# The Hive Security Tool:

## *Empowering Scalable and Collaborative Security Incident Response*

**Authors:**

Sumaiya Saeha (1905033)
Fariha Zaman Aurin (1905049)
Debjany Ghosh Aronno (1905053)

March 9, 2024

# Contents

# 1 Introduction

TheHive stands as a robust Security Incident Response Platform, meticulously crafted to streamline operations for Security Operations Centers (SOCs), Computer Security Incident Response Teams (CSIRTs), CERTs, and all information security professionals entrusted with the expeditious investigation and resolution of security incidents. As an open-source tool, TheHive is not only freely accessible but also allows users the liberty to modify and share its functionalities. Constructed using Java and AngularJS, it leverages Elasticsearch for the indexing and storage of critical data, underscoring its commitment to efficiency, flexibility, and collaborative cybersecurity practices.

# 2 History

TheHive, conceived by Thomas Franco, originated from his role as a security analyst at CERT-EU. Originally an internal project, it transitioned into an open-source initiative in 2014. The ongoing development and maintenance of TheHive are orchestrated by TheHive Project, a non-profit organization headquartered in France. With a global footprint, TheHive has garnered widespread adoption, finding application in numerous organizations worldwide. Distinguished users include the NATO Computer Incident Response Capability (NCIRC) and the Computer Emergency Response Team of the European Union Institutions (CERT-EU).

# 3 Overview of Key Features

The Hive is a security tool that aims to make life easier for security incident responders. Some of the key features of The Hive are:

- **Case Management:** TheHive allows users to create cases from different sources, such as email, MISP events, SIEM alerts, or manually. Users can assign tasks to analysts, track the progress of the investigation, add observables, attach files, and write notes. Users can also use templates to standardize their case creation and workflow.
- **Observable Analysis:** TheHive integrates with Cortex, a powerful observable analysis and active response engine. Thanks to Cortex, users can analyze observables such as IP and email addresses, URLs, domain names, files, or hashes using a web interface or through the REST API. Users can also automate these operations and submit large sets of observables from TheHive or from alternative SIRP platforms, custom scripts, or MISP.
- **Active Response:** Cortex also enables users to perform active response actions on observables, such as blocking an IP address, disabling a user account, or quarantining a file. These actions can be triggered manually or automatically based on predefined rules.

- **Information Sharing:** TheHive is tightly integrated with MISP, a platform for sharing threat intelligence among security teams. Users can import MISP events as cases in TheHive or export cases as MISP events. Users can also synchronize their observables with MISP attributes and enrich them with MISP taxonomies and galaxies.

# 4 Overview of the Source Code

The source code of TheHive is written mainly in Scala, a general-purpose programming language that runs on the Java Virtual Machine (JVM). The code is organized into several modules and packages, each with a specific purpose and functionality. Figure 1 shows the structure of the source code.

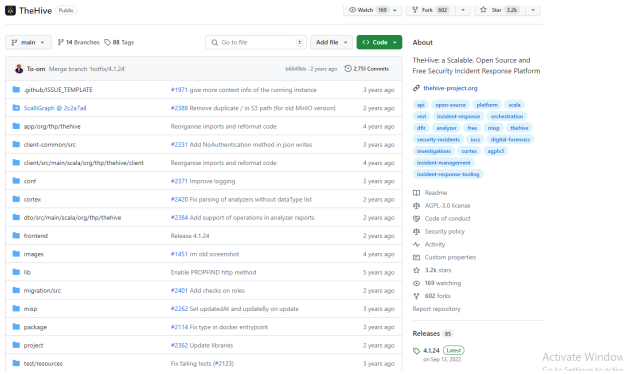


Figure 1: The structure of the source code of TheHive

We will briefly describe the main modules and packages of the source code in the following subsections.

## 4.1 app

This module contains the core logic and functionality of TheHive. It includes the following packages:

- **org.thp.thehive:** This package contains the main classes and traits that define the application, such as TheHiveApp, TheHiveModule, and TheHiveConfig.
- **org.thp.thehive.controllers:** This package contains the controllers that handle the HTTP requests and responses for the different endpoints of the application, such as Cases, Tasks, Observables, Alerts, and Users.
- **org.thp.thehive.models:** This package contains the case classes and objects that represent the data models of the application, such as Case, Task, Observable, Alert, User, and Organisation.

- **org.thp.thehive.services:** This package contains the services that provide the business logic and operations for the data models, such as CaseSrv, TaskSrv, ObservableSrv, AlertSrv, UserSrv, and OrganisationSrv.
- **org.thp.thehive.connector:** This package contains the classes and traits that enable the integration with external tools and platforms, such as MISP and Cortex.

### 4.2 client

This module contains the code for the web-based user interface of TheHive. It includes the following packages:

- **org.thp.thehive.client:** This package contains the classes and objects that define the client-side application, such as ClientApp and ClientConfig.
- **org.thp.thehive.client.pages:** This package contains the components that render the different pages of the user interface, such as DashboardPage, CasePage, TaskPage, ObservablePage, AlertPage, and UserPage.
- **org.thp.thehive.client.services:** This package contains the services that provide the client-side logic and operations for the user interface, such as ApiService, NotificationService, UserService, and OrganisationService.

### 4.3 conf

This module contains the configuration files for the application, such as `application.conf` and `logback.xml`.

### 4.4 cortex

This module contains the code for the integration with Cortex. It includes the following packages:

- **org.thp.cortex.client:** This package contains the classes and objects that define the client-side communication with Cortex, such as CortexClient and CortexConfig.
- **org.thp.cortex.dto:** This package contains the case classes and objects that represent the data models of Cortex, such as Analyzer, Job, Report, Responder, Action, Response.

### 4.5 dto

This module contains the code for the data transfer objects (DTOs) that are used to exchange data between different layers of the application. It includes the following package:

- **org.thp.thehive.dto:** This package contains the case classes and objects that represent the DTOs of TheHive, such as CaseDTO, TaskDTO, ObservableDTO, AlertDTO, UserDTO.

### 4.6 frontend

This module contains the code for building and packaging the frontend assets of TheHive. It includes files such as `webpack.config.js` and `package.json`.

### 4.7 lib

This module contains some third-party libraries that are used by TheHive. It includes files such as `scala-graph.jar` and `elastic4play.jar`.

### 4.8 migration

This module contains some scripts and tools for migrating data from previous versions of TheHive. It includes files such as `migration.sh` and `migration.conf`.

### 4.9 misp

This module contains some scripts and tools for synchronizing data with MISP. It includes files such as `misp.sh` and `misp.conf`.

### 4.10 project

This module contains some files for managing the project dependencies and build process. It includes files such as `build.sbt` and `plugins.sbt`.

### 4.11 test

This module contains some files for testing the application. It includes files such as `test.conf` and `test.sh`.

## 5 Architecture

The overall system architecture is composed 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.

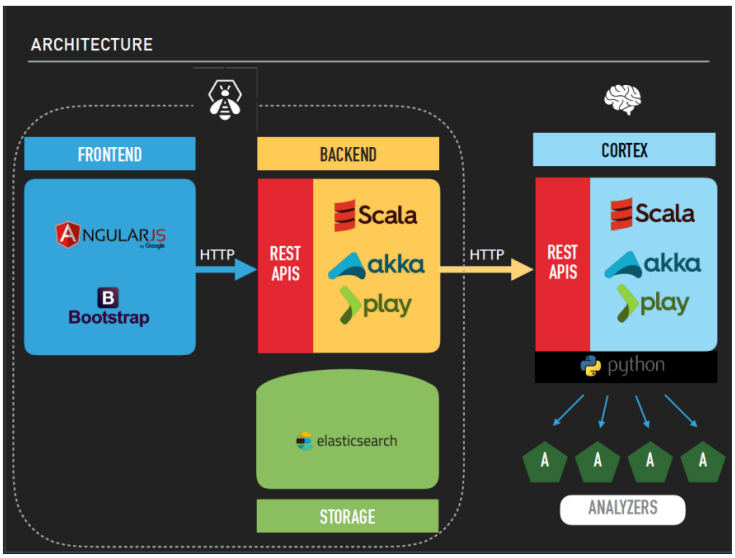


Figure 2: TheHive Architecture Diagram

- **Cortex:** Cortex is a real-time streaming analytics platform used to process the data from the backend. It is built using Scala, Akka, Play Framework, and Python.
- **Storage:** The storage layer is employed to store the data from the system. It is comprised of a distributed database, such as Elasticsearch.
- **Analyzers:** The analyzers are utilized to analyze the data from the system. They can perform tasks such as anomaly detection, fraud detection, and trend analysis.

.

## 5.1 Collaboration with Cortex

TheHive is tightly integrated with Cortex, another powerful tool from TheHive Project. With Cortex, security professionals can conduct in-depth analysis of various types of observables, enhancing incident response efforts through a convenient web interface.

## 5.2 Integration with MISP

TheHive is integrated with MISP (Malware Information Sharing Platform), enhancing its capabilities in handling security incidents.

## 5.3 Workflow of TheHive

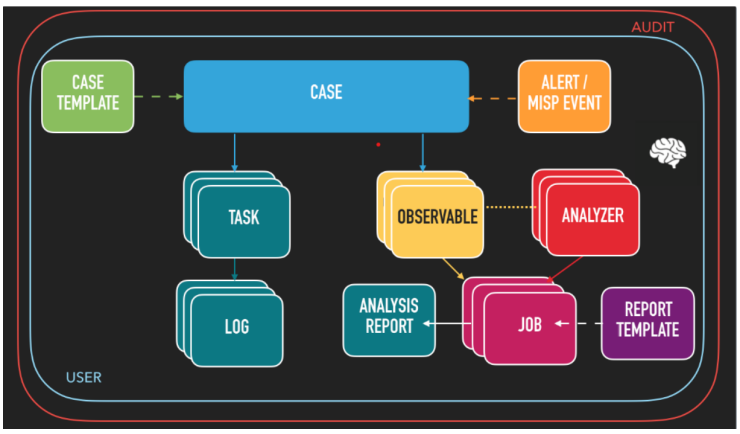


Figure 3: Workflow of TheHive

TheHive workflow involves the following key steps:

1. **Create Case Template**: Create a case template to define the structure of incident cases. This includes the fields and attributes that will be used to document and manage incidents.
2. **Create Case**: Document and manage incidents by creating cases. Assign cases to analysts or teams for resolution.
3. **Create Tasks**: Assign tasks and responsibilities within cases to ensure organized incident response.
4. **Create Alerts**: Create alerts to notify analysts of potential security incidents.
5. **Create Observables**: Create observables to document and analyze potential threats associated with incidents.
6. **Run Analyzers**: Use various analyzers to gather additional information and context about incidents and associated observables.
7. **Create Logs**: Create logs to document actions taken by analysts during incident response.
8. **Create Analysis Reports**: Use analysis reports to document findings and conclusions about incidents and observables.
9. **Create Jobs**: Create jobs to automate incident response tasks.
10. **Create Report Templates**: Create report templates to document incident response activities and outcomes.

# 6 Documentation to run Features

TheHive has many amazing functionalities that make it a powerful tool for security incident response. Here we will discuss some of the most important ones.

## 6.1 Admin side

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. Administrators can create users, assign roles to them, and manage their permissions. They can also configure the tool to send notifications via email or SMS when certain events occur, such as new incidents being created or updated, or when certain actions are performed by users, such as adding comments or attachments to incidents. list of features:

- Organization management
- Link organizations
- Account management
- Entities
- Permission management
- Observables types
- Case Status
- Alert Status

**Organization management**

### 6.1.1 Create an Organization

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.

To create a new organization, follow these steps:
1. Click on the **Add an Organization** button.
2. Edit the required fields in the drawer:

- A placeholder exists and a logo of the Organisation can be added.
- Name: Name of the new Organization.

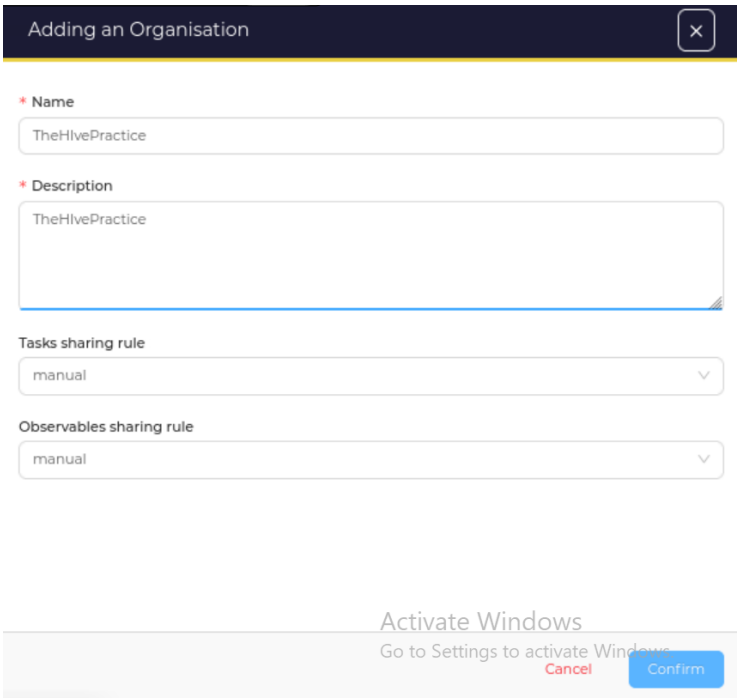


Figure 4: Create An Organization

- Description: Description for the new Organization.
- Task sharing rule: default sharing rule for Tasks that will be applied when a Case will be shared with another Organization.
- Observables sharing rule: default sharing rule for Observables that will be applied when a Case will be shared with another Organization.

3. Click **Confirm** to create the organization.
   We can see this in Figure 5 that organization is created.

### 6.1.2 Link Organization

TheHive allows administrators to link multiple organizations together. This allows for better collaboration between different teams within an organization, such as a SOC team and a CSIRT team.
To link an organization, follow these steps:

Here are the steps to manage links in TheHive:
1. Open the detailed view of an Organization.
2. Open the Linked Organization tab.

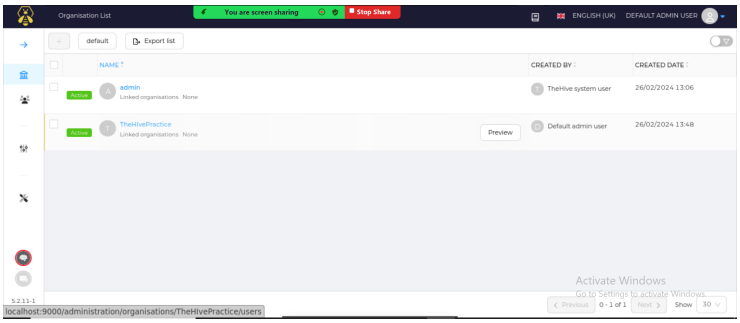


Figure 5: Organization Management

We can see this in Figure 6.

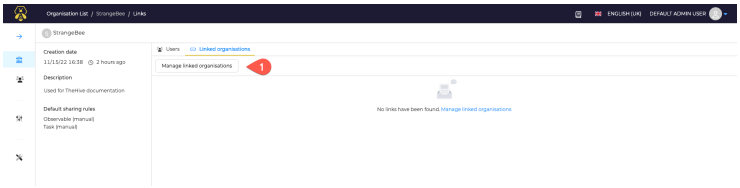


Figure 6: Link Organization

3. Click on the button named **Manage linked Organizations**.

We can see this in Figure 7.

4. For each other organization, select:

- If you want the current Organization to be linked with it.
- The types of link that should be created.

3 types of links are available:

- 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.

## 6.2 Account Management

TheHive allows administrators to create multiple user accounts within the tool. Each user account can have its own set of roles and permissions. This allows for

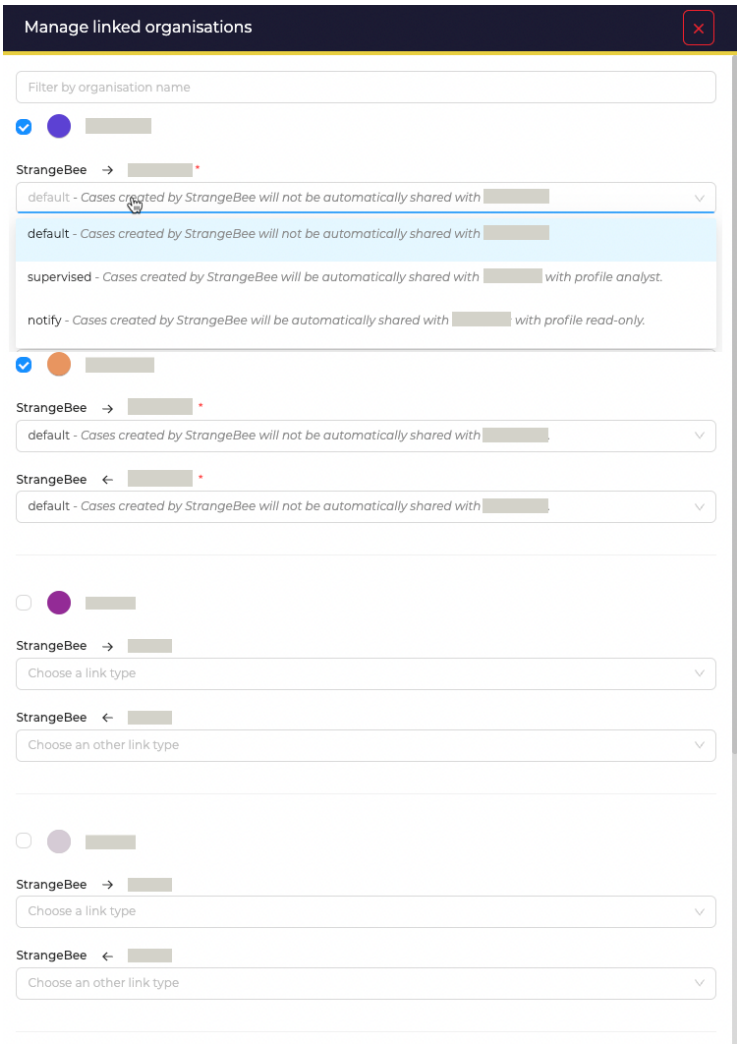


Figure 7: Manage Link Organization

better separation of duties and responsibilities between different users within an organization, such as a SOC team and a CSIRT team.
Accounts can be created or edited from several places in TheHive:

1. As Administrator, in the Users view
2. As Administrator in the detailed page of an Organisation
3. As Org-admin, in the Organisation configuration page

We can see this in Figure 8.

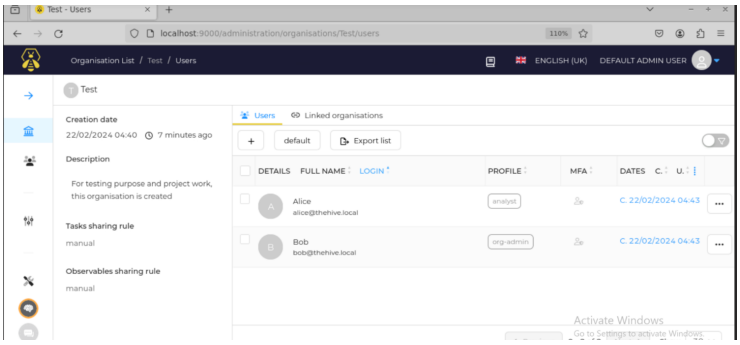


Figure 8: Users

Starting with TheHive 5.0, two types of accounts exist in the application:

1. Normal accounts: These are used for standard users, such as analysts. These accounts can be used to open a session on the web UI, utilize all available authentication methods, and API keys if enabled.

2. Service accounts: These are recommended for use by accounts in charge of automation within the application, such as those used to create Alerts. Service accounts can only be used to authenticate the application through the API, using an API key.

Click on the **Add a User** button.
To create an account:

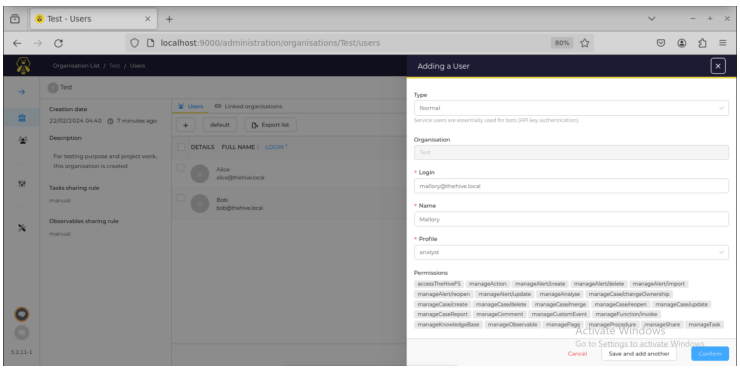


Figure 9: Add User

1. Choose the type of account, either Normal or Service.

2. Fill in the login name (formatted as an email address).

3. Specify a name for the account.
4. Select the organizations and associated profiles for this account.
5. Click on "Set as default" to define the default organization for the account.
6. Finally, click "Confirm."

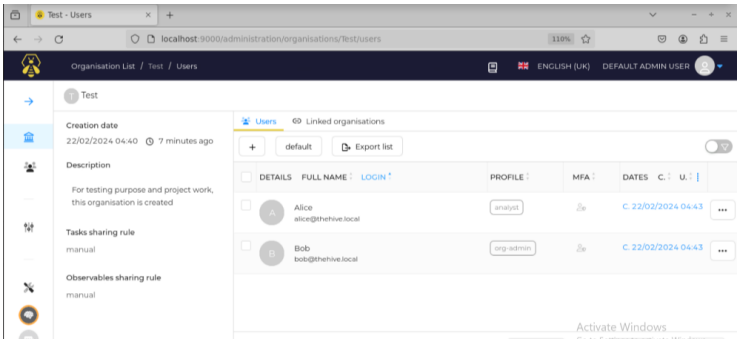


Figure 10: Successful Creation of User

We can see The final look after creating Users in Figure 10. We can also edit an existing account by clicking on the **preview** button.

## 6.3 Entities & Permissions

TheHive comes with a set of predefined profiles for Administrators and Organsations ; this set can be enriched with custom profiles you can create depending on your needs.
We can see this in Figure 18.

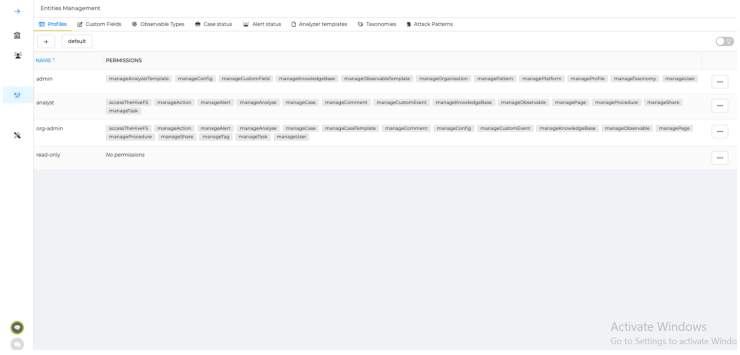


Figure 11: Entities avaliable

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

- admin
- analyst
- org-admin
- read-only

## 6.4 Users Roles

Now that we have created our users, we need to assign them roles.
We have the entities given in Figure 18. We can give roles according to our needs.

1. **Admin**:
   - **Description**: 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.
   - **Privileges**:
     - Full access to all features and functionalities.
     - User and organization management.
     - Configuration and system settings control.
     - Incident case management.
2. **Analyst**:
   - **Description**: 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.
   - **Privileges**:
     - Access to incident case management.
     - Ability to work on and update cases.
     - Collaboration with other analysts.
     - Limited access to system configurations.
3. **Org-admin** (Organization Administrator):
   - **Description**: Organization administrators have administrative privileges limited to a specific organization within TheHive. They can manage users, incidents, and configurations for their assigned organization.

- **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.

4. **Read-only**:

   - **Description**: 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.
   - **Privileges**:
     - View-only access to incident cases and data.
     - Cannot modify or update cases.
     - Limited interaction with the platform.

## 6.5 Cases

A case furnishes details about potentially suspicious activity within an environment. It encompasses information regarding security incidents, observables, alerts, and impacted users. Security analysts utilize cases for targeted analyses, evaluating the potential threats present. Cases can originate from diverse sources and typically include a title, tags, task rules, observable rules, a detailed description of case specifics, and all pertinent details essential for constructing a rationale to identify and address specific threats.
After logging into an user account ,a user can see the list of cases of his organization. It is shown in figure

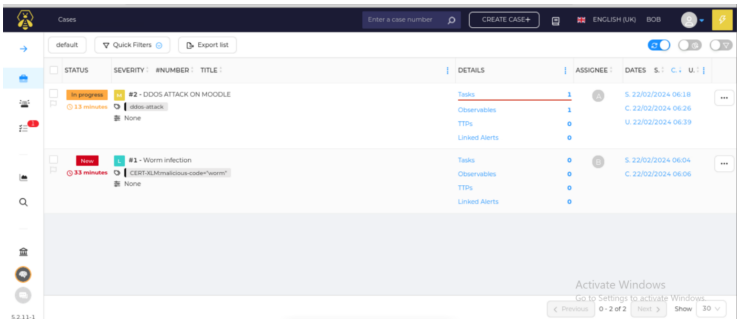


Figure 12: Cases

### Create a Case

To create new cases using templates, follow these steps:

1. Click on "Create Case +" located in the header.


Figure 13: Create Case

2. Cases can be created from the following. Either of these can be selected.
   - Empty Case
   - Case Template
   - Archive
   - From MISP (.json)

   It can be shown in Figure 14.

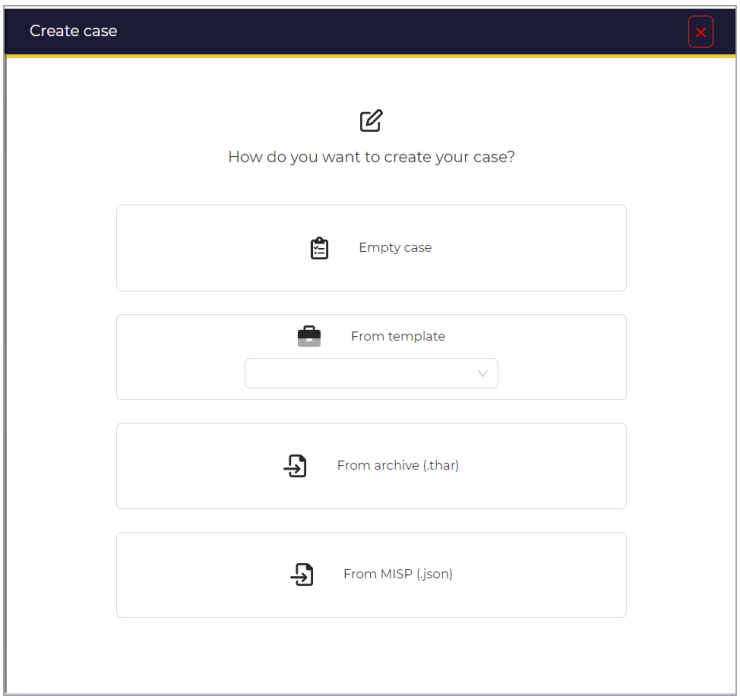


Figure 14: Create Case from

We will create case from empty case.

### Creating a New Case from an Empty Case

To create a new case from an empty case, these steps are followed:

- Enter the case title in the "Title" field.
- Select a date from the "Date" field.
- Select the severity level (Low/Medium/High/Critical).
- Select the TLP (Traffic Light Protocol) level (White/Green/Amber/Red).
- Select the PAP (Perceived Attribution Program) level (White/Green/Amber/Red).
- Click the "+" button to add tags (refer to "Add Tags").
- Enter the case description in the "Description" field.
- Choose a Task rule from the list (manual/existingOnly/upcomingOnly/all).
- Choose an Observable rule from the list (manual/existingOnly/upcomingOnly/all).
- Add tasks (refer to "Add Tasks").
- Add custom fields (refer to "Add Custom Field Values").
- Click the "Confirm case creation" button to create the case.

It can be shown in Figure 16.

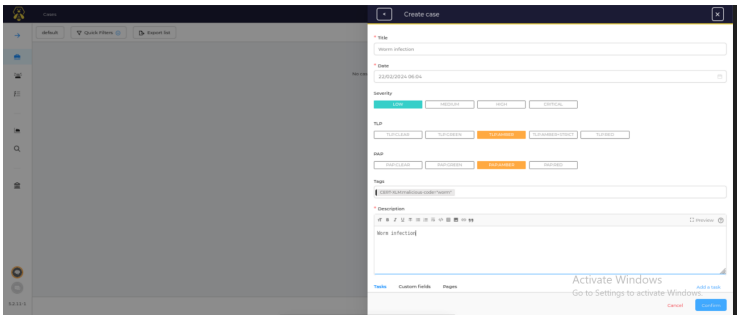


Figure 15: Empty Case

### Statistics

We can view the statistics by enabling the stats toggle button

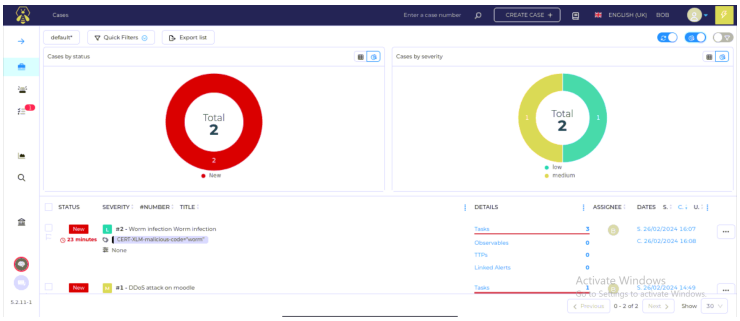


Figure 16: Statistics

## 6.6 Task

After creating a new case ,a user can create tasks which should be performed to resolve the case and assign those tasks to different users. So,For a particular case while adding a task we need to fill up the following dialogbox with necessary information about that task

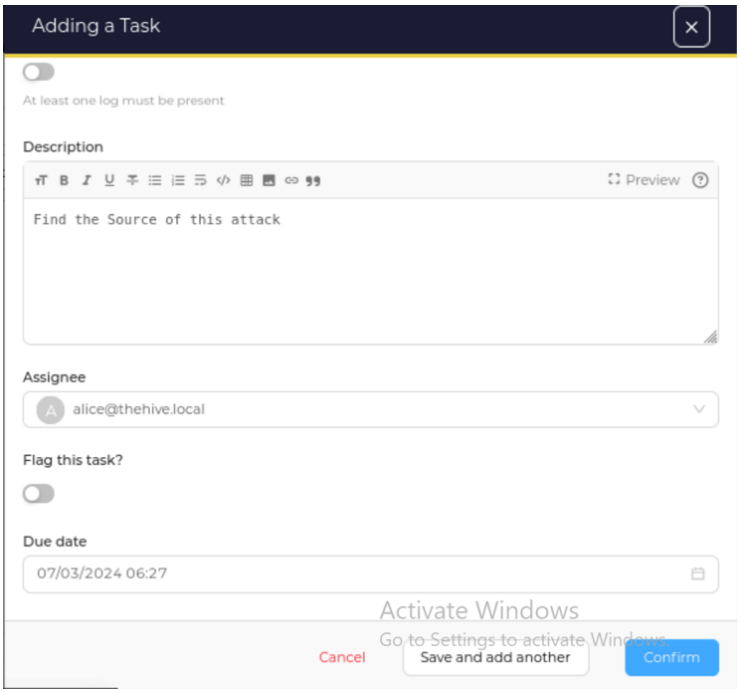


Figure 17: Adding a task

Then after creating a task successfully the dashboard of a case under "Tasks" tab will look like below

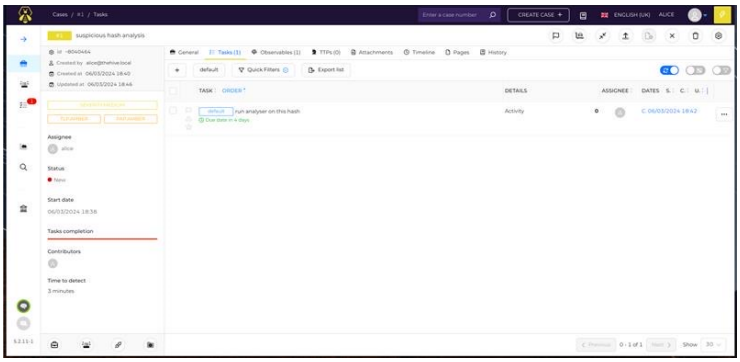

Figure 18: Case dashboard(after adding a new task)

## 6.7 Observables types

Administrators using The Hive have the flexibility to establish various observable types, each equipped with its unique attributes. This feature enables a more efficient distribution of tasks and responsibilities among distinct teams within an organization, fostering improved collaboration between, for instance, a Security Operations Center (SOC) team and a Computer Security Incident Response Team (CSIRT).
The following steps creates a new observable type:

1. Click on the **Add an Observable Type** button.
2. Edit the required fields in the drawer:
   - Name: Name of the new Observable Type.
   - Description: Description for the new Observable Type.
   - Attribute: Attribute for the new Observable Type.
3. Click **Confirm** to create the observable type.

We can see this in Figure 28.

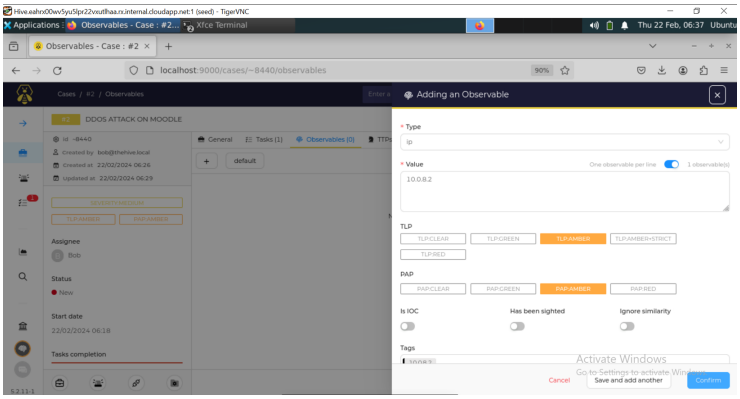


Figure 19: Create Observables

After creating observables we cam find the list of observables for a particular case. It is shown in 20

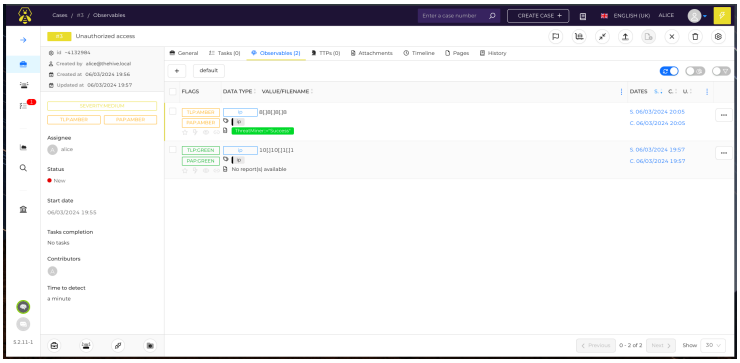

Figure 20: Observables list

## 6.8 Cases and Alert Status

Admin also have the capability to introduce new statuses for both cases and alerts. Admin must provide the following details to define a status:

1. **Stage**: select the stage of the new status.
2. **Value**: select a name for the new status.
3. **Color**: select a color for users to quickly identify the status

for example:

- **Stage**: Investigation

- **Value**: In Progress
- **Color**: redRed

Here, for the "Investigation" stage a status "Processing" is defined with a red color for users to quickly identify the status.

## 6.9 User side

TheHive boasts a user-friendly web interface facilitating tool access from any Internet-connected computer. Users can initiate incidents, augment them with comments and attachments, delegate tasks to peers, and conclude incidents upon resolution. Additionally, users have the capability to conduct targeted searches for incidents based on criteria like status, severity level, or creation date. The tool offers diverse features, including: list of features:

- Incident management
- Case management
- Task management
- Report management
- Dashboard management
- Integration with other tools

### 6.9.1 Templetes

As an organization administrator, you have the ability to craft templates for various components such as incidents, cases, pages, and reports. Following is the process of creating templates specifically for cases: First, let's see the lists of case templetes.

- Access to the list by opening the Organisation menu, then the Templates tab, and the Cases tab. It is shown in Figure 21
- Click the plus button to create a new Case template. It is shown in Figure 22.

## Configuration parameters:

When creating a Case template, the following parameters can be configured:

- **Prefix**:A string that will be prepended to the title of a Case when it is created with this template.
- **Name**: The identifier of the Case template, utilized for recognition through the API.

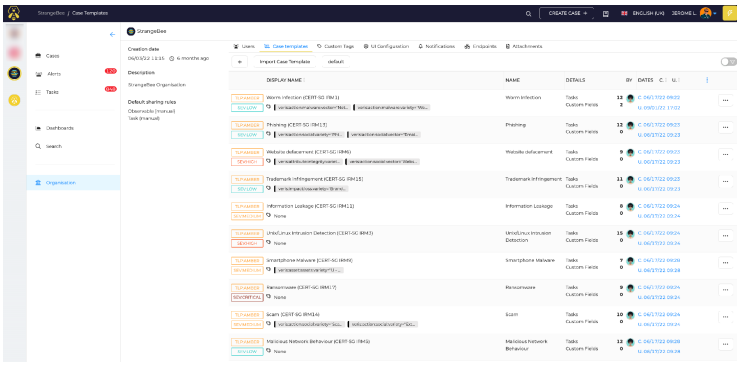

Figure 21: List of Case templates

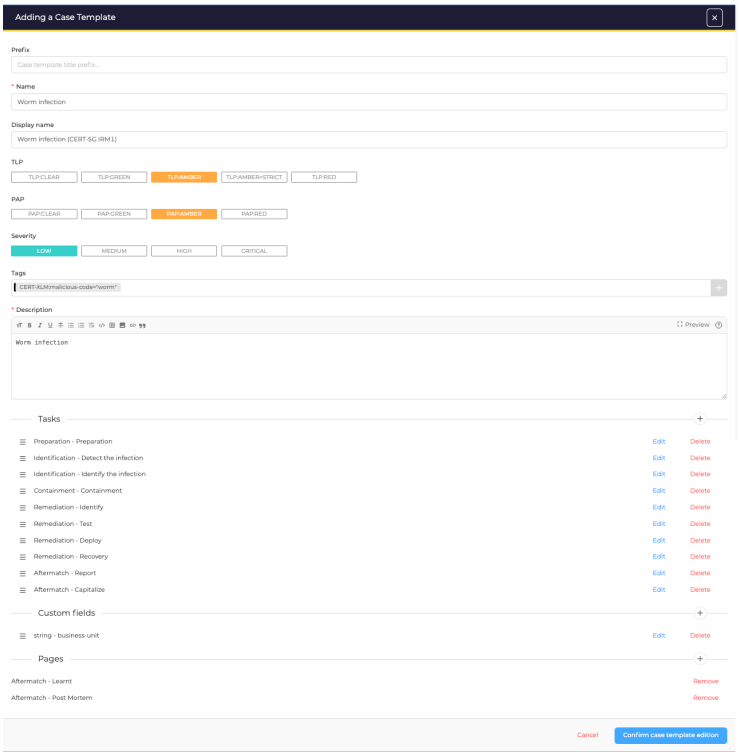


Figure 22: New Case template

- **Display Name**: The name of the Case template as presented in the UI.
- **TLP**: The default TLP (Traffic Light Protocol) of the Case when it is created with this template.

- **PAP**: The default PAP (Perceived Attribution Program) associated with the Case when created using this template.
- **Severity**:The default severity level assigned to the Case when created with this template.
- **Tags**: A list of tags that will be added to the Cases created with this template.
- **Description**: The default description assigned to Cases when they are created using this template if no modifications are made.
- **Tasks**: Tasks can be included in the templates, and they will be automatically integrated into the Case when it is created with this template.
- **Custom Fields**: Custom fields can be added to the template, with the option to set default values for these fields.
- **Pages**: Page templates can be added to the template, and they will be automatically included in the Case when it is created using this template.

# Import and Export

## Exporting a Case Template

Exporting a Case template involves the following steps:

1. Click on the option icon, typically represented as three dots or a gear icon.
2. Select "Export case template" from the menu

The Case template will be exported and saved as a JSON file. //
It is shown in Figure 23.

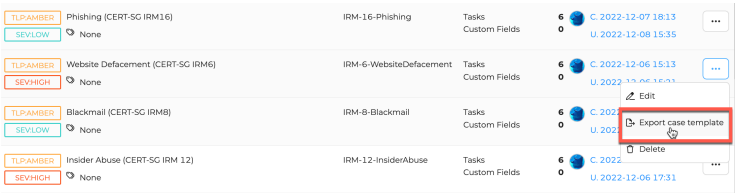


Figure 23: Export Case template

### Importing a Case Template

Importing a Case template involves the following steps:

1. Click on the **Add a Case Template** button.
2. Choose the JSON file that holds the Case template.
3. Click "Confirm" to initiate the import of the Case template.

It is shown in Figure 24.

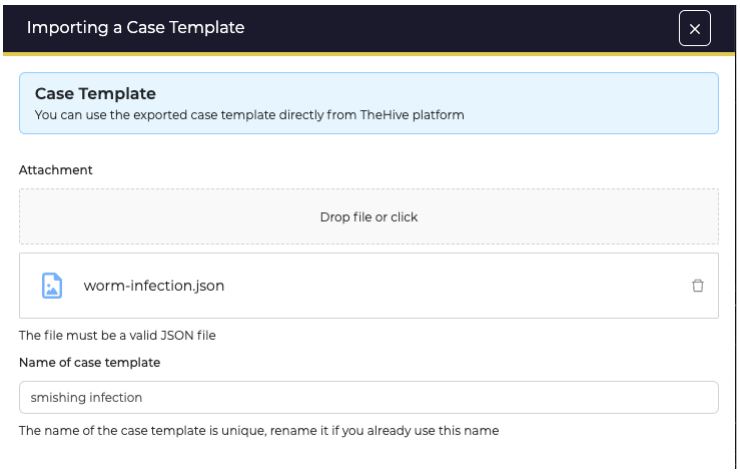


Figure 24: Import Case template

## 6.10 Alerts

Alerts serve as timely notifications that convey essential information regarding ongoing security issues, vulnerabilities, and potential exploits. They play a crucial role in keeping individuals and organizations informed about the current state of their digital security, enabling proactive responses to mitigate risks and address emerging threats promptly.

### 6.10.1 View Alert Details

To view the details of a specific alert, steps are the following:

1. Navigate to the left menu and click on the "Alerts" button.
2. Select the specific alert you wish to examine.

Upon clicking on the alert, the Alerts page will show various tabs with additional details. These tabs include, the General tab, Observables, TTPs, Similar Cases, Similar Alerts, and the Responders tab. These tabs can be explored to gain a fine understanding of the alert and its associated information.

It is shown in Figure 25.

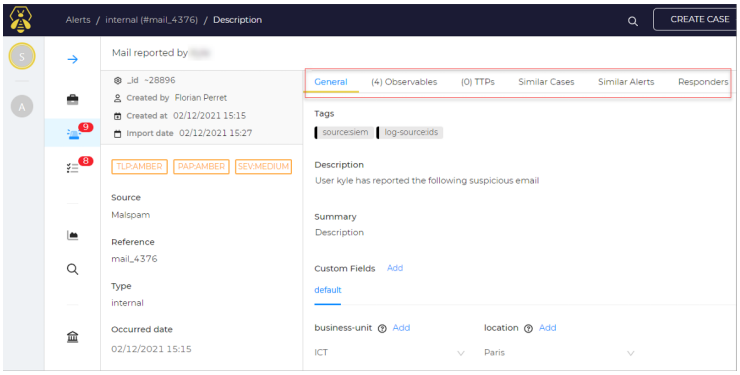


Figure 25: Alerts

### 6.10.2 Create a Case from an Alert

The main page shows different alerts - some are new, and some are imported. You can only create a new case from the selection for the new alerts, making it easier to manage and respond to recently identified security issues.

It is shown in Figure 26.

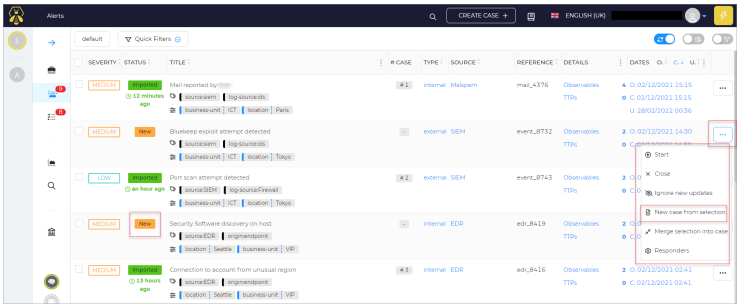


Figure 26: Create Case from Alert

To add a new case from a selection, follow these steps:

- Navigate to the alert details page.
- Choose the alert for which you want to create a new case.
- Click on the "New Case from Selection" option.

- A new window will open, enabling you to easily create a new case based on your chosen alert.

When an empty case or a case template is chosen, a new case will be generated, incorporating the observables and Tactics, Techniques, and Procedures (TTPs) from the selected alert. This streamlines the process of case creation by automatically including relevant information from the alert into the new case.

## 6.11 Seamless Collaboration with MISP

TheHive is closely integrated with MISP (Malware Information Sharing Platform), significantly augmenting its capabilities in effectively managing and responding to security incidents. This tight integration ensures seamless collaboration and information sharing between the two platforms, enhancing overall incident handling and response capabilities.

## 6.12 Stronger Analysis with Cortex Integration

TheHive provides strong observable analysis by working closely with Cortex, another potent tool from TheHive Project. Cortex enables security experts to delve into detailed analysis of different observables, making incident response more effective through an easy-to-use web interface.

Highlights of observable analysis with Cortex include:

- **Comprehensive Analysis Tools**: Cortex offers a diverse array of analyzers and responders, enabling thorough investigations on different observable types, including:
  - IP addresses
  - Email addresses
  - URLs
  - Domain names
  - Files (e.g., attachments)
  - Hashes (e.g., MD5, SHA-256)
  - Registry keys (e.g., Windows Registry entries)
  - And more...

  These tools can reveal crucial information about potential threats associated with these observables.

- **Integration with TheHive**: we can initiate observable analysis directly from our incident cases, improving efficiency and reducing response times.

- **Automation**: Automate the analysis process by crafting analysis templates that define which analyzers to run for specific observable types. This automation simplifies your incident response workflow, making it more efficient.
- **Customization**: We can customize Cortex by adding our own analyzers or responders to tailor the analysis capabilities to your organization's specific needs.
- **Scalability**: Cortex is crafted to manage a large volume of observables, making it well-suited for organizations with extensive security operations.

### 6.12.1 Analyzers and Responders

When you go to the case details page, you can view all the cases associated with the organization. It is shown in 27.

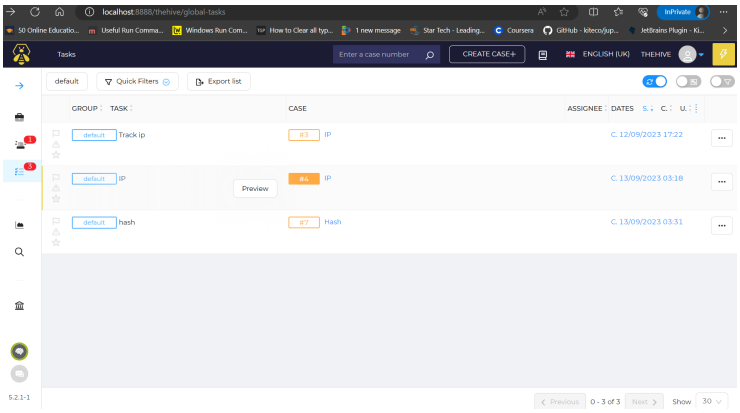


Figure 27: Cases

Click on the case you want to analyze. And then click on the **observables** tab of your task. It is shown in 28.

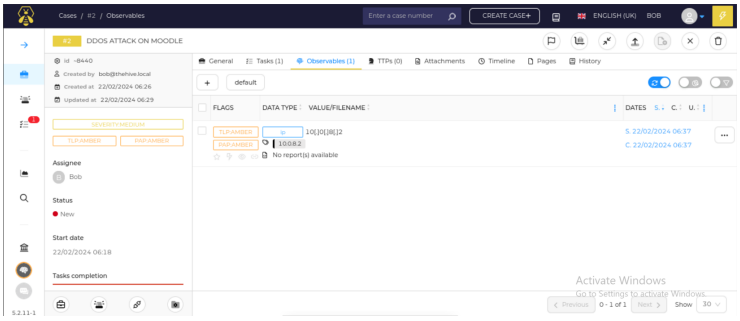


Figure 28: Observables

Currently, you can access all the observables related to the case and initiate the creation of new observables. To create an observable, you'll need to provide some essential basic information.

- **Type**: Type of the observable.
- **Value**: Value of the observable.
- **Tags**: Tags of the observable, that will help us to search for the observable.
- **Description**
- **TLP**: TLP of the observable.
  - **White**
  - **Green**
  - **Amber**
  - **Red**
- **PAP**: PAP of the observable.
  - **White**
  - **Green**
  - **Amber**
  - **Red**

### 6.12.2 Analyzers

Cortex offers an extensive selection of analyzers for diverse analysis needs. We can get the whole list of analyzer and there task in Cortex. This is shown in 29. Once the observable is created, you'll encounter the analyzers option. For instance, if you're working with an IP address observable, you can observe the available analyzers. 30 displays the list of analyzers.

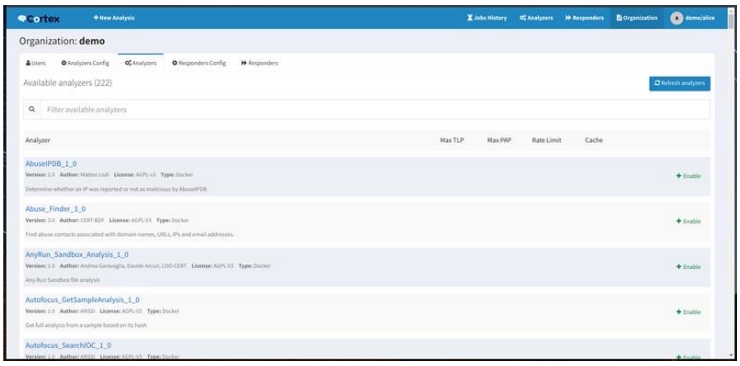


Figure 29: Analyzers

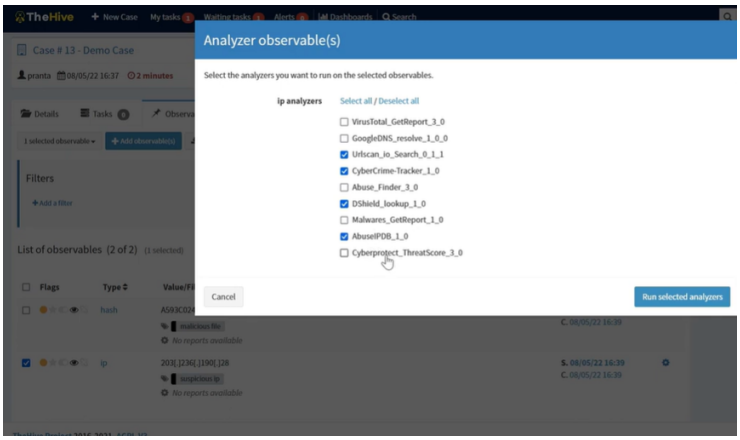


Figure 30: Analyzers

Cortex provides a wide range of analyzers such as:

- **Abuse Finder**
- **Google DNS Resolver**
- **URL Scan**
- **Cyber Protect Threat Score**

Another example is shown in 31 . Here we can see the available analyzers for hash observable.

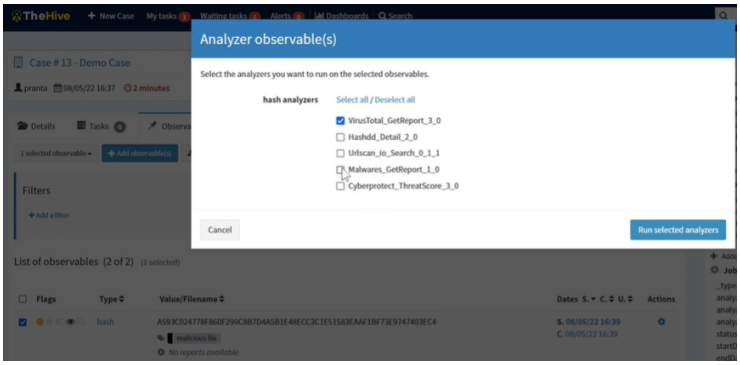


Figure 31: Analyzers

31.

### 6.12.3 Analysis Report

After running the analyzer, we can see the analysis report. Here danger levels are shown with results from different analyzers **Color Coded**. For example, we can see the analysis report of the hash observable. It is shown in 32. Two blue colors indicate that, according to that particular analyzer, the hash is not considered malicious. Conversely, two red colors indicate that the hash is identified as malicious by that specific analyzer.

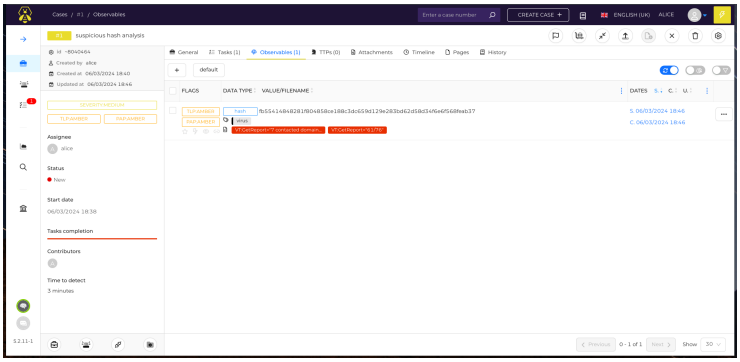

Figure 32: Analysis Report

We can see the report in details at 33

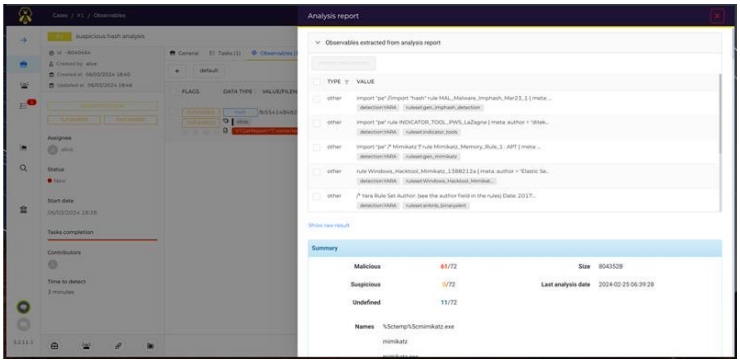

Figure 33: Analysis Report

We can see the Job history from Cortex where all the analyzers result run on the observables are saved. See this in 34 Here We can see the job details per observable and find report in JSON format. It is shown in 35

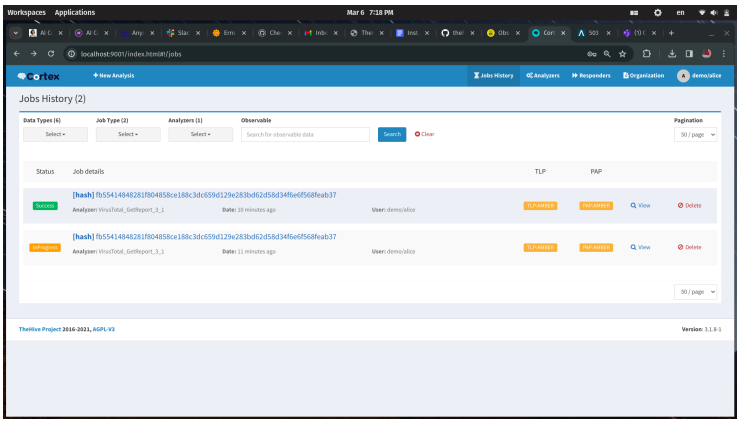


Figure 34: Job History

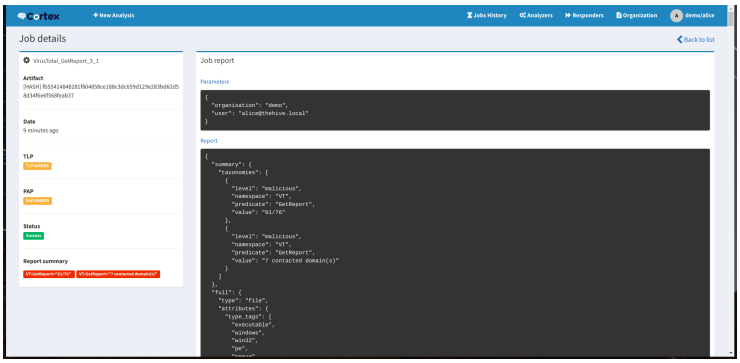


Figure 35: Analysis Report

# 7 Use Cases

Here we can discuss some specific use cases where TheHive excels.

- **Incident management:** TheHive streamlines efficient security incident management by offering a centralized platform. It facilitates the creation of cases, assignment of tasks, and real-time tracking of investigation progress.
- **Automation:** Leverage The Hive's integration with Cortex for automating incident response processes. Cortex, a potent engine, allows the analysis of observables like IP addresses, email addresses, URLs, domain names, files, or hashes through a user-friendly web interface. Automation extends to large sets of observables from TheHive, Cortex REST API, alternative SIRP platforms, custom scripts, or MISP.

- **Collaboration:** Enhance collaboration with other teams using TheHive. Share information on security incidents, create alerts, exchange observables, and communicate seamlessly with other teams in real-time.
- **Reporting:** TheHive provides comprehensive reports on incident response activities. Generate detailed reports on metrics such as the number of cases created, tasks assigned, and the overall progress of investigations.

# 8 Conclusion

The Hive stands out as a potent and adaptable Security Incident Response System (SIRS) suitable for organizations of all sizes. It undergoes continuous updates, introducing new features and enhancements. With a flexible architecture and a user-friendly interface, it equips security teams with the necessary tools for efficient orchestration of incident response processes. The platform's automation capabilities, seamless integration with external security tools, and comprehensive reporting and analytics empower security professionals to streamline their workflows. Overall, in the face of evolving threat landscapes, The Hive remains a valuable asset, enhancing organizational security posture, streamlining incident response, and promoting a proactive cybersecurity approach.