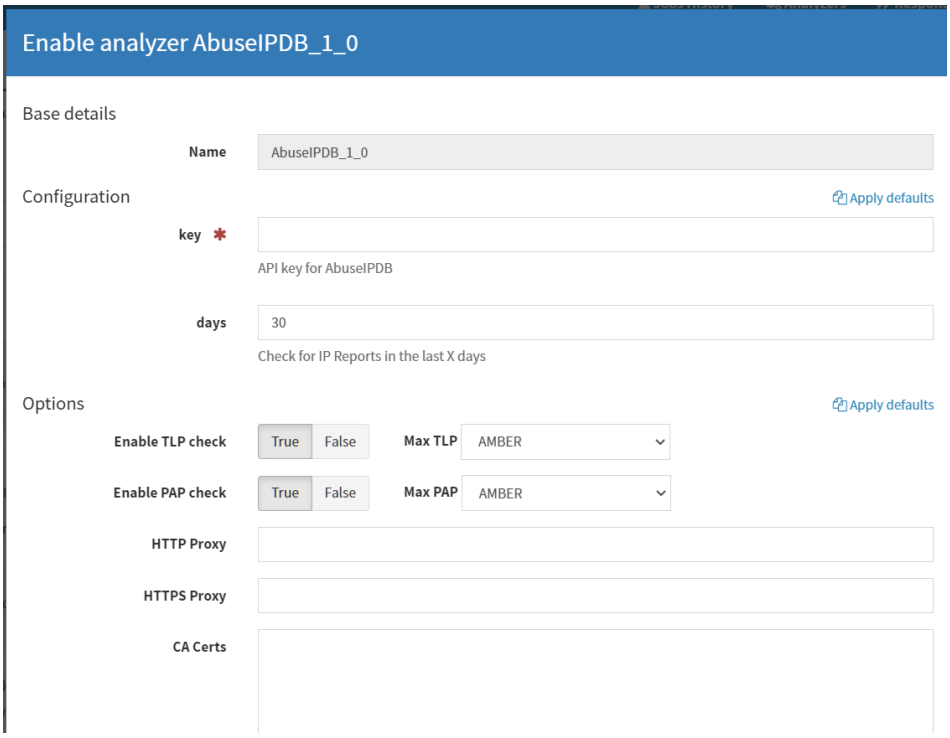


Figure 14.3: Enabling an Analyzer In Cortex Continued

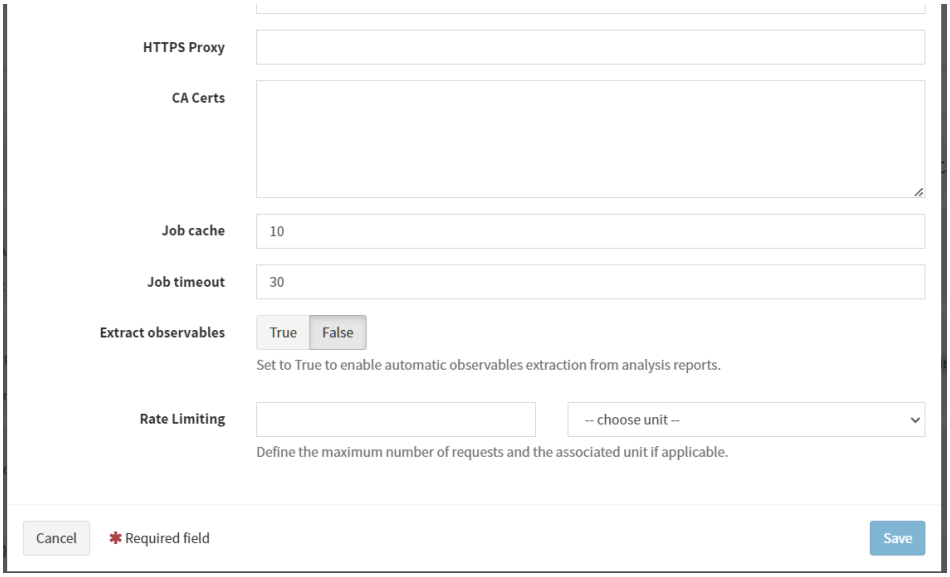


Figure 14.4: Enabling an Analyzer In Cortex Continued

14.2.3 Using Enabled Analyzer From Hive

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

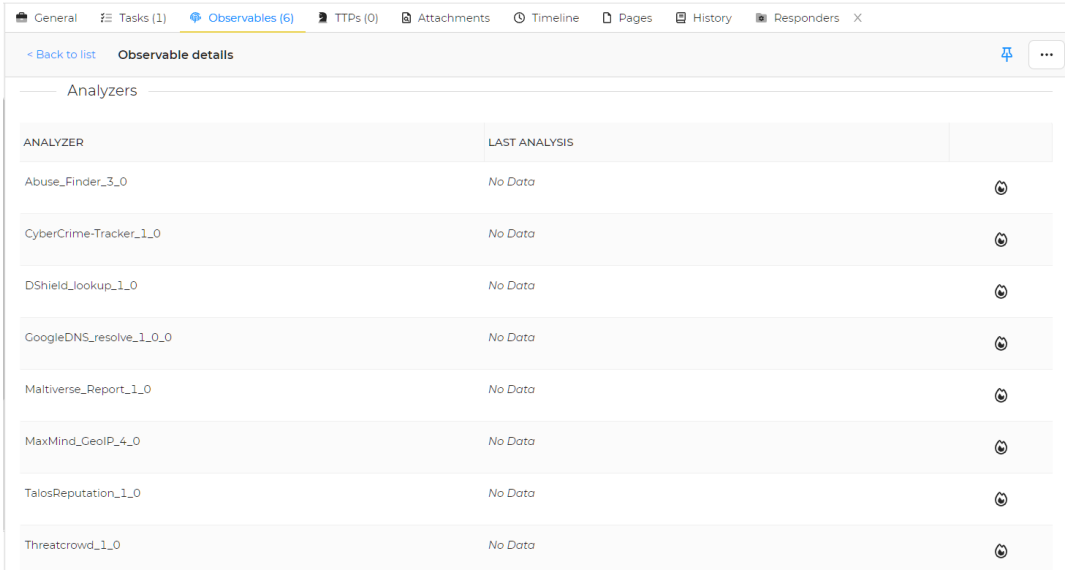


Figure 14.5: Analyzers Available in The Hive-Before

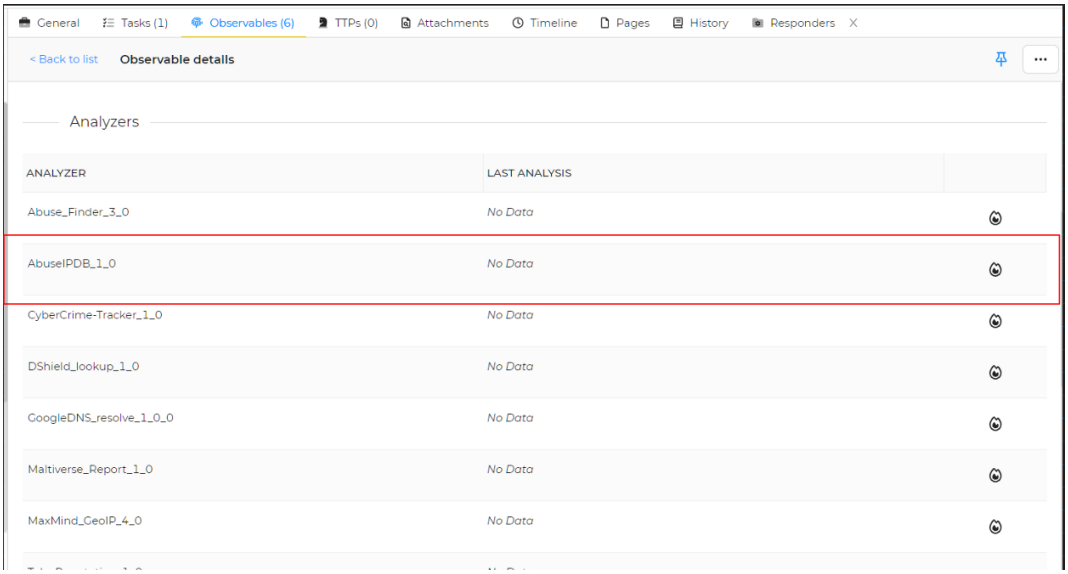


Figure 14.6: Analyzers Available in The Hive-After

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

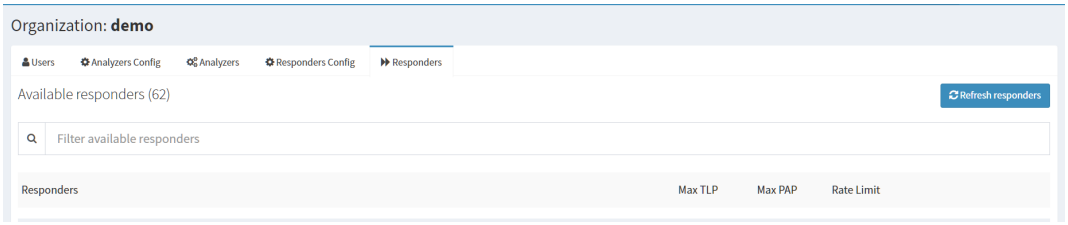


Figure 14.7: Available Responders In Cortex

14.3.2 Enalbling 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.

Figure 14.8: Enabling A Responder In Cortex

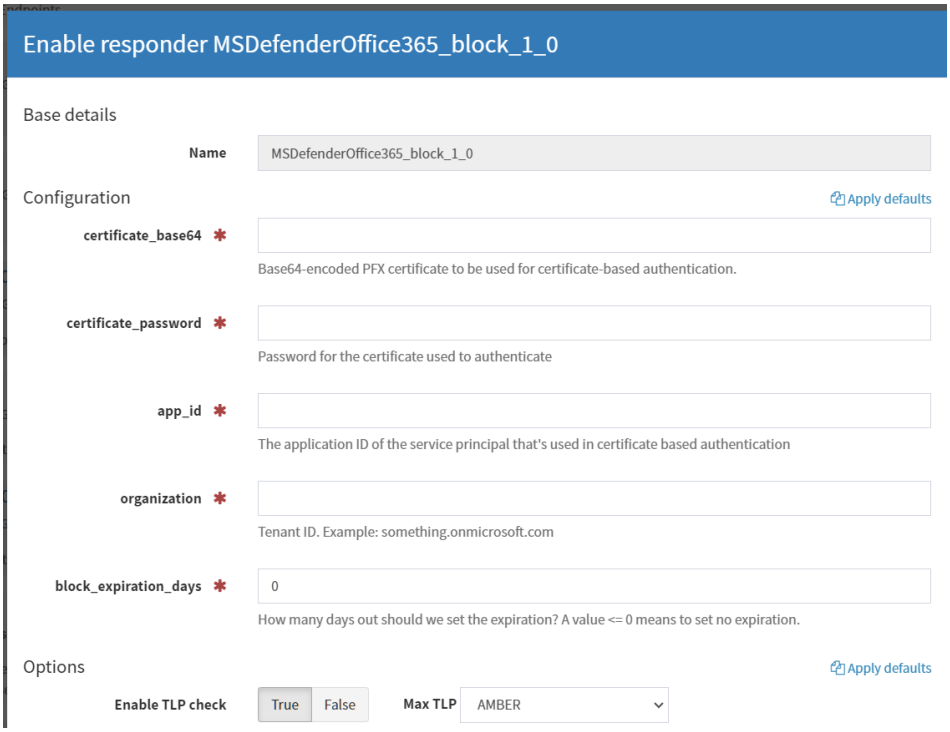


Figure 14.9: Enabling a Responder In Cortex Continued

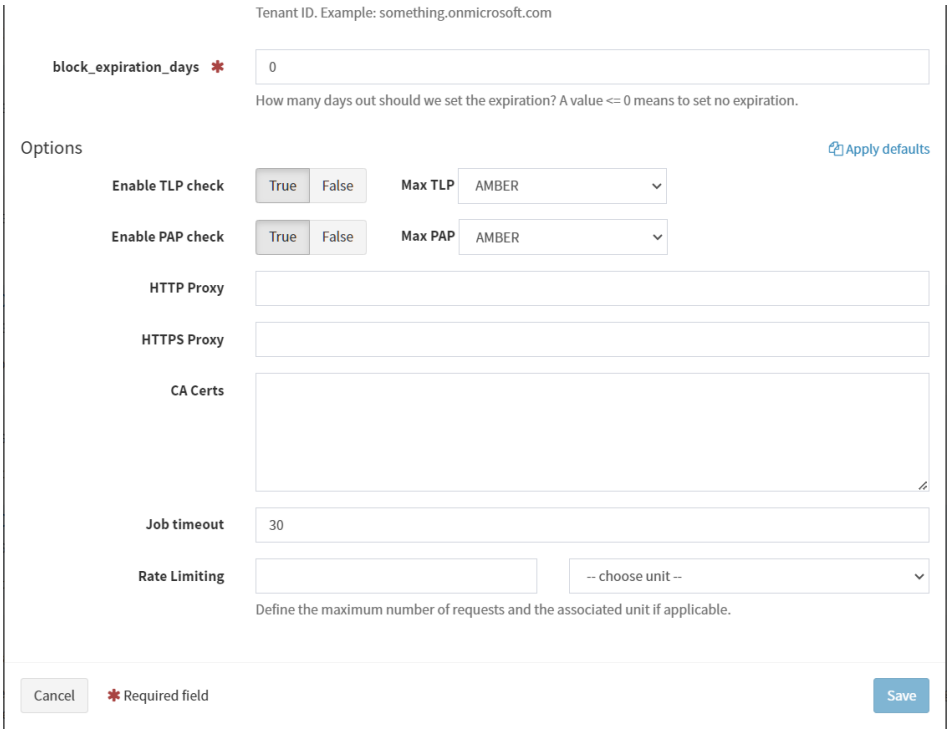


Figure 14.10: Enabling a Responder In Cortex Continued

14.3.3 Using Enabled Responder From Hive

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

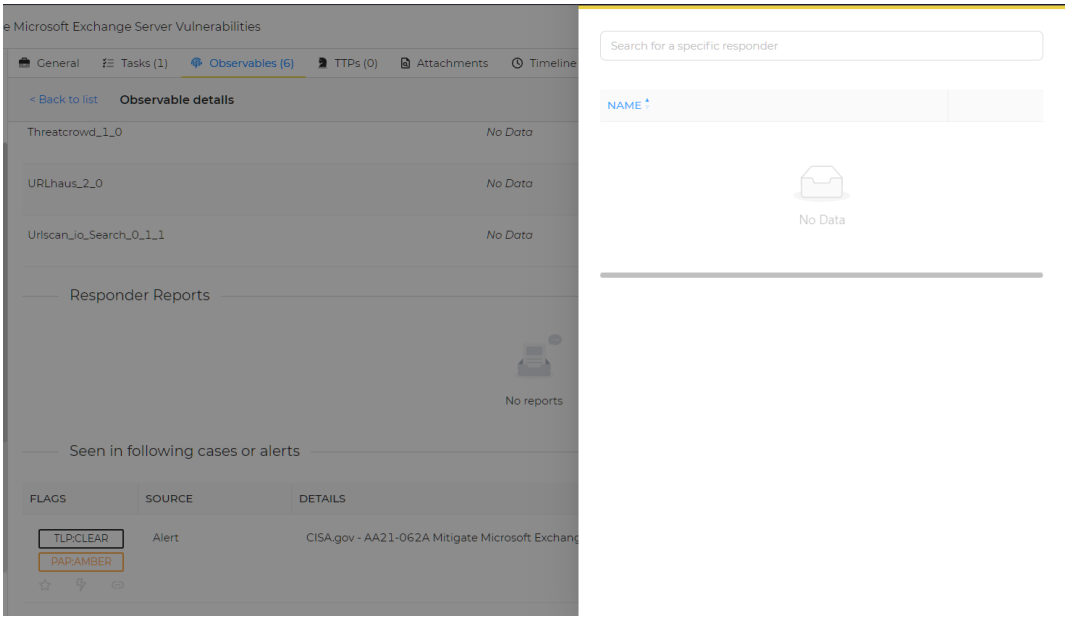


Figure 14.11: Responders Available in The Hive-Before

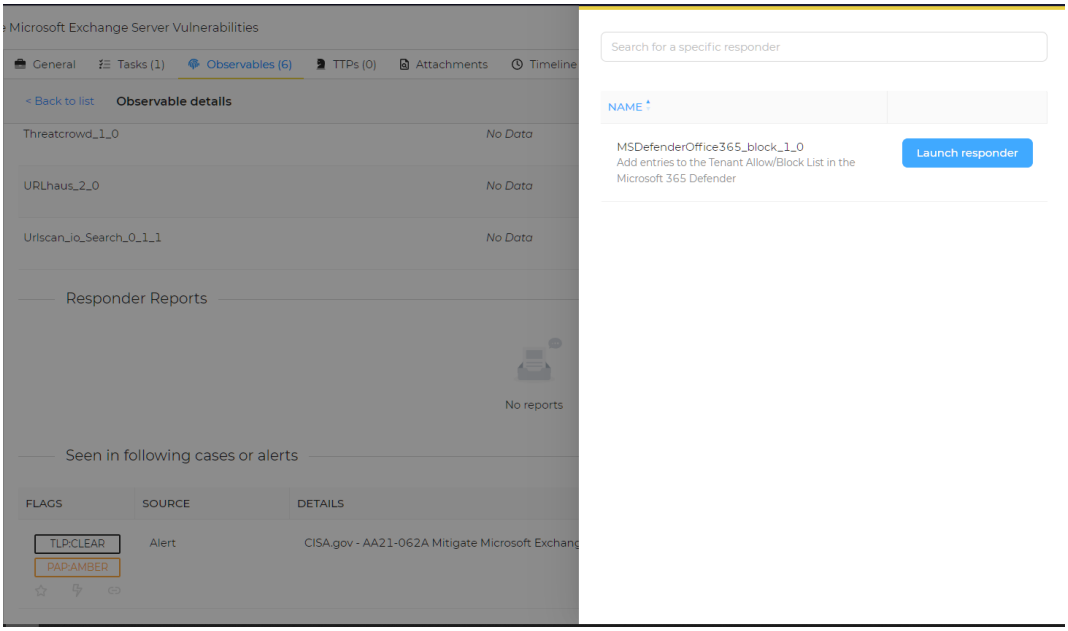


Figure 14.12: Responders Available in The Hive-After

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 facilititates 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

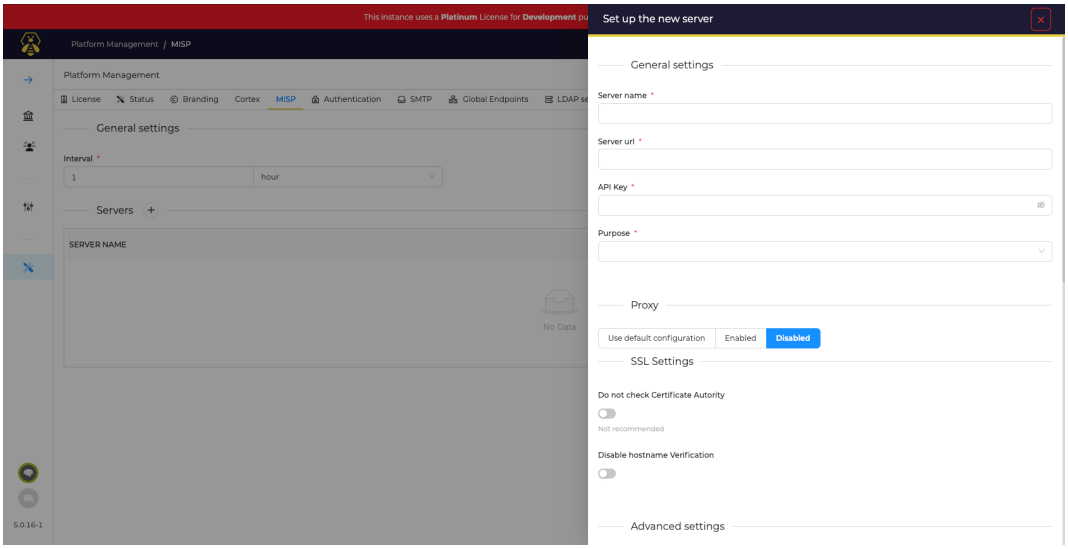
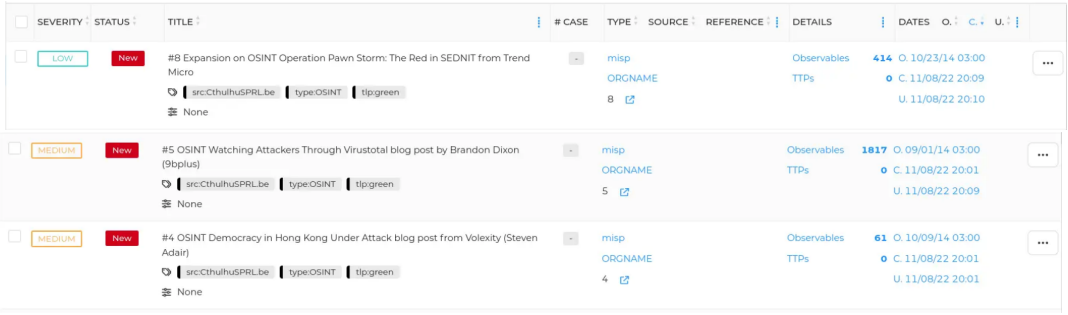


Figure 15.1: Add MISP Server

15.3 MISP Alerts

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



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

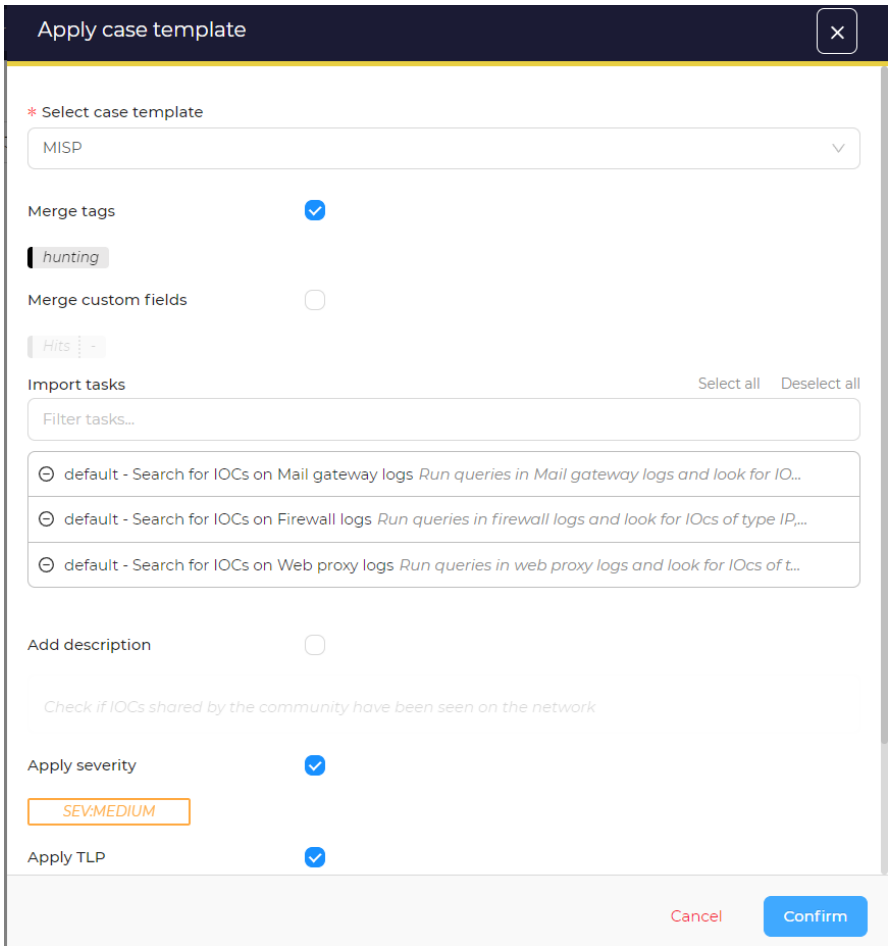


Figure 15.3: Case Creation From MISP Template

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

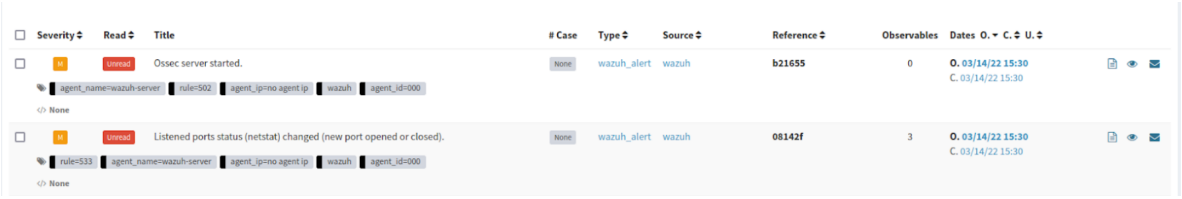


Figure 16.1: Alerts from Wazuh

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/