



Bangladesh University of Engineering and Technology

Project Report on

The Hive: Incident Response Platform

Prepared By

Mohaiminul Islam - 1905018

Tanveer Rahman - 1905025

Department of CSE, BUET

Contents

1	Why TheHive ?	5
1.1	Overview	5
1.1.1	Overview of Features	5
2	Architecture	7
2.1	Organization of Servers	7
2.2	Overall Structure	9
2.2.1	Incident Response with TheHive	10
3	Workflow	11
4	Installation	13
4.1	Install Docker	13
4.2	Create Docker Container	14
4.3	Install The Hive	14
5	Admin Side Management	17
5.1	Organization Management	17
5.1.1	Create Organization	17
5.1.2	Link Organization	18
5.2	User Management	20
5.2.1	Permission and Roles	20
6	Case	21
6.1	Create Case	21
6.1.1	Create Empty Case	22
6.1.2	Create a new case from EDR template	24
6.1.3	Create a new case from Phishing template	25
6.1.4	Create a new case from MISP	26
6.2	Case Properties	27
6.2.1	Tasks	27
6.2.2	Observables	28
6.2.3	TTP	29
6.2.4	Add Tags	30
6.3	Demonstration of a Case Creation	31
6.3.1	Organization and Users	31
6.3.2	Case Creation Page	31
6.3.3	Tasks	33
6.3.4	Observable	34
6.3.5	Analyzer Reports	35
7	Cortex	37
7.1	Cortex: Key Features	37
7.1.1	Automation	37

7.1.2	Analyzer Integration	37
7.1.3	Responder Integration	37
7.1.4	Extensibility	37
7.1.5	Integration with TheHive	37
7.2	Cortex Analyzers	38
7.3	Enabling An Analyzer	39
7.4	Running An Analyzer in Cortex	41
7.5	Raw Report of Analyzer	42
8	Platform Integration	43
8.1	Integration with Cortex	43
8.2	Integration with MISP	44
9	Conclusion	45

Chapter 1

Why TheHive ?

1.1 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.

1.1.1 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 users can view the alert details, make comments, and identify similar alerts.
- **Case Management:** The Hive allows users to create cases and associate them with alerts, tasks, and observables. Users can also define custom statuses and fields for cases.
- **Task Management:** The Hive allows users to create tasks and assign them to users. Users can also track the progress of tasks and set due dates.
- **Observable Management:** The Hive allows users to store and manage a variety of observables, such as IP addresses, domains, and hashes. Users can also define custom observable types.
- **User Management:** The Hive allows users to create and manage user accounts. Users 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 organizations track their incident response activities. This aids in assessing incident response effectiveness.

Chapter 2

Architecture

2.1 Organization of Servers

Each layer, TheHive application, the Database and index engine, and file storage, is independant and can be set up as a standalone node or cluster. As a result, TheHive could be setup and work in a complex clustered architecture, using virtual IP addresses and load balancers. For a **standalone server**, all applications are installed on the same server.

- Cassandra
- Elasticsearch
- Files are store on the filesystem (or MinIO if desired)
- NGINX (optional): to manage HTTPS communications
- TheHive



Figure 2.1: Standalone server

For **Hybrid architecture** we take a different approach. TheHive and all applications of the stack are flexible enough to choose the right setup according with the needs.

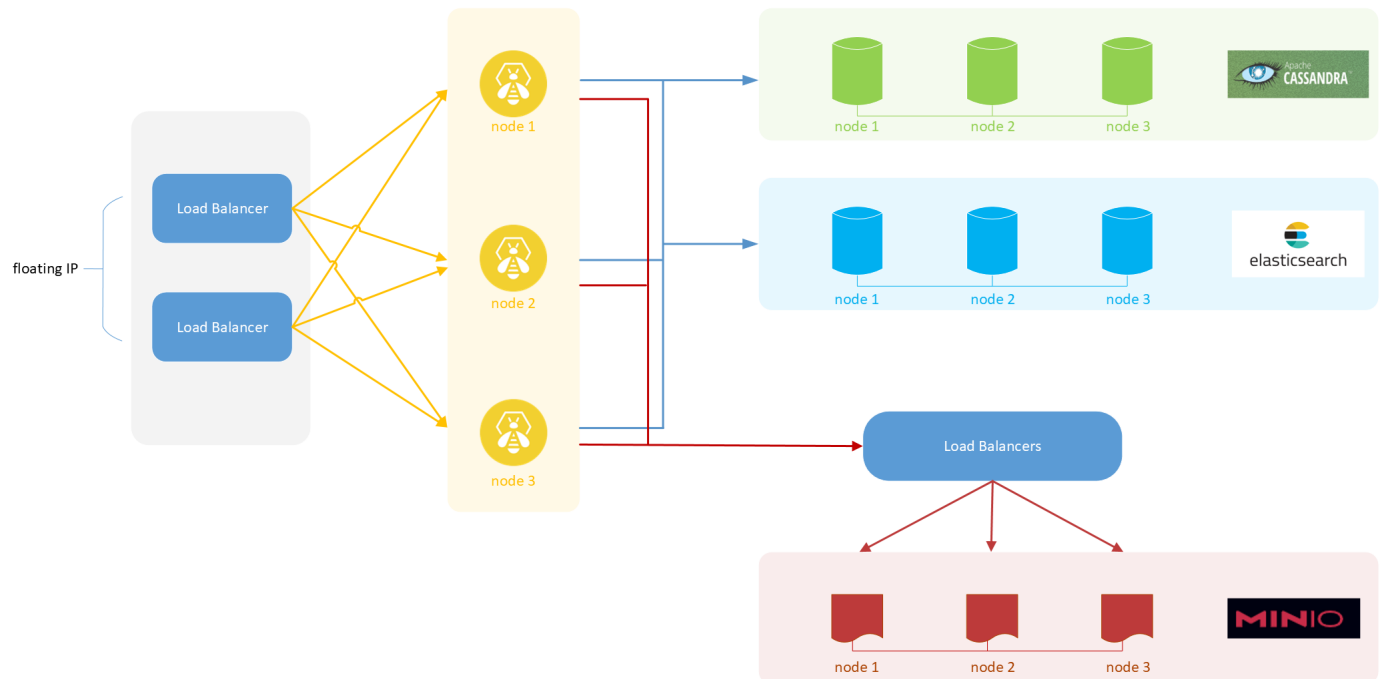


Figure 2.2: Hybrid Architecture

2.2 Overall Structure

TheHive is written in *Scala* and uses *ElasticSearch* to store and access data on the back end. The front end uses *AngularJS* and *Bootstrap*. A number of REST API endpoints are also provided to allow for integrations and bulk actions.

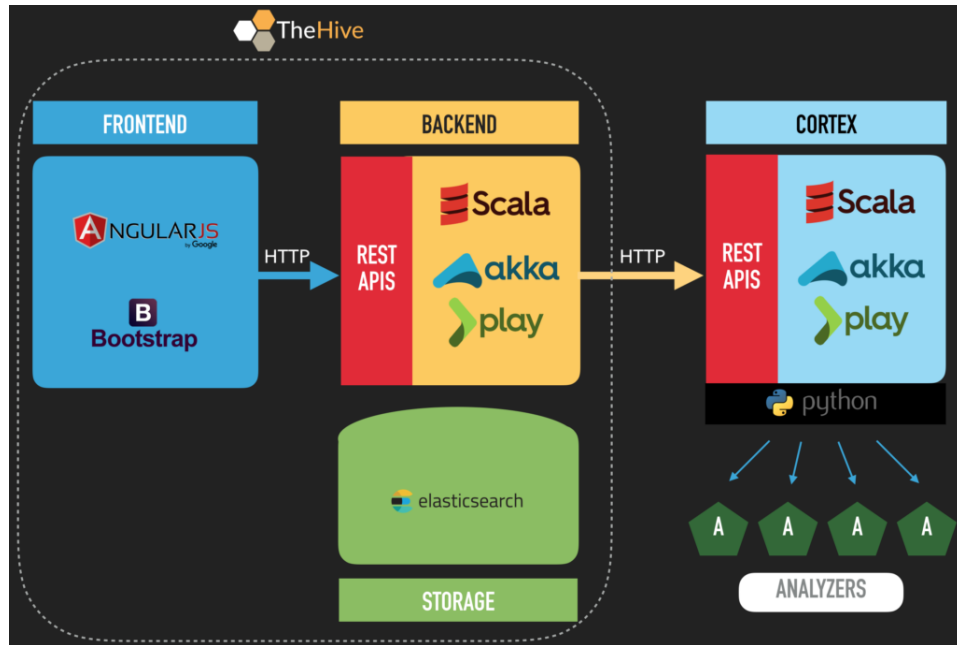


Figure 2.3: TheHive Architecture

- **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 used to process 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:** Analyzers are used to analyze the data from the system. They can perform tasks such as anomaly detection, fraud detection, and trend analysis.

2.2.1 Incident Response with TheHive

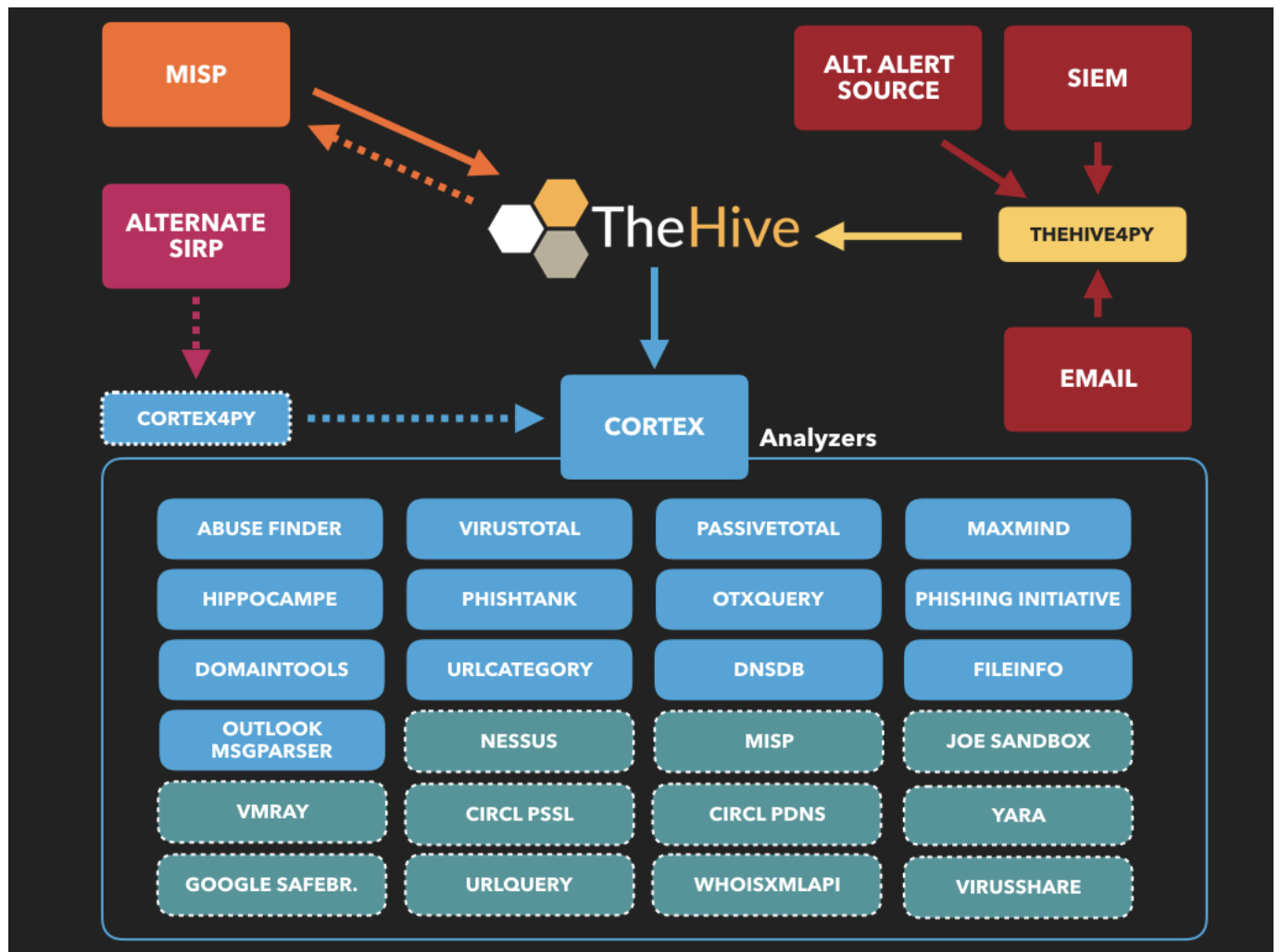


Figure 2.4: TheHive with Cortex and MISP

Workflow



- **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

Installation

We have used docker to install the hive and other related applications like Cortex and MISP. The provided installation is valid for Ubuntu or debian based operating systems.

4.1 Install Docker

- Ensure that your system has the latest information about available software packages

```
sudo apt-get update
```

- Installs necessary packages for securely downloading and installing software from HTTPS sources.

```
sudo apt install apt-transport-https ca-certificates curl gnupg lsb-release
```

- Install a package containing common utilities for adding and managing software repositories.

```
sudo apt install software-properties-common
```

- Create the directory */etc/apt/keyrings* if it does not exist

```
sudo mkdir -p /etc/apt/keyrings
```

- To see the contents of the `/etc/apt/keyrings` directory.

```
ll /etc/apt/keyrings/
```

- Download the Docker GPG key and saves it as `/etc/apt/keyrings/docker.gpg`.

```
curl -fsSL https://download.docker.com/linux/ubuntu/gpg | \
sudo gpg --dearmor -o /etc/apt/keyrings/docker.gpg
```

- Add the Docker repository information to the `docker.list` file in `/etc/apt/sources.list.d/`

```
echo "deb [arch=$(dpkg --print-architecture) signed-by=/etc/apt/keyrings/docker.gpg] \
https://download.docker.com/linux/ubuntu $(lsb_release -cs) stable" | \
sudo tee /etc/apt/sources.list.d/docker.list > /dev/null
```

- Updates the package lists to include the Docker repository.

```
sudo apt update
```

- Install Docker and related packages.

```
sudo apt-get install docker-ce docker-ce-cli containerd.io docker-compose-plugin
```

4.2 Create Docker Container

Docker Installation is Done. For checking the Docker Info:

```
sudo docker info
```

To create new Docker Container :

```
sudo docker run hello-world
```

4.3 Install The Hive

- Create a new directory named 'TheHive' in the current working directory.

```
mkdir 'TheHive'
```

- Go to the directory

```
cd 'TheHive'
```

- Creates an empty file named 'docker-compose.yaml' in the current working directory.

```
touch docker-compose.yaml
```

- Copy contents from the provided link to the .yaml file. [GitHub Link](#)
- If your System does not have the docker-compose plugin then install it.
 - To check if the plugin is available:

```
docker-compose -version
```

- If not installed then install it

```
sudo apt-get install docker-compose-plugin
```

- Execute the Docker Compose command to start the services defined in the 'docker-compose.yaml' file in detached mode (-d).

```
sudo docker-compose up -d
```

After completing the installation, The Hive will be opened at [The Hive](#).

Reference Videos:

1. [Install Docker](#)
2. [The Hive installation](#)

Chapter 5

Admin Side Management

TheHive is a web application that can be installed on a server and accessed from a web browser. It has a web-based administration interface that allows administrators to configure the tool according to their needs. TheHive allows administrators to create multiple organizations within the tool. Each organization can have its own set of users, roles, permissions, and notifications. This allows for better separation of duties and responsibilities between different teams within an organization, such as a SOC team and a CSIRT team.

5.1 Organization Management

5.1.1 Create Organization

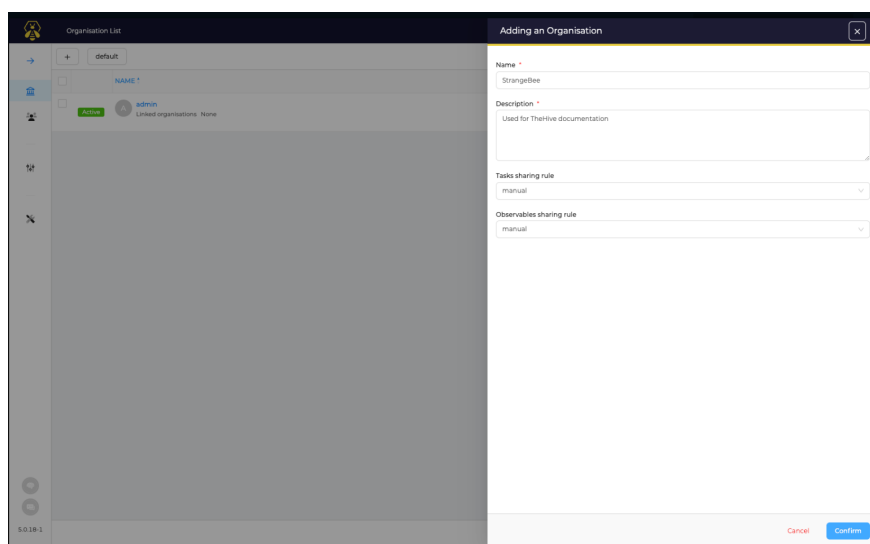
The screenshot shows the 'Adding an Organisation' modal in TheHive. The modal is a light gray box with a dark header bar containing a close button (X). The main content area is white and contains several form fields: 'Name' (a text input field with 'Strangerbee' entered), 'Description' (a text area with 'Used for Thehive documentation'), 'Tasks sharing rule' (a dropdown menu with 'manual' selected), and 'Observables sharing rule' (a dropdown menu with 'manual' selected). At the bottom right of the modal are 'Cancel' and 'Confirm' buttons. In the background, the 'Organisation List' interface is visible, showing a table with columns for 'Name', 'Status', and 'Users'. The table has one row with 'Strangerbee' as the name, 'Active' as the status, and 'admin' as the user. The left sidebar of the application is also visible, showing navigation icons for Home, Organizations, Users, Tasks, and Observables.

Figure 5.1: Create Organization

To create an organization:

- Click on the + button
- Fill up the necessary fields
- Click on Confirm

5.1.2 Link Organization

By default, organisations are not linked each other: each one does not know about the others on the instance. So, we can link organizations so that two organizations can also collaborate with each other.

In order to create Link between organizations,

- Click on the **Linked Organizations** tab in the detailed view
- Click on **Manage linked Organisations**

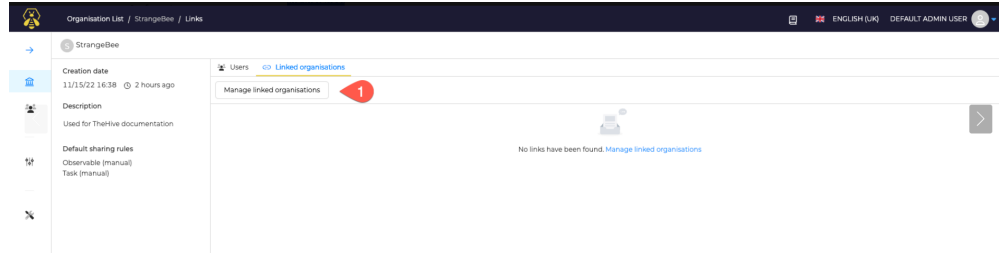


Figure 5.2: Manage Linked Organizations

Select the organizations to be linked with each other and the details page is viewed in fig 5.3.

Three types of links are available. They are :

- **Default:** Cases created by the current Organisation will not be shared with the other one
- **Supervised:** Cases created by the current Organisation will be automatically shared with the other one, with the profile Analyst
- **Notify:** Cases created by the current Organisation will be automatically shared with the other one, with the profile Read-only

Manage linked organisations

Filter by organisation name

StrangeBee

→

default - Cases created by StrangeBee will not be automatically shared with

default - Cases created by StrangeBee will not be automatically shared with

supervised - Cases created by StrangeBee will be automatically shared with

with profile analyst.

notify - Cases created by StrangeBee will be automatically shared with

with profile read-only.

StrangeBee

→

default - Cases created by StrangeBee will not be automatically shared with

StrangeBee

←

default - Cases created by StrangeBee will not be automatically shared with

StrangeBee

→

Choose a link type

StrangeBee

←

Choose an other link type

StrangeBee

→

Choose a link type

StrangeBee

←

Choose an other link type

Figure 5.3: Form for Link Management

5.2 User Management

TheHive allows administrators to create multiple user accounts within the tool. Each user account can have its own set of roles and permissions. Accounts can be created or edited from several places in TheHive:

- As Administrator, in the Users view
- As Administrator in the detailed page of an Organisation
- As Org-admin, in the Organisation configuration page
- As Administrator of the platform, open the Users page.

5.2.1 Permission and Roles

Users are given Permissions by their roles. Permissions are defined for each entity of the application. The following entities are available:

- **Admin:** Administrators have full control over TheHive platform. They can create, modify, and delete accounts, organizations, and configurations. Administrators typically manage the overall settings and ensure the platform functions smoothly. Their privileges:
 - Full access to all features and functionalities.
 - User and organization management.
 - Configuration and system settings control.
 - Incident case management.
- **Analyst:**Analysts are standard users responsible for working on incident cases and investigations within TheHive. They have access to case management and analysis tools to investigate and respond to security incidents. Their privileges:
 - Access to incident case management
 - Ability to work on and update cases.
 - Collaboration with other analysts.
 - Limited access to system configurations.
- **Org-admin** (*Organization Administrator*): Organization administrators have administrative privileges limited to a specific organization within TheHive. They can manage users, incidents, and configurations for their assigned organization. Their privileges:
 - User management within their organization.
 - Incident case management within their organization.
 - Limited access to system-wide configurations
 - May not have access to other organizations' data.
- **Read-only** Read-only users have limited access and are primarily meant for users who need to view incident cases and data without making changes or updates. They can review and gather information but cannot modify cases. Their privileges:
 - View-only access to incident cases and data
 - Cannot modify or update cases.
 - Limited interaction with the platform

Chapter 6

Case

A case provides information on suspicious activity in the environment. Security analysts can conduct specific analysis based on cases to assess the possibilities of threats.

6.1 Create Case

The Header has a button named **CREATE CASE** +.



Figure 6.1: Create Case +

A new screen opens and from this screen we can open new cases.

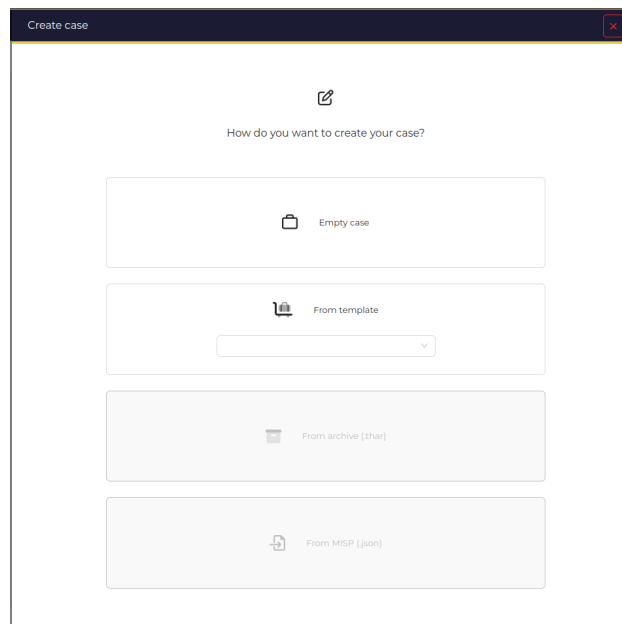


Figure 6.2: New page for Create Case

6.1.1 Create Empty Case

Create a new empty case after filling up the necessary information.

The screenshot shows a 'Create case' form with the following sections:

- Title:** A text input field with placeholder 'Case title...'.
- Date:** A date and time picker showing '20/02/2024 23:57'.
- Severity:** Four buttons: LOW, MEDIUM (selected), HIGH, and CRITICAL.
- TLP:** Five buttons: TLP:CLEAR, TLP:GREEN, TLP:AMBER (selected), TLP:AMBER+STRICT, and TLP:RED.
- PAP:** Four buttons: PAP:CLEAR, PAP:GREEN, PAP:AMBER (selected), and PAP:RED.
- Tags:** A text input field with placeholder 'Tags'.
- Description:** A rich text editor with a toolbar (bold, italic, underline, link, list, etc.) and a 'Preview' button.
- Footer:** Tabs for 'Tasks', 'Custom fields', and 'Pages'. Below the tabs is a message: 'No tasks have been found. Add a task'. At the bottom right are 'Cancel' and 'Confirm' buttons.

Figure 6.3: Create empty case

PAP(Permissible Actions Protocol)

Defines what actions you can take with the information without alerting the attacker.

- **White:** No restrictions. Any action can be taken openly.
- **Green:** Active actions like blocking IPs are okay. But avoid actions that might reveal your awareness of the attack, like sending honeypots.
- **Amber:** Only passive actions like monitoring are allowed. Don't interact with the attacker directly.
- **Red:** No detectable actions. Treat the information as highly sensitive and keep all analysis hidden.

TLP (Traffic Light Protocol)

TLP defines the confidentiality level of information within the case

- **White:** Public information, freely distributable.
- **Green:** Internal use only, within your organization.
- **Amber:** Limited distribution outside your organization, with specific need-to-know basis
- **Red:** Classified information, restricted to a very small group with strict control.

Tasks

- Tasks are specific actions to be taken during the investigation and response process for a case.
- They offer a structured way to assign responsibilities, track progress, and ensure all necessary steps are completed.

Custom Fields

- Custom fields extend the default information captured in a case to accommodate specific needs or workflows.
- These fields allow capturing additional context relevant to the incident, like affected systems, impact level, or mitigation actions taken.
- Custom fields enhance data collection, reporting, and filtering capabilities within TheHive.

6.1.2 Create a new case from EDR 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.

Create case from template: Worm infection (CERT-SG 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:SLM:malicious-code="worm"

Description
Worm infection

Tasks Custom fields Pages Sharing

Add a task

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

Cancel Confirm

Figure 6.4: Case from EDR Template

6.1.3 Create a new case 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: Custom fields Pages Sharing

Add a task

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

Cancel Confirm

Figure 6.5: Case from Phishing Template

6.1.4 Create a new case from MISP

Files exported from MISP can be used to create new Case in Hive. The MISP file exported as .json and then uploaded to create a new case

The screenshot shows a modal window titled "Import from MISP". At the top left is a back arrow icon, and at the top right is a close button (X). Below the title bar, there is a section labeled "File *" with a red asterisk. Underneath this is a large, light gray box labeled "Attachment". Below the attachment box are two tabs: "Tasks" (which is selected and underlined in blue) and "Custom fields". In the "Tasks" tab area, there is a printer icon and the text "No tasks have been found. Add a task". To the right of this text is a blue button labeled "Add a task". At the bottom of the modal, there are two buttons: a "Cancel" button on the left and a "Confirm case creation" button on the right.

Figure 6.6: Case from MISP

6.2 Case Properties

6.2.1 Tasks

The task feature in TheHive is a crucial component for managing the investigation process within a case. It allows the user to break down the investigation into smaller, actionable steps, ensuring a structured and efficient approach.

Why Task ?

- Structured Approach
- Improved Collaboration
- Accountability
- Improved Communication

The tasks are defined by the organization manager. They are grouped together for better Communication and collaboration.

The organization manager can assign certain task to a certain analyst and can give a deadline for the completion of the task. Thus, proper accountability is maintained.

Tasks can be prioritized based on their urgency and importance to the overall investigation.

Each task can have its own dedicated comment section. This enables analysts to discuss the task, share findings, and collaborate effectively. Analysts can document their actions and findings related to the task by adding logs.



Figure 6.7: Task Page

6.2.2 Observables

Observables represent stateful properties or measurable events that are pertinent to the operation of computers and networks. The IP of the Source, the Destination IP, the PCAP files all can be added as observables.

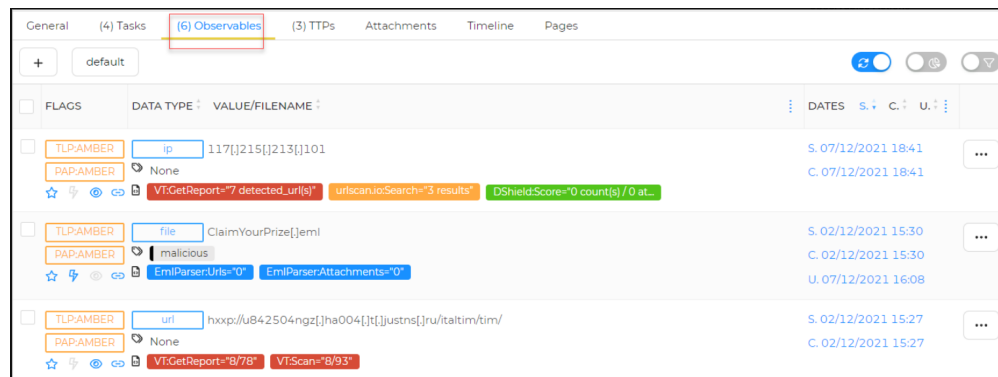


Figure 6.8: Observables

The create observables has the PAP, TLP, fields like before. It also has some special fields. Like:

- **Is IOC** This is a button, that can be turned on or off. IOC means *Indicator of Compromise*. This allows the users to centralize evidence and track potential malicious activity effectively.
- **Ignore Similarity** This is also a button. Which determines whether we want to co-relate this observable with other existing observables.
- **Has Been Sighted** Button that serves the purpose of checking if the observable has already sighted in the system or if it has assigned before.

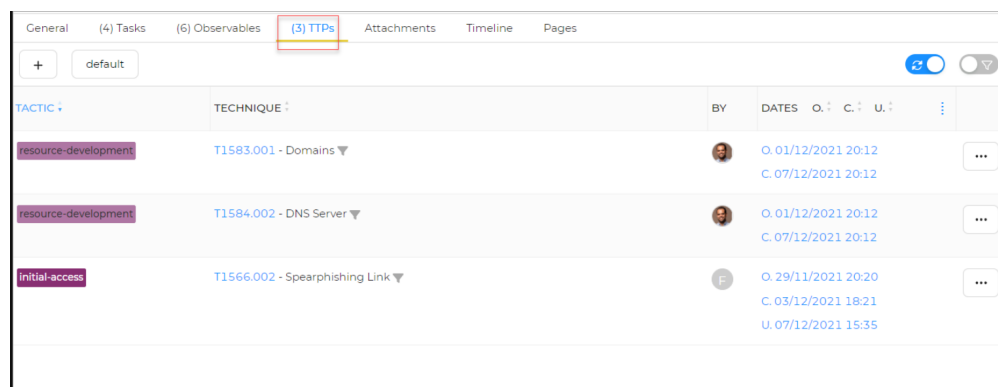
We can perform various actions over the observables, like:

- Delete
- Run Analyzers
- Export - To download the observable
- Copy

6.2.3 TTP

TTP stands for *Tactics, Techniques, and Procedures*. These represent the specific methods attackers employ to carry out their malicious activities.

1. **Tactics** Broad approaches or goals attackers aim to achieve during an attack (e.g., initial access, persistence, privilege escalation, data ex-filtration).
2. **Techniques** Specific tools and methods attackers use to implement their tactics (e.g., phishing emails, exploiting vulnerabilities, installing malware).
3. **Procedures** Step-by-step instructions that detail how attackers execute their techniques (e.g., crafting a social engineering email, deploying a specific exploit kit).



TACTIC	TECHNIQUE	BY	DATES	O	C	U	
resource-development	T1583.001 - Domains		O 01/12/2021 20:12 C 07/12/2021 20:12				...
resource-development	T1584.002 - DNS Server		O 01/12/2021 20:12 C 07/12/2021 20:12				...
initial-access	T1566.002 - Spearphishing Link		O 29/11/2021 20:20 C 03/12/2021 18:21 U 07/12/2021 15:35				...

Figure 6.9: TTP

The use of TTP :

1. Improves Threat Detection
2. More Effective Response
3. Proactive Mitigation - By studying TTPs, security teams can develop preventive measures to thwart attacks that rely on those methods.

6.2.4 Add Tags

- Choose tags from the Taxonomy. The selected tag will appear in the Selected Tags box
- Click the Add selected tags button.

Select tags from library

Selected tags: (1)

Clear selection

circl:incident-classification="phishing"

Choose tags from taxonomy: circl

Choose another taxonomy

Filter tags...

☒ circl:incident-classification="phishing" ?

☐ circl:topic="individual" ?

☐ circl:incident-classification="system-compromise" ?

☐ circl:incident-classification="screenlocker" ?

☐ circl:incident-classification="sabotage" ?

☐ circl:incident-classification="sql-injection" ?

☐ circl:incident-classification="covid-19" ?

☐ circl:topic="finance" ?

Add selected tags

Figure 6.10: add Tags

6.3 Demonstration of a Case Creation

6.3.1 Organization and Users

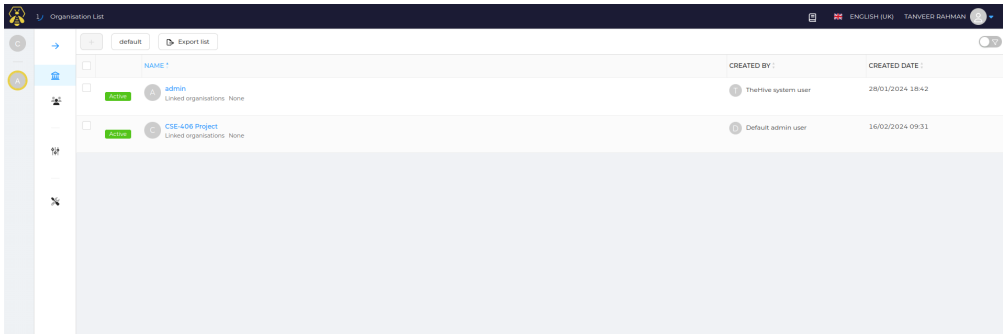


Figure 6.11: Newly created CSE-406 organization

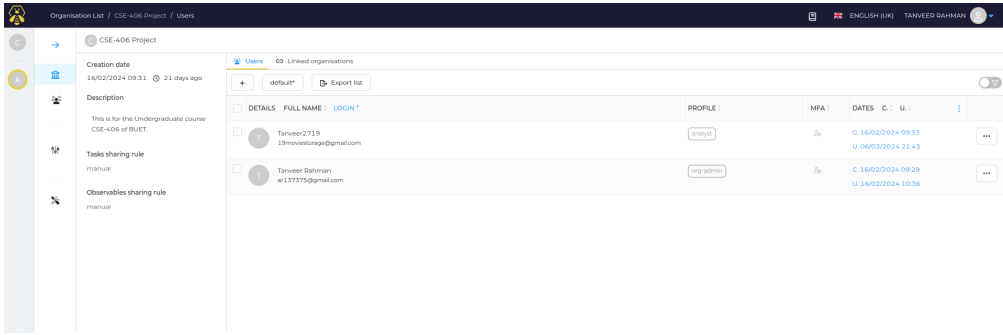


Figure 6.12: Users of CSE-406

6.3.2 Case Creation Page

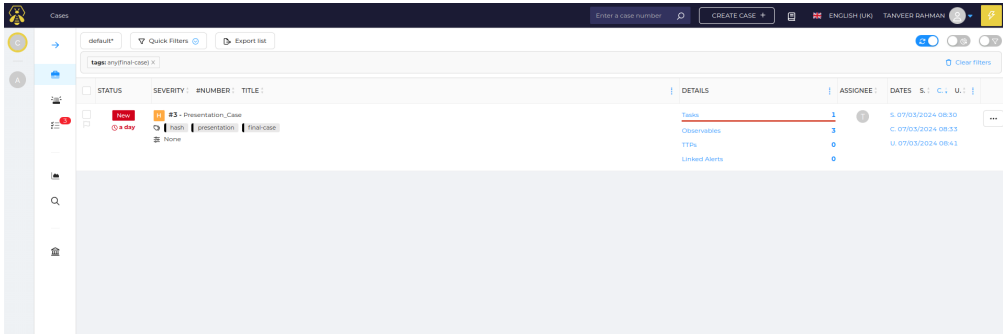


Figure 6.13: Cases of CSE-406

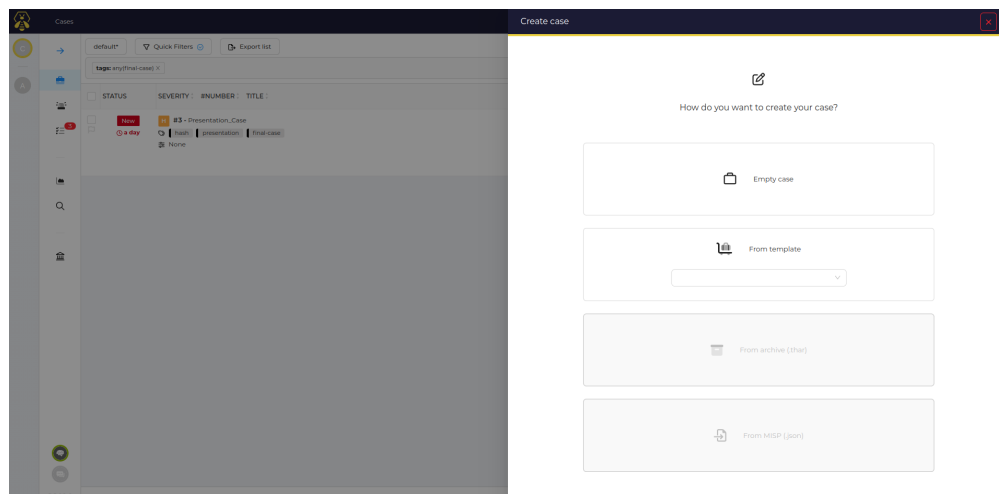


Figure 6.14: Create case

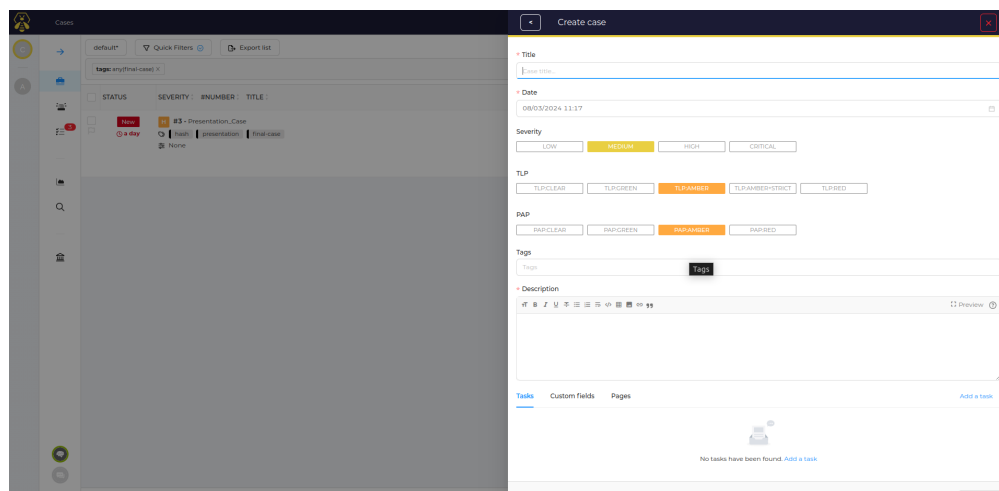


Figure 6.15: Empty case

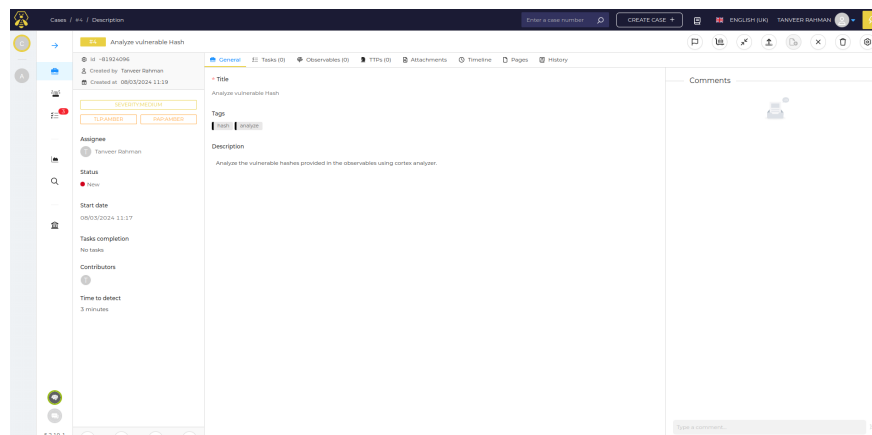


Figure 6.16: Newly Created case

6.3.3 Tasks

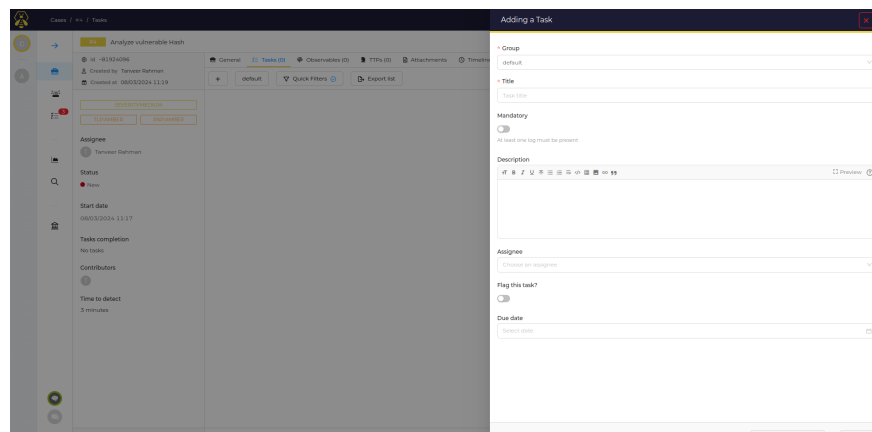


Figure 6.17: Add Task to the case

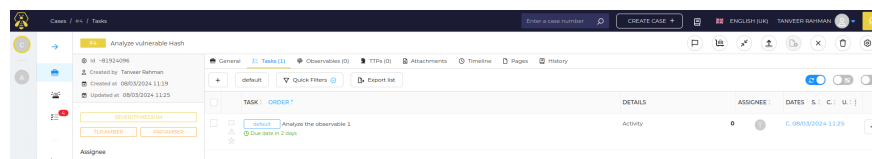


Figure 6.18: Tasks of the case

6.3.4 Observable

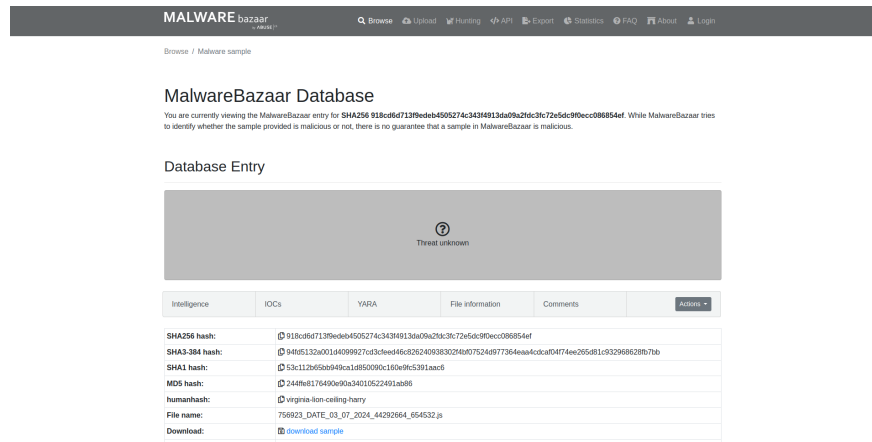


Figure 6.19: Get Hash from MalwareBazar

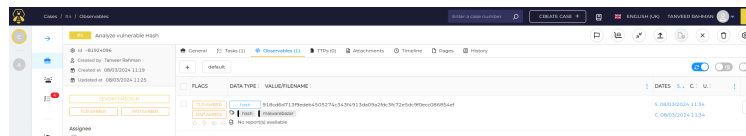


Figure 6.20: Observables List

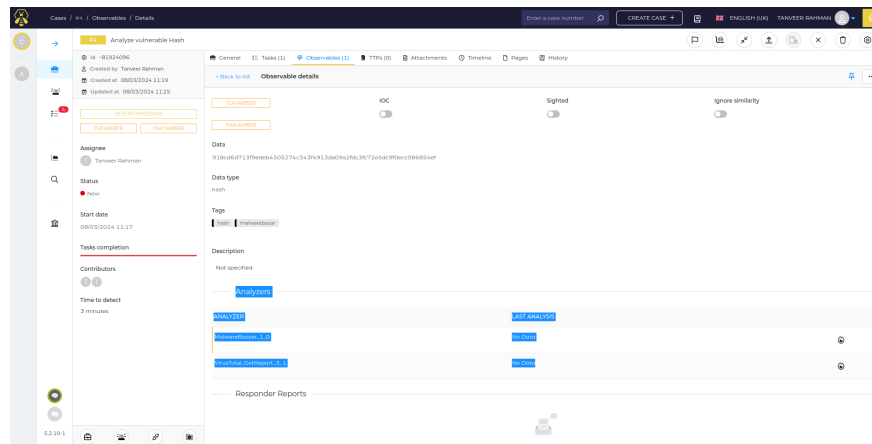


Figure 6.21: Analyze Observable

6.3.5 Analyzer Reports

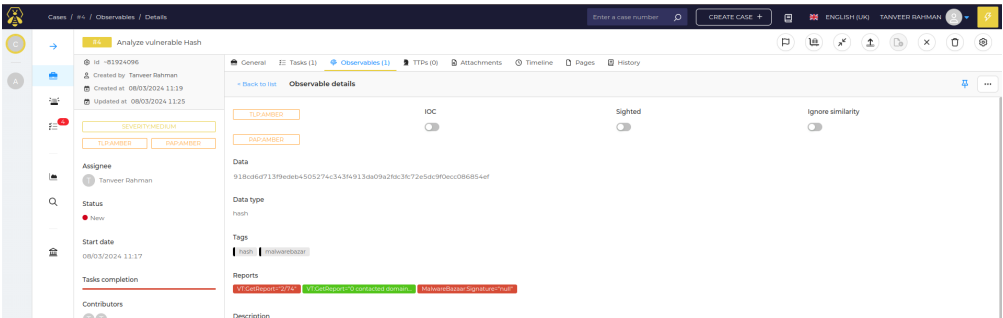


Figure 6.22: Analyzer Reports

After clicking the report we want to view, we get the report generated by the analyzer.

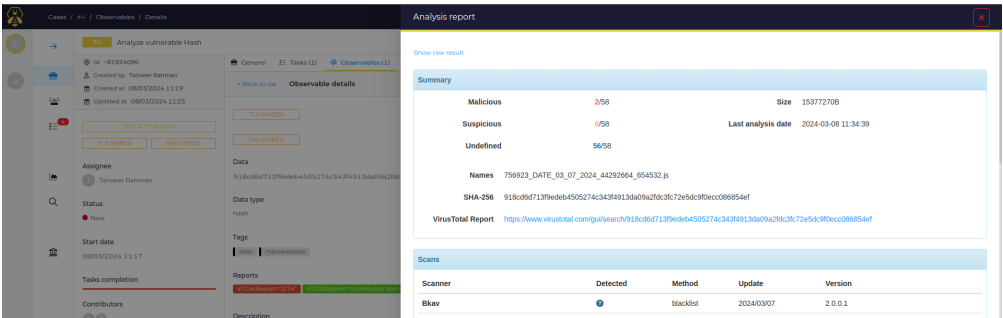


Figure 6.23: View Report

Chapter 7

Cortex

Cortex is a software project that complements and extends the capabilities of TheHive, a security incident response platform. It serves as an automation and orchestration engine. It automates the execution of various analysis tasks and security operations related to incident response by making api calls to various threat intelligence feeds and collects their outputs.

7.1 Cortex: Key Features

7.1.1 Automation

Cortex allows users to define and execute a wide range of actions, such as analyzing observables, querying threat intelligence feeds such as VirusTotal, CyberCrime-Tracker etc. and interacting with other security tools and services.

7.1.2 Analyzer Integration

Cortex includes a collection of analyzers, which are plugins, enabled by adding API key, can be used to analyze different types of observables, for example, IP addresses, urls, hashes etc. These analyzers can be integrated into TheHive through Cortex and automatically perform tasks like malware analysis, DNS lookups etc. The generated reports can be shared with other security analysts of the organization which saves analysts time and standardize the investigation process.

7.1.3 Responder Integration

Responders are plugins that can take action based on the analysis results. For example, if an analyzer detects a malicious URL, a responder can be configured to block the URL at the firewall or update an indicator of compromise blacklist.

7.1.4 Extensibility

Cortex allows organizations to develop custom analyzers and responders tailored to their specific needs. This flexibility makes it a valuable tool for organizations with unique security requirements.

7.1.5 Integration with TheHive

By integrating cortex with TheHive, it is easy to automate analysis and response actions into TheHive's case management and incident tracking workflows.

7.2 Cortex Analyzers

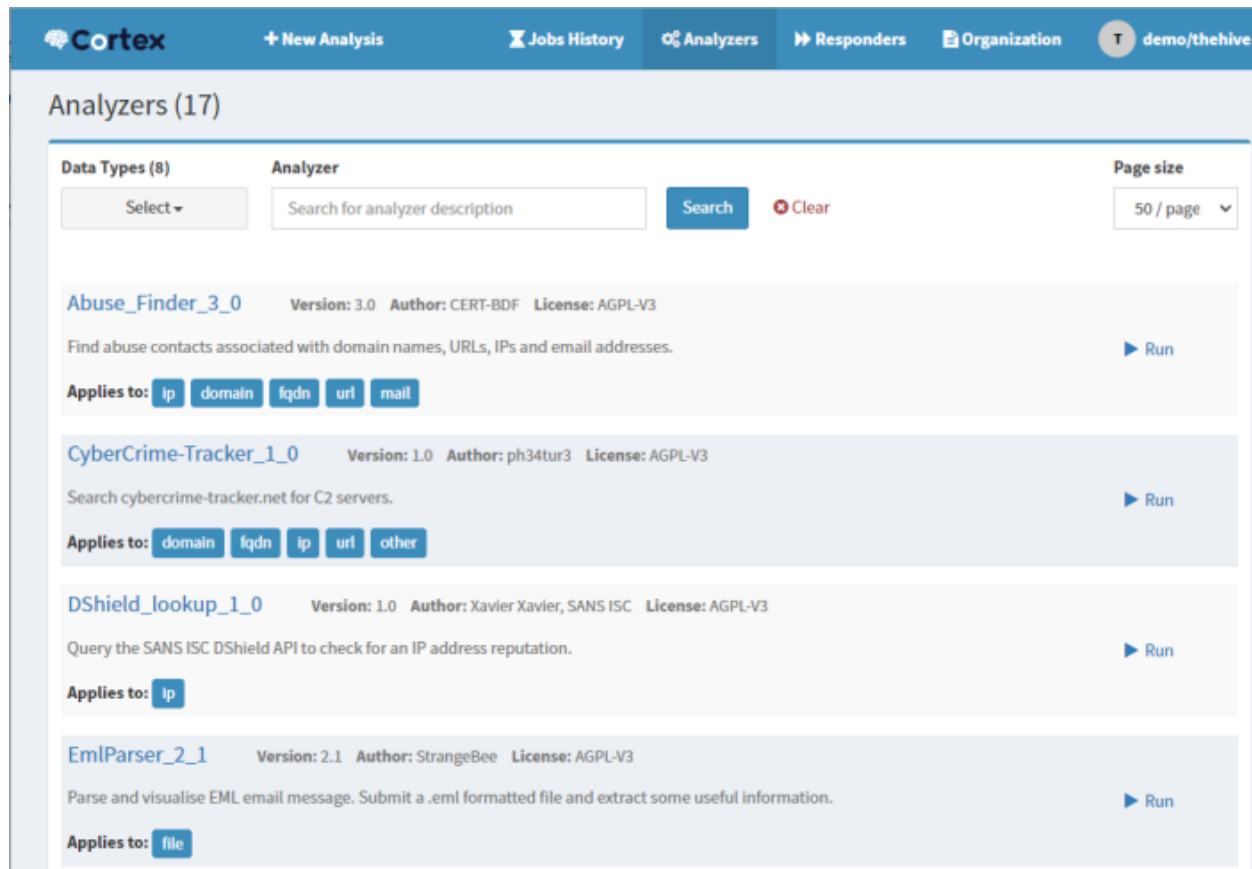


Figure 7.1: Cortex Analyzers

We have used total of 216 analyzers available and 16 of them are enabled with API key. To enable a new Analyzer, we just need to add the API key for that. A snapshot of some of the Analyzers from Cortex is shown below.

7.3 Enabling An Analyzer

In the Organization tab of Cortex, all the available analyzers are provided. To enable an analyzer, press the enable button.

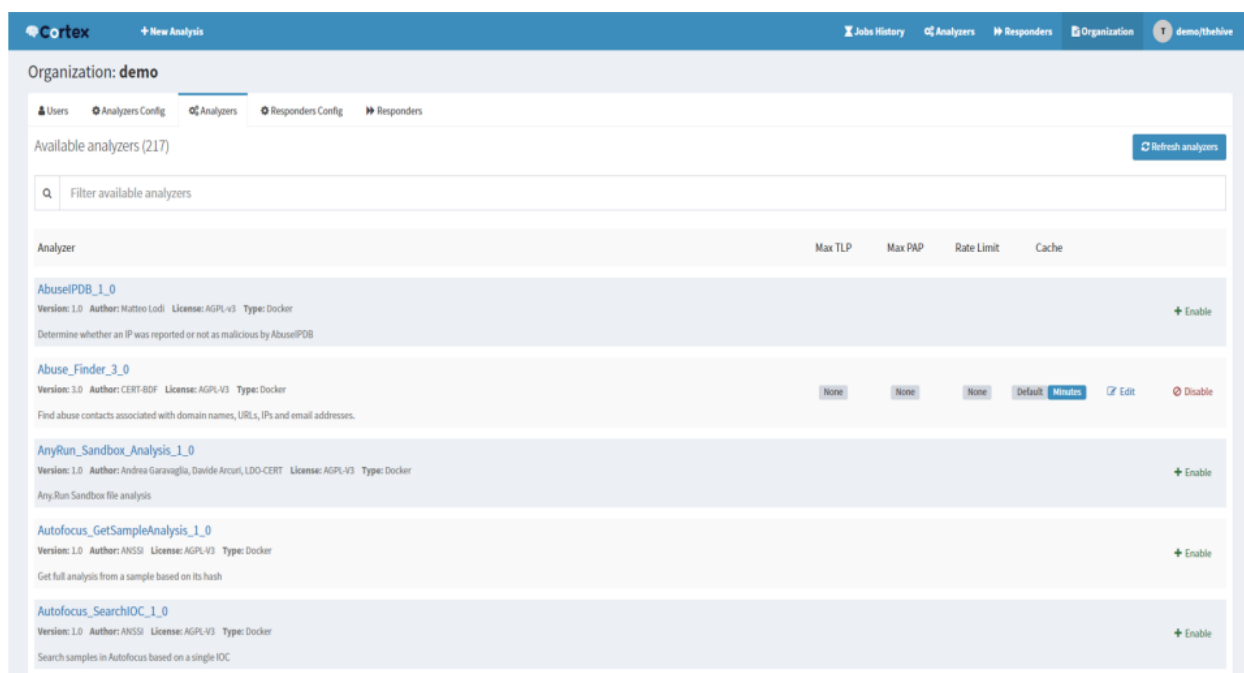


Figure 7.2: Enabling An Analyzer

The following box will be shown after pressing the enable button. To enable an analyzer, go to its website and get the API key and put it here in the key option.

Enable analyzer VirusTotal_GetReport_3_1

Base details

Name

VirusTotal_GetReport_3_1

Configuration

key

*

API key for Virustotal

polling_interval

60

Define time interval between two requests attempts for the report

rescan_hash_older_than_days

30

Rescan hash observable if report is older than selected days

highlighted_antivirus

1.

Add taxonomy if selected AV don't recognize observable

download_sample

True

False

Download automatically sample as observable when looking for hash

download_sample_if_highlighted

True

False

Download automatically sample as observable if highlighted antivirus didn't recognize

Options

Enable TLP check

True

False

Max TLP

AMBER

Enable PAP check

True

False

Max PAP

AMBER

HTTP Proxy

HTTPS Proxy

Figure 7.3: Ading the API Key

7.4 Running An Analyzer in Cortex

To run an analyzer, fill up the TLP, PAP, Data Type and Data and select the suitable analyzer accordingly. We can also select multiple analyzers for the same data.

The screenshot shows the 'Run analysis' interface. It includes the following fields and options:

- TLP ***: AMBER (dropdown)
- PAP ***: AMBER (dropdown)
- Data Type ***: ip (dropdown)
- Data ***: 8.8.8.8 (text input)
- Analyzers ***: A list of analyzers with checkboxes. 'Abuse_Finder_3_0' is checked. Other analyzers include CyberCrime-Tracker_1_0, DShield_lookup_1_0, GoogleDNS_resolve_1_0_0, Maltiverse_Report_1_0, MaxMind_GeoIP_4_0, TalosReputation_1_0, Threatcrowd_1_0, URLhaus_2_0, and Urlscan_io_Search_0_1_1.

At the bottom, there is a 'Cancel' button, a legend for the asterisk (*) indicating a 'Required field', and a 'Start' button.

Figure 7.4: Running An Analyzer

The running log can be seen from the Jobs History in Cortex. If the status is Success, then it has successfully generated report by querying into that analyzer. If the status is Failure, then there may be a problem in data type or format or the server may be down.

The screenshot shows the 'Jobs History' table with the following structure and data:

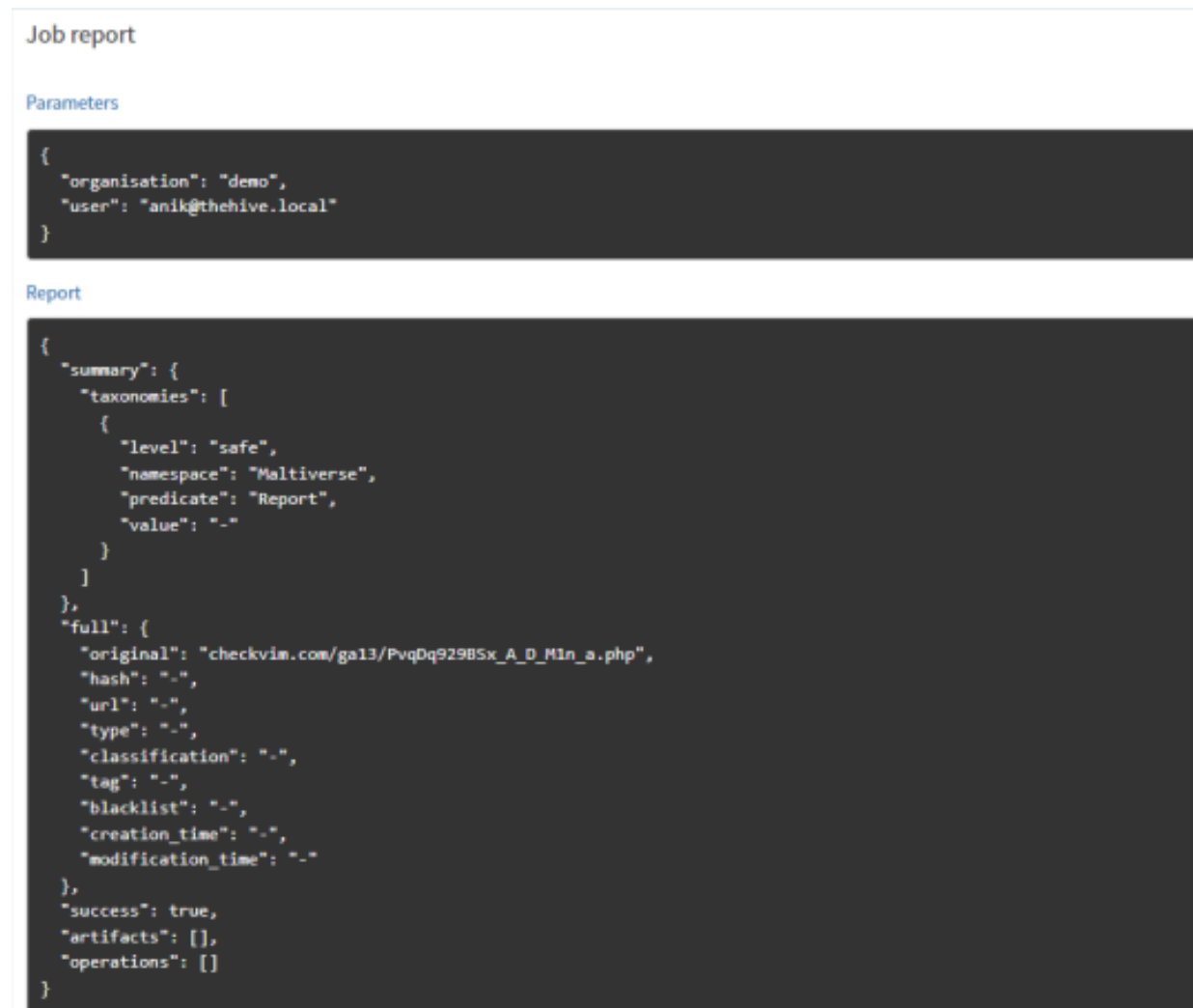
Status	Job details	TLP	PAP
Success	[ip] 8[.]8[.]8[.]8 Analyzer: Abuse_Finder_3_0	TLP:AMBER	PAP:AMBER

Additional details from the screenshot include a search bar for observable data, a 'Clear' button, and pagination controls showing '50 / page'.

Figure 7.5: Jobs History

7.5 Raw Report of Analyzer

By default in Cortex, the report generated by any analyzer is in JSON format which is not so human readable.



```
Job report

Parameters

{
  "organisation": "demo",
  "user": "anik@thehive.local"
}

Report

{
  "summary": {
    "taxonomies": [
      {
        "level": "safe",
        "namespace": "Maltiverse",
        "predicate": "Report",
        "value": "-"
      }
    ]
  },
  "full": {
    "original": "checkvim.com/ga13/PvqDq92985x_A_D_Min_a.php",
    "hash": "-",
    "url": "-",
    "type": "-",
    "classification": "-",
    "tag": "-",
    "blacklist": "-",
    "creation_time": "-",
    "modification_time": "-"
  },
  "success": true,
  "artifacts": [],
  "operations": []
}
```

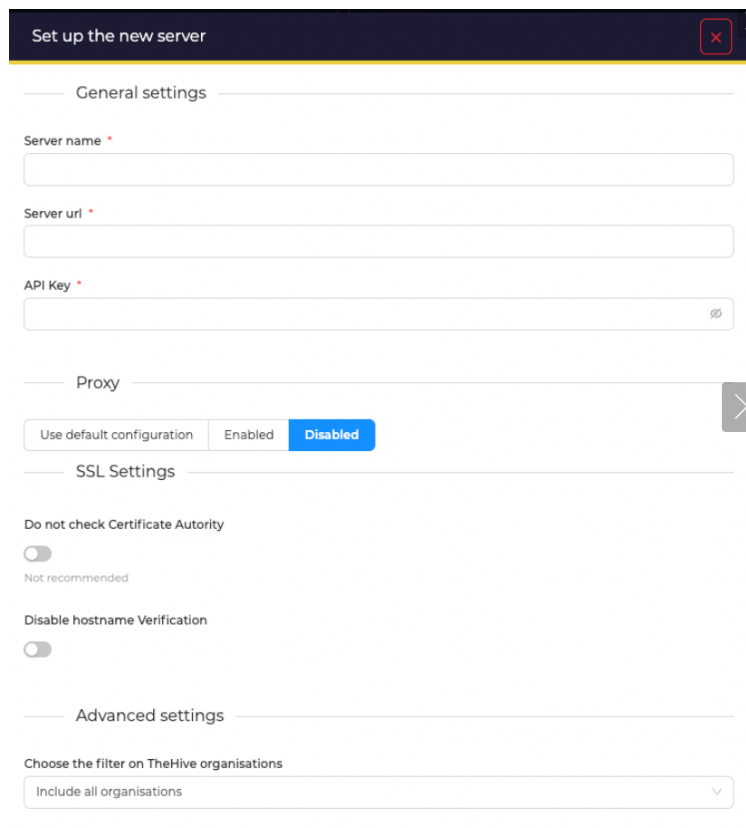
Figure 7.6: Raw Report of Analyzer

Chapter 8

Platform Integration

8.1 Integration with Cortex

- Click on Platform Management
- Go to Cortex
- Click on + in the Servers field



The screenshot shows a 'Set up the new server' dialog box with a dark blue header and a close button (X) in the top right corner. The dialog is divided into several sections:

- General settings**: Contains three text input fields labeled 'Server name *', 'Server url *', and 'API Key *'. The 'API Key' field has a small icon on the right.
- Proxy**: Contains a section with three buttons: 'Use default configuration', 'Enabled', and 'Disabled' (which is highlighted in blue). A right arrow button is visible on the right side of this section.
- SSL Settings**: Contains two toggle switches. The first is labeled 'Do not check Certificate Authority' and is currently turned off, with the text 'Not recommended' below it. The second is labeled 'Disable hostname Verification' and is also turned off.
- Advanced settings**: Contains a dropdown menu labeled 'Choose the filter on TheHive organisations' with the option 'Include all organisations' selected.

Figure 8.1: Add Cortex Server

8.2 Integration with MISP

One or more MISP instances can be connected to TheHive. MISP events can be imported as Alerts in TheHive. A set of filter can refine the imported events. Observables flagged as IOCs in a Case can be exported in a new event in MISP

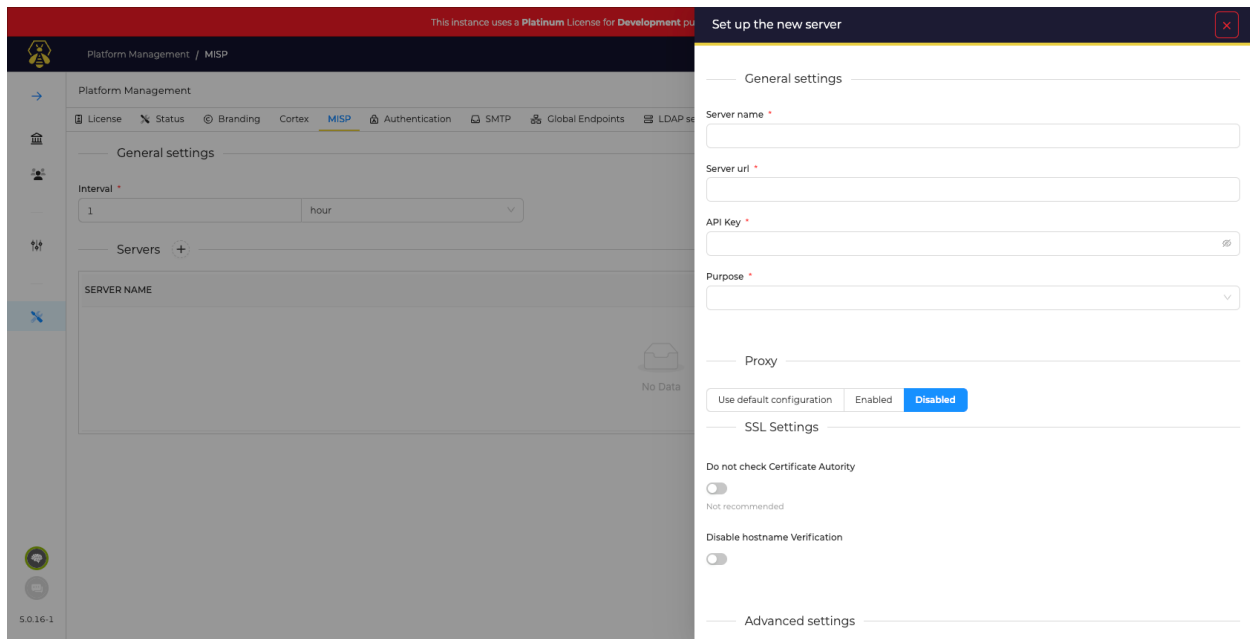


Figure 8.2: Add Misp Server

Chapter 9

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. 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.