



CSE406-Computer Security Sessional

Report on TheHive - an open source and free Security Incident Response Platform

Ashfaque Rahman
1805047
Hasan Masum
1805052

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

September 14, 2023

Contents

1	Introduction	3
2	Overview of the Source Code	3
2.1	app	4
2.2	client	4
2.3	conf	4
2.4	cortex	4
2.5	dto	4
2.6	frontend	5
2.7	lib	5
2.8	migration	5
2.9	misp	5
2.10	project	5
2.11	test	5
3	Key Features	5
4	Key Components	6
4.1	Organizations	6
4.2	Cases	6
4.3	Task	6
4.4	Observables	6
5	Documentation of Key features	6
5.1	Organization Admin	6
5.1.1	Manage Users	6
5.1.2	Templates	10
5.1.3	Tags	14
5.2	Analyst	15
5.2.1	Cases	15
5.2.2	Tasks	24
5.3	Observables	29
5.3.1	Create Case Observables	29
5.3.2	Run analyzers	30

1 Introduction

TheHive is an open source and free security incident response platform that helps security professionals deal with cyber threats and incidents. It is developed and maintained by TheHive Project, a community of security experts and enthusiasts. The source code of TheHive is hosted on GitHub, where anyone can access, review, or contribute to it. In this report, we will provide a high level overview of the main modules and packages of the source code, and explain their purpose and functionality.



2 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.

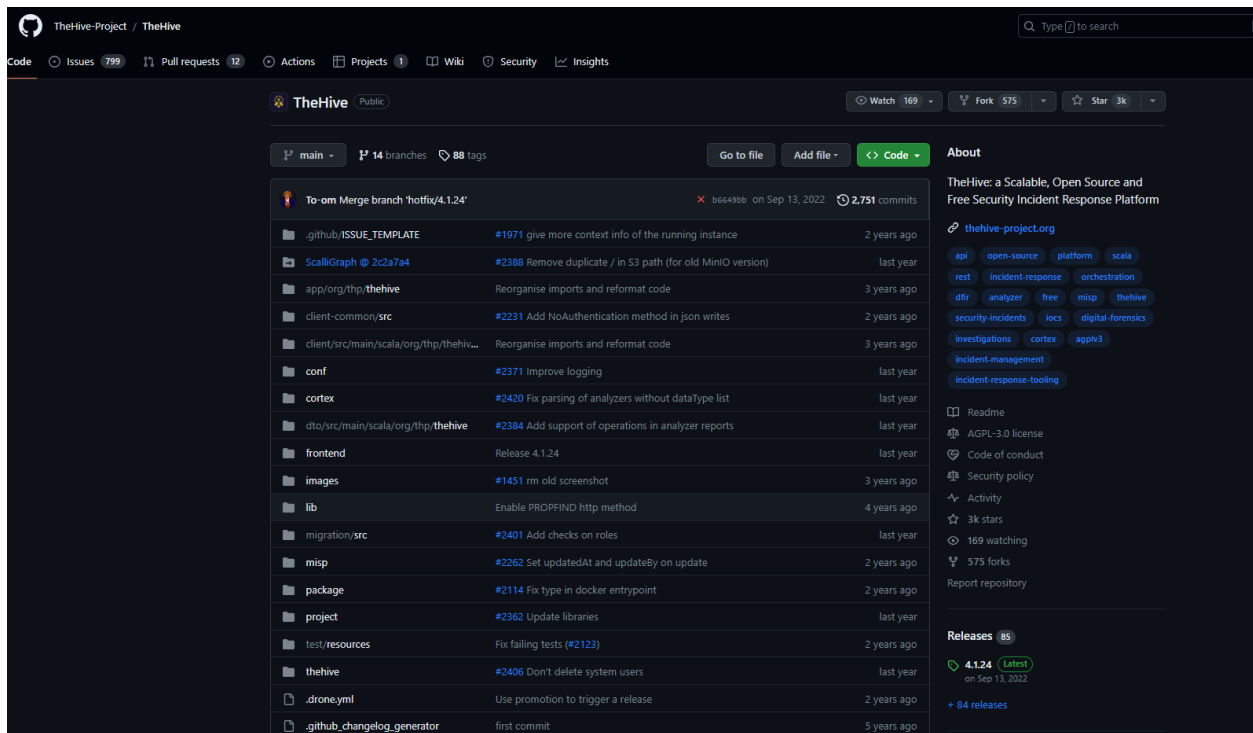


Figure 1: The structure of the source code of TheHive

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

2.1 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`.

2.2 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`.

2.3 conf

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

2.4 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`, and `Response`.

2.5 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`, and `UserDTO`.

2.6 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.

2.7 lib

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

2.8 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.

2.9 misp

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

2.10 project

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

2.11 test

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

3 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 Key Components

4.1 Organizations

- **Organization settings:** Allow users to configure the name, description, logo, and default roles of an organization.
- **Organization users:** The members of an organization who can access and work on cases and observables. Users can have different roles and permissions within an organization, such as admin, analyst, or read-only.
- **Organization templates:** Predefined case templates that can be used by an organization to create new cases with specific tasks and metrics . Templates can be shared with other organizations or imported from external sources.
- **Organization metrics:** Custom fields that can be used to measure and track the performance and progress of an organization's cases. Metrics can be defined by an organization admin and assigned to case templates or individual cases.

4.2 Cases

Cases are the security incidents that need to be investigated and handled by analysts using The Hive security tool. Cases can have various attributes, such as title, description, severity, start date, end date, tasks, and observables. Cases can also be shared with other organizations or platforms, such as MISP or Cortex.

4.3 Task

Task is a component of The Hive security tool that represents a sub-activity that needs to be performed to handle a case. Tasks can have their own title, description, status, owner, start date, end date, logs, and attachments. Tasks can also be assigned to different analysts or teams within an organization. Tasks can be created from case templates or manually by users.

4.4 Observables

Observables are the data elements that can be analyzed by Cortex or shared with MISP within The Hive security tool. Observables can have different types, such as IP address, URL, file, hash, etc., and different tags, such as IOC, TLP, or custom tags. Observables can also be ignored for similarity calculation between cases and alerts.

5 Documentation of Key features

5.1 Organization Admin

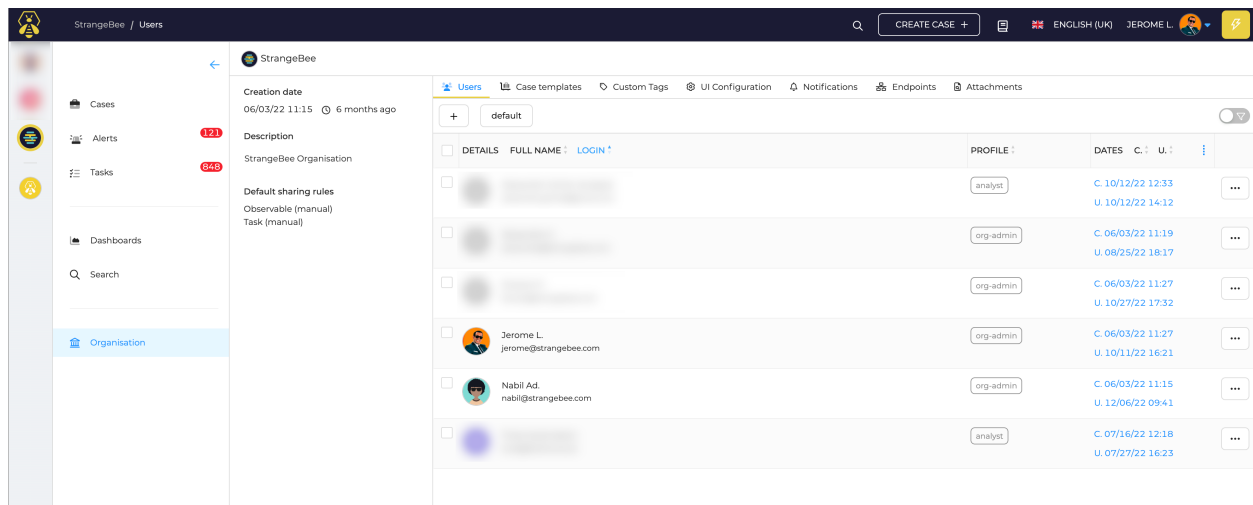
5.1.1 Manage Users

List of Users

To see a list of people in your organization, click on Organisation in the menu on the left. Users is the first tab.

User information

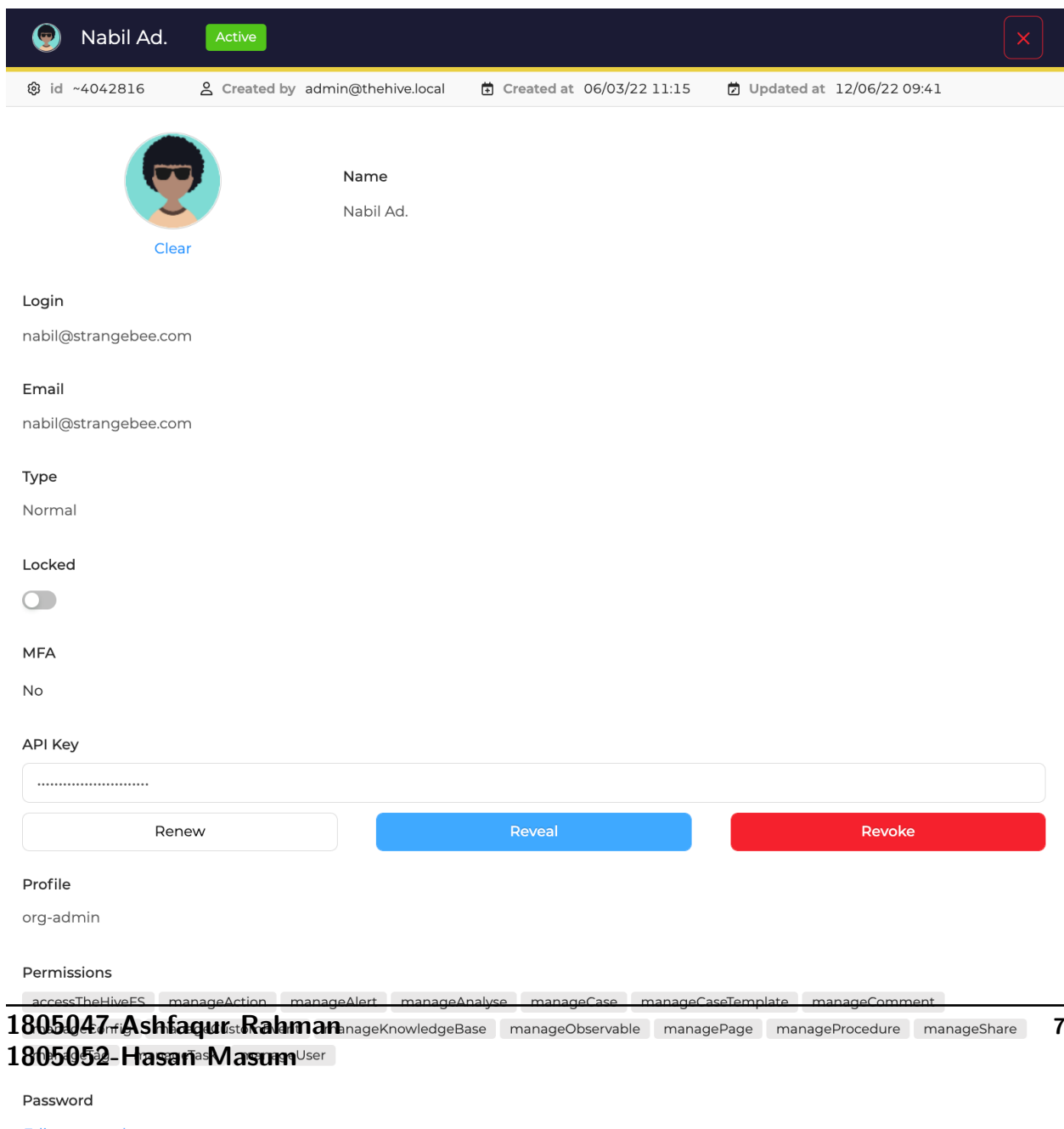
Click the Preview button to see more details about a user.



The screenshot shows the 'Users' page for the 'StrangeBee' organization. The left sidebar contains navigation links for Cases, Alerts (121), Tasks (646), Dashboards, and Search. The main content area displays a table of users with columns for checkboxes, details, full name, login link, profile, dates, and actions. The table lists several users, including Jerome L. and Nabil Ad., with their respective roles (analyst, org-admin) and creation/last update timestamps.

	DETAILS	FULL NAME	LOGIN	PROFILE	DATES	C.	U.	
<input type="checkbox"/>				analyst	C. 10/12/22 12:33 U. 10/12/22 14:12			...
<input type="checkbox"/>				org-admin	C. 06/03/22 11:19 U. 08/25/22 18:17			...
<input type="checkbox"/>				org-admin	C. 06/03/22 11:27 U. 10/27/22 17:32			...
<input type="checkbox"/>		Jerome L. jerome@strangebee.com		org-admin	C. 06/03/22 11:27 U. 10/11/22 16:21			...
<input type="checkbox"/>		Nabil Ad. nabil@strangebee.com		org-admin	C. 06/03/22 11:15 U. 12/06/22 09:41			...
<input type="checkbox"/>				analyst	C. 07/16/22 12:18 U. 07/27/22 16:23			...

Figure 2: List of user accounts



The screenshot shows the user profile page for 'Nabil Ad.' who is 'Active'. The page displays various user details and settings. At the top, there is a header with the user's name, status, and a close button. Below this, a summary bar shows the user's ID, creation details, and update date. The main content area includes a profile picture, name, and a 'Clear' button. Below the profile picture, there are sections for Login, Email, Type, Locked, MFA, API Key, Profile, and Permissions. The API Key section has a 'Renew' button, a 'Reveal' button, and a 'Revoke' button. The Profile section shows the user's role as 'org-admin'. The Permissions section lists various permissions, including 'accessTheHiveES', 'manageAction', 'manageAlert', 'manageAnalyse', 'manageCase', 'manageCaseTemplate', 'manageComment', 'manageKnowledgeBase', 'manageObservable', 'managePage', 'manageProcedure', 'manageShare', and 'manageUser'.

id ~4042816 **Created by** admin@thehive.local **Created at** 06/03/22 11:15 **Updated at** 12/06/22 09:41

Name
Nabil Ad.

Login
nabil@strangebee.com

Email
nabil@strangebee.com

Type
Normal

Locked
☐

MFA
No

API Key
[REDACTED]

Profile
org-admin

Permissions
accessTheHiveES, manageAction, manageAlert, manageAnalyse, manageCase, manageCaseTemplate, manageComment, manageKnowledgeBase, manageObservable, managePage, manageProcedure, manageShare, manageUser

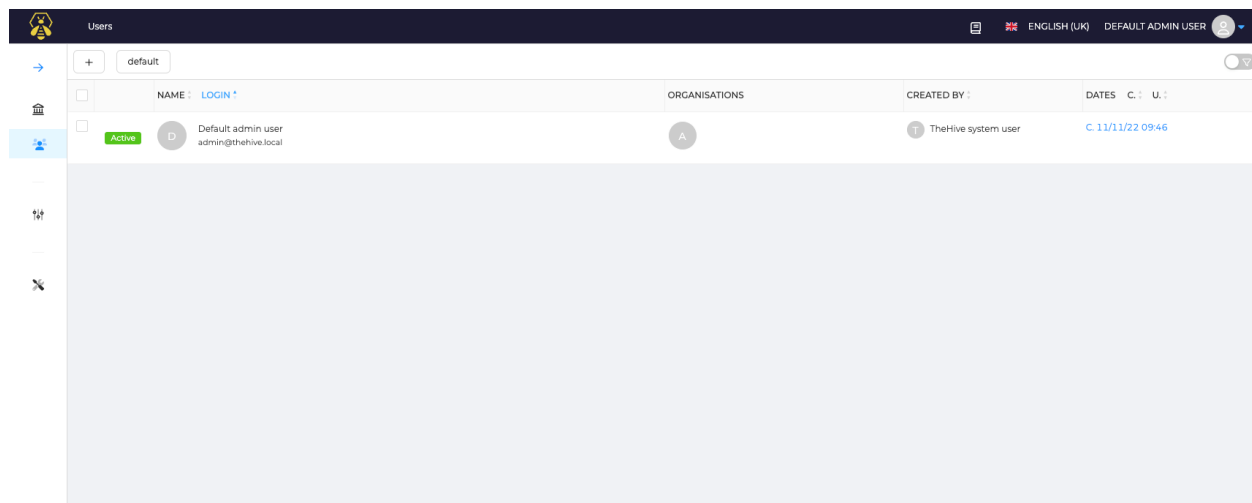
Renew **Reveal** **Revoke**

Configuration parameters

- **Avatar** : Update the avatar associated with the user by drag&drop a new file (PNG or JPG files).
- **Login**: User login
- **Email** : email address for the account. This is used to send notifications or reset password links to users. Login is used if no email is filled there
- **Type** : Type of the account. Normal or Service. A Service account cannot open interactive session
- **Locked** : Block a user from logging in the application
- **MFA** : Tells if a user has configured MFA or not (Multi Factor Authentication). If yes, Yes is displayed
- **API Key** : Define, Renew, Reveal or Revoke API key of the account
- **Profile** : Information about the profile given to the user
- **Permissions** : List of permissions included in the profile
- **Password** : Create or update the password of the user
- **Reset Password** : If the application is configured with a SMTP server, send an email with a magic link to the user. link is active for a short time period.
- **Sessions** : List of opened interactive sessions. Click delete to close a session

Add Users

org-admin users or users with the role manageUser in their profile can add users in the current Organisation.



Click the + button to add an account in the current organisation, and follow create an account and update an account guides.

The screenshot shows the 'Adding a User' form in TheHive. The form is divided into several sections with red numbered annotations:

- 1**: Type dropdown menu, currently set to 'Normal'.
- 2**: Login text input field containing 'jerome@strangebee.com'.
- 3**: Name text input field containing 'Jérôme L.'.
- 4**: Organisations section showing a list of organisations ('admin', 'StrangeBee') with a dropdown menu open, showing options: 'analyst', 'org-admin', and 'read-only'.

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

In the list of accounts, click Preview to open accounts details view.

The screenshot shows the user details view for 'Jérôme L.' in TheHive. The view is divided into several sections with red numbered annotations:

- 1**: Name field showing 'Jérôme L.' with a 'Clear' button.
- 2**: Email field showing 'jerome@strangebee.com'.
- 3**: MFA (Multi-Factor Authentication) toggle switch, currently set to 'No'.
- 4**: Password section with a 'Set a new password' link.
- 5**: Password section with a 'Reset the password' button.
- 6**: Organisations section showing 'StrangeBee' as the 'Default organisation' with a dropdown menu set to 'org-admin'.
- 7**: A red 'Delete user' button at the bottom.

5.1.2 Templates

- Case

List of Case Templates

Access to the list by opening the Organisation menu, then the Templates tab, and the Cases tab.

The screenshot shows the 'Case Templates' page in TheHive. The left sidebar contains navigation links: Cases, Alerts (120), Tasks (640), Dashboards, and Organisation (selected). The main content area shows the 'StrangeBee' organisation details, including creation date (06/03/22 11:15) and description. Below this is a table of case templates.

DISPLAY NAME	NAME	DETAILS	BY	DATES	C.	U.	
TLP:AMBER SEV:LOW Worm Infection (CERT-SG IRM1)	Worm Infection	Tasks Custom Fields	12	C. 06/17/22 09:22 U. 09/01/22 17:02			...
TLP:AMBER SEV:LOW Phishing (CERT-SG IRM13)	Phishing	Tasks Custom Fields	12	C. 06/17/22 09:23 U. 06/17/22 09:23			...
TLP:AMBER SEV:HIGH Website defacement (CERT-SG IRM6)	Website defacement	Tasks Custom Fields	9	C. 06/17/22 09:23 U. 06/17/22 09:23			...
TLP:AMBER SEV:LOW Trademark infringement (CERT-SG IRM15)	Trademark infringement	Tasks Custom Fields	11	C. 06/17/22 09:23 U. 06/17/22 09:23			...
TLP:AMBER SEV:MEDIUM Information Leakage (CERT-SG IRM11)	Information Leakage	Tasks Custom Fields	8	C. 06/17/22 09:24 U. 06/17/22 09:24			...
TLP:AMBER SEV:HIGH Unix/Linux Intrusion Detection (CERT-SG IRM3)	Unix/Linux Intrusion Detection	Tasks Custom Fields	15	C. 06/17/22 09:24 U. 06/17/22 09:24			...
TLP:AMBER SEV:MEDIUM Smartphone Malware (CERT-SG IRM9)	Smartphone Malware	Tasks Custom Fields	7	C. 06/17/22 09:28 U. 06/17/22 09:28			...
TLP:AMBER SEV:CRITICAL Ransomware (CERT-SG IRM17)	Ransomware	Tasks Custom Fields	9	C. 06/17/22 09:24 U. 06/17/22 09:24			...
TLP:AMBER SEV:MEDIUM Scam (CERT-SG IRM14)	Scam	Tasks Custom Fields	10	C. 06/17/22 09:24 U. 06/17/22 09:24			...
TLP:AMBER SEV:LOW Malicious Network Behaviour (CERT-SG IRM5)	Malicious Network Behaviour	Tasks Custom Fields	12	C. 06/17/22 09:28 U. 06/17/22 09:28			...

Figure 4: List of case templates

New Case template

Click the + button to create a new Case template.

Adding a Case Template

Prefix

Case template title prefix...

Name

Worm infection

Display name

Worm infection (CERT-SG IRM1)

TLP

TLP: CLEAR

TLP: GREEN

TLP: AMBER

TLP: AMBER-STRICT

TLP: RED

PAP

PAP: CLEAR

PAP: GREEN

PAP: AMBER

PAP: RED

Severity

LOW

MEDIUM

HIGH

CRITICAL

Tags

CERT-XLM:malicious-code="worm"

Description

Worm infection

Tasks

Preparation - Preparation

Identification - Detect the infection

Identification - Identify the infection

Containment - Containment

Remediation - Identify

Remediation - Test

Remediation - Deploy

Remediation - Recovery

Aftermatch - Report

Aftermatch - Capitalize

Custom fields

string - business-unit

Pages

Aftermatch - Learnit

Aftermatch - Post Mortem

Cancel

Confirm case template edition

Figure 5: New case template

Configuration parameters

- **Prefix** : String that will be prepended to the title of a Case when created with this template
- **Name** : Name of the Case template. Used to identify the Case template with the API
- **Display Name** : Name of the Case template displayed in the UI
- **TLP** : Default TLP of the Case when created with this template
- **PAP** : Default PAP of the Case when created with this template
- **Severity** : Default Severity of the Case when created with this template
- **Tags** : List of tags that will be added to the Cases created with this template
- **Description** : Default description of Cases created with this template if not modified.
- **Tasks** : Add tasks to the templates. They will be automatically added to the Case when created

- with this template
 - **Custom Fields** : Add Custom fields to the template. Default value can be set for Custom fields as well.
 - **Pages** : Add pages template to the template. They will be automatically added to the Case when created with this template
- Pages

List of Page Templates

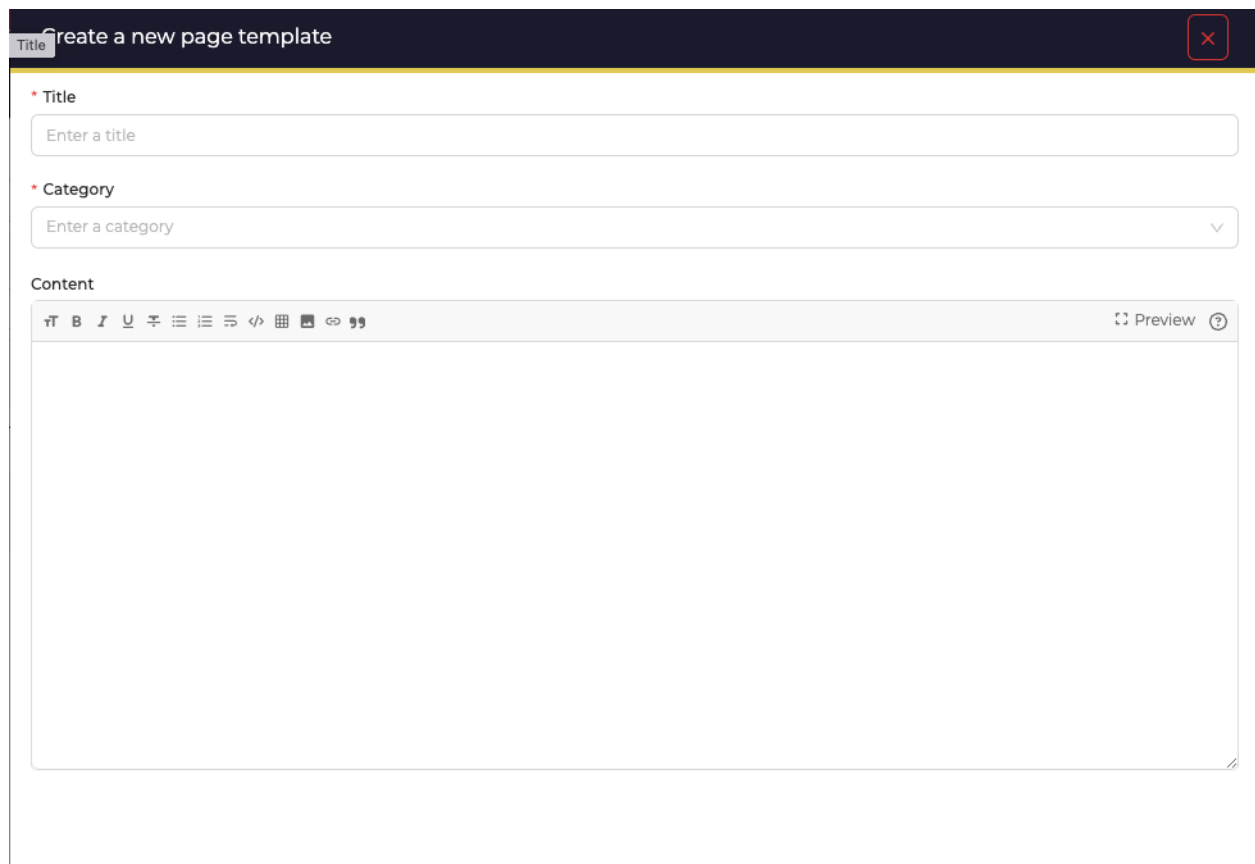
Access to the list by opening the Organisation menu, then the Templates tab, and the Pages tab.

<div> Users Templates Custom Tags UI Configuration Notifications Endpoints Functions^{BETA} Attachments </div>									
<div> Cases Pages Reports </div>									
<div> + Import Page Template default </div>									
CATEGORY	TITLE	DETAILS	BY	DATES	C.	U.			
Aftermatch	Post Mortem	Linked case templates	2	C. 27/06/2023 08:32					...
Aftermatch	Learnt	Linked case templates	2	C. 27/06/2023 08:32					...

Figure 6: List of pages templates

New Case template

Click the + button to create a new Page template.



Create a new page template

*** Title**
Enter a title

*** Category**
Enter a category

Content

Rich text editor toolbar: Bold, Italic, Underline, Text color, Background color, Bulleted list, Numbered list, Indent, Outdent, Source code, Table, Link, Unlink, Undo, Redo. Preview button.

Figure 7: New Page template

Configuration parameters

- **Title** : Page template title. Used to identify the Page template with the API. Also used as a page title when the template is used in a case.
- **Category** : Category for grouping pages on a common theme. Is used as a page tree in the case of.
- **Content** : Default page content when the page template is used in a case.

5.1.3 Tags

Custom tags

Custom tags collect all tags from Alerts or added to Cases or Observables that are not included in TheHive Taxonomies, even if they are not activated.

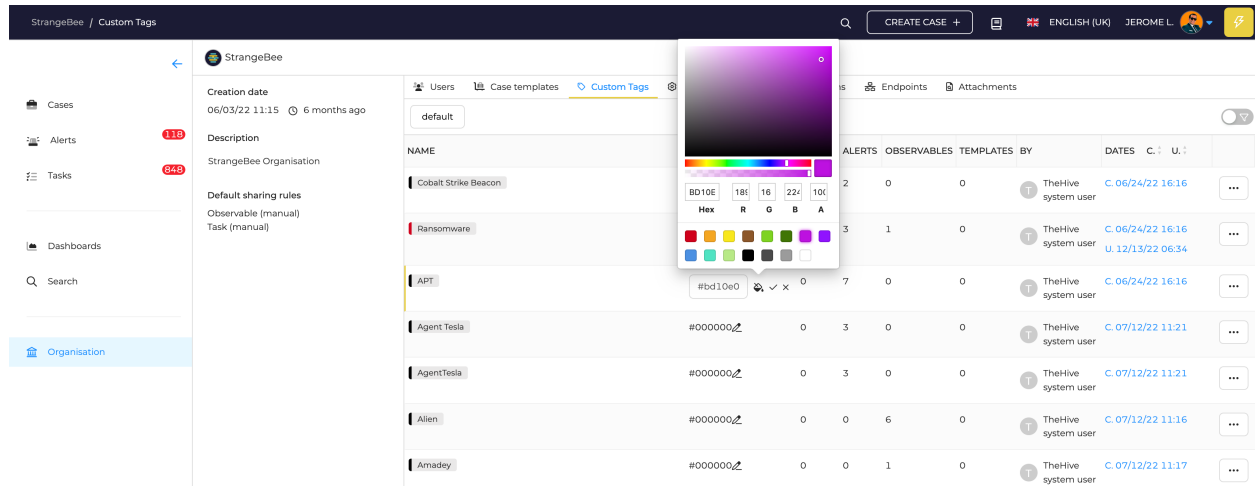


Figure 8: Custom tags

Configuration

- Names and colors can be adjusted for all Custom tags
- Each tag can also be deleted

Warning: Deleting a tag from this menu will remove the tag on every Alert, Case & Observables in the organisation.!

5.2 Analyst

5.2.1 Cases

- Create

Create new cases

A User can create new cases using templates. Click Create Case + on the header.

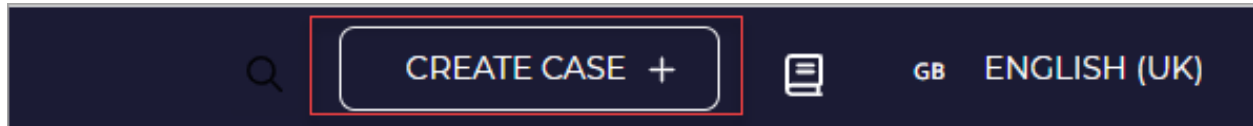


Figure 9: create case header

A new screen opens. A user can create cases by selecting any one of the following options:

Click the below links to create each type of new case.

Empty Case EDR / Phishing Template Archive MISP

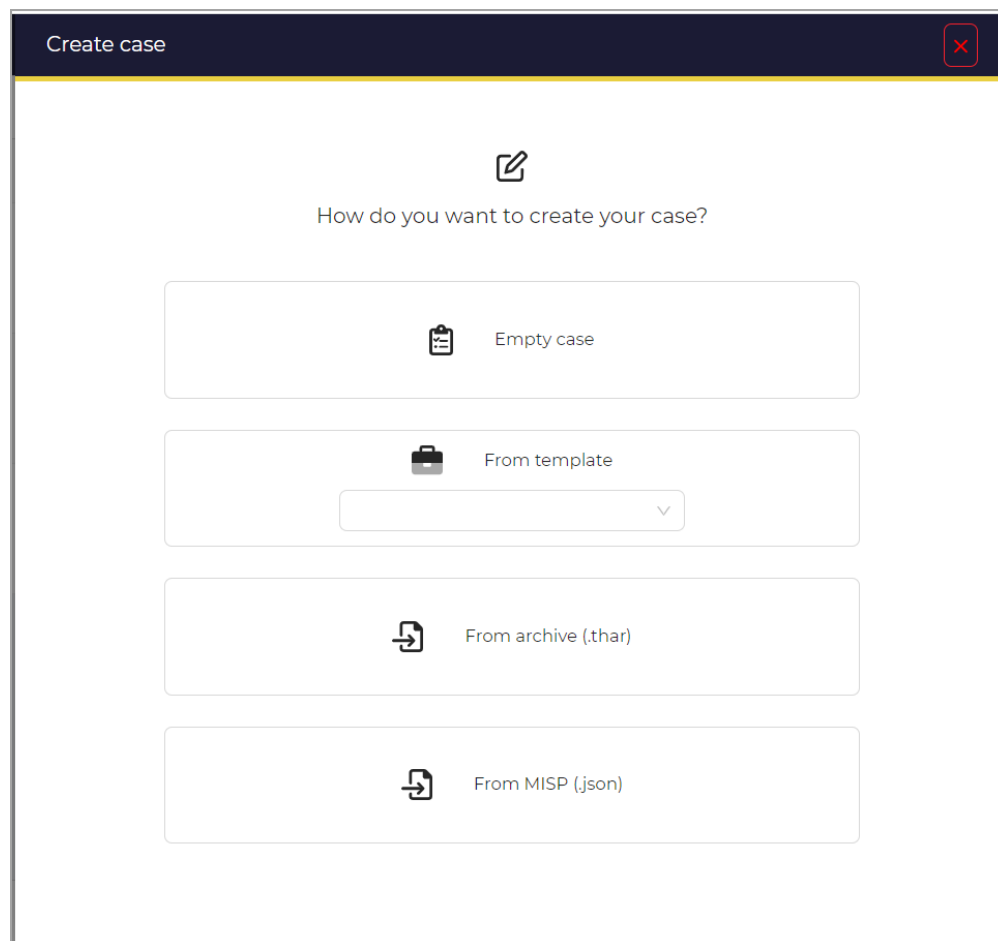


Figure 10: create case

From an empty case

Create a new case from an empty case.

- Enter the case title in the Title.
- Select the date from the Date.
- Select Severity, (Low/Medium/High/Critical).
- Select TLP, (White/Green/Amber/Red).
- Select PAP, (White/Green/Amber/Red).
- Click + to add Tags. (Refer to Add tags).
- Enter the case description in the Description.
- Choose a Task rule from the list, (manual/existingOnly/upcommingOnly/all).
- Choose an Observable rule from the list, (manual/existingOnly/upcommingOnly/all).
- Add Tasks. (Refer to Add tasks).
- Add Custom Fields. (Refer to Add custom field values).
- Click the Confirm case creation button.

The screenshot shows the 'Create case' form in TheHive. The form has a dark blue header with a back arrow and a close button. The main content area is white with a yellow border. It contains the following fields and options:

- Title ***: A text input field with the placeholder 'Case title...'.
- Date ***: A date and time picker showing '17/02/2022 07:13'.
- Severity**: Four buttons: LOW, MEDIUM (selected), HIGH, and CRITICAL.
- TLP**: Four buttons: TLP:WHITE, TLP:GREEN, TLP:AMBER (selected), and TLP:RED.
- PAP**: Four buttons: PAP:WHITE, PAP:GREEN, PAP:AMBER (selected), and PAP:RED.
- Tags ****: A text input field with the placeholder 'Tags' and a '+' button to add tags.
- Description ****: A rich text editor with a toolbar and a 'Preview' button. The placeholder text is 'Describe the case here...'.

Below the description field, there is a red error message: 'At least, one required field **'. At the bottom of the form, there are two tabs: 'Tasks' and 'Custom fields'. The 'Tasks' tab is active, showing a message: 'No tasks have been found. [Add a task](#)'. There is a blue 'Add a task' button next to this message. At the very bottom, there are two buttons: 'Cancel' and 'Confirm case creation'. The 'Confirm case creation' button is highlighted with a red box.

Figure 11: create empty case

From template

- Enter the case title in the Title.
- Select the date from the Date.
- Select Severity, (Low/Medium/High/Critical).
- Select TLP, (White/Green/Amber/Red).
- Select PAP, (White/Green/Amber/Red).
- Click + to add Tags. (Refer to Add tags.)
- Enter the case description in the Description.
- Choose a Task rule from the list, (manual/existingOnly/upcommingOnly/all).
- Choose an Observable rule from the list, (manual/existingOnly/upcommingOnly/all).
- Add Tasks. (Refer to Add tasks. / Edit tasks. /Delete tasks.)
- Add Custom Fields. (Refer to Add custom field values. /Edit custom field values. /Delete custom field values.)
- Add Pages. (Refer to Add pages. /Delete pages.) Sharing (Refer to Sharing.)
- Click the Confirm case creation button.

The screenshot shows the 'Create case from template: Worm infection (CERT-SG IRM1)' form. The form is divided into several sections:

- Title:** A text input field containing 'Worm Infection'.
- Date:** A date picker showing '2023-06-26'.
- Severity:** Radio buttons for LOW, MEDIUM, HIGH, and CRITICAL. 'LOW' is selected.
- TLP:** Radio buttons for TLP-CLEAR, TLP-GREEN, TLP-AMBER, TLP-AMBER-STRICT, and TLP-RED. 'TLP-AMBER' is selected.
- PAP:** Radio buttons for PAP-CLEAR, PAP-GREEN, PAP-AMBER, and PAP-RED. 'PAP-AMBER' is selected.
- Tags:** A text input field containing 'CERT:XML:malicious-code:worm'.
- Description:** A rich text editor containing 'Worm infection'.
- Tasks:** A list of tasks with 'Edit' and 'Delete' buttons. The tasks are:
 - Preparation - Preparation
 - Identification - Detect the infection
 - Identification - Identify the infection
 - Containment - Containment
 - Containment - Mobile devices
 - Remediation - Identify
 - Remediation - Test
 - Remediation - Deploy
 - Remediation - Recovery
 - Aftermatch - Report
 - Aftermatch - Capitalize
- Buttons:** 'Add a task' (circled in red), 'Cancel', and 'Confirm' (circled in red).

Figure 12: create case from template

- Preview

Preview Cases

On the list of case details page, there is a Preview button corresponding to the specific case name. Click the Preview option.

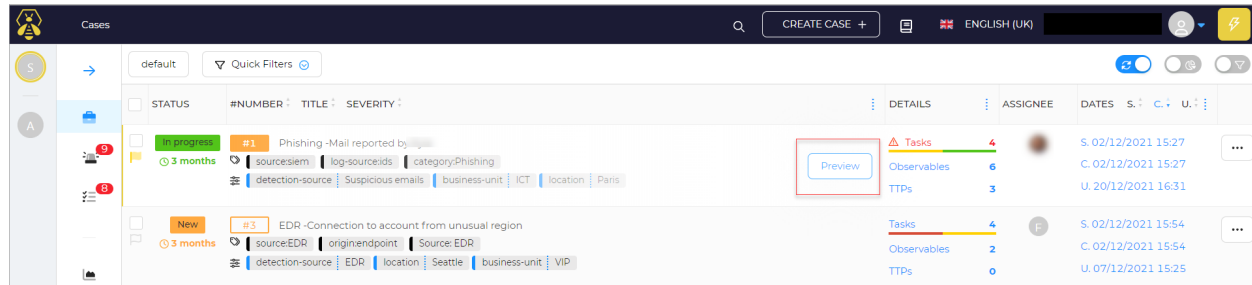


Figure 13: case list

The case details preview window opens.

Case #1

_id ~40976456

Created by

Created at 02/12/2021 15:27

Updated at 20/12/2021 16:31

TLP:AMBER

PAP:AMBER

SEV:MEDIUM

Assignee

Contributors

Start date

End date

Tasks 4

Observables 6

TTPs 3

Title *

Phishing -Mail reported by

Status

In progress

Tags

source:siem log-source:ids category:Phishing

Description

User kyle has reported the following suspicious email

Custom Fields Add

default 3

business-unit ? Add

detection-source ? Add

location ? Add

ICT

Suspicious emails

Paris

Actions

Go to details

- Adding Task and Pages

Add tasks

The task Group is default.

- Enter the task Title.
- Enter the task description in the Description.
- Switch the toggle button to Flag this task?.
- Select the Due date.
- Click Save and add another, to add another task.
- Click Confirm.

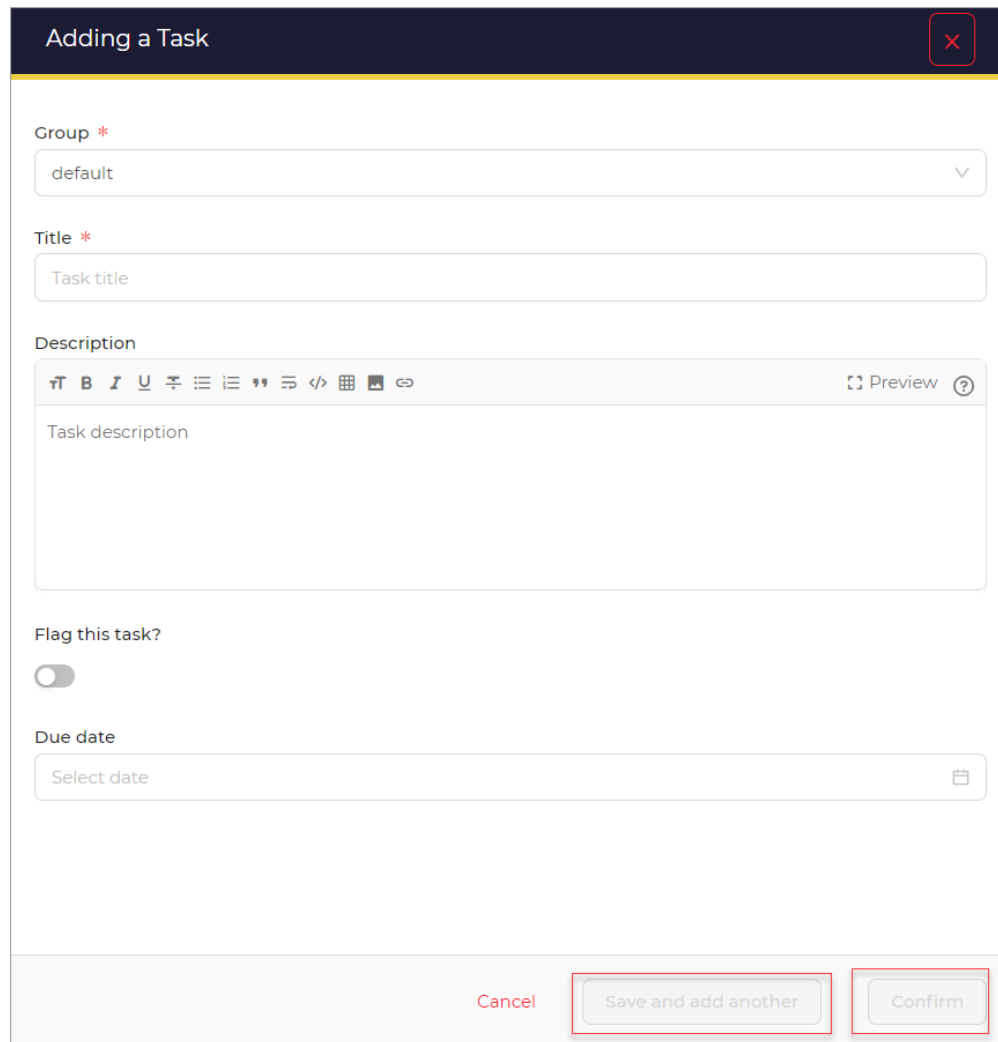


Figure 14: add a task

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 15: add tags

Add pages

By selecting Create new page

- Enter the page Title.
- Enter or select the Category.
- Enter the page content in the content.
- Click Confirm.
- Click Save and add another, to add another task.

Add new page

Create new pageUse an existing page template

TitleEnter a titleCategoryEnter a category

Content< B I U List Bulleted Numbered Code Link Image Video Embed Preview ?>

CancelSave and add anotherConfirm

Figure 16: add a new page

By selecting Use an existing page template

Choose template(s) from those available in the list of existing templates Click Confirm. Click Save and add another, to add another task.

Adding a page

Import Page Template

Choose an action

Create new page

Use an existing page template

• Import Page Template

Search by category or title

Aftermatch

Learnt

Post Mortem

Cancel

Confirm

Figure 17: with an existing page

5.2.2 Tasks

- About

To view task details

You can click on any of the tasks in the list to view more details.

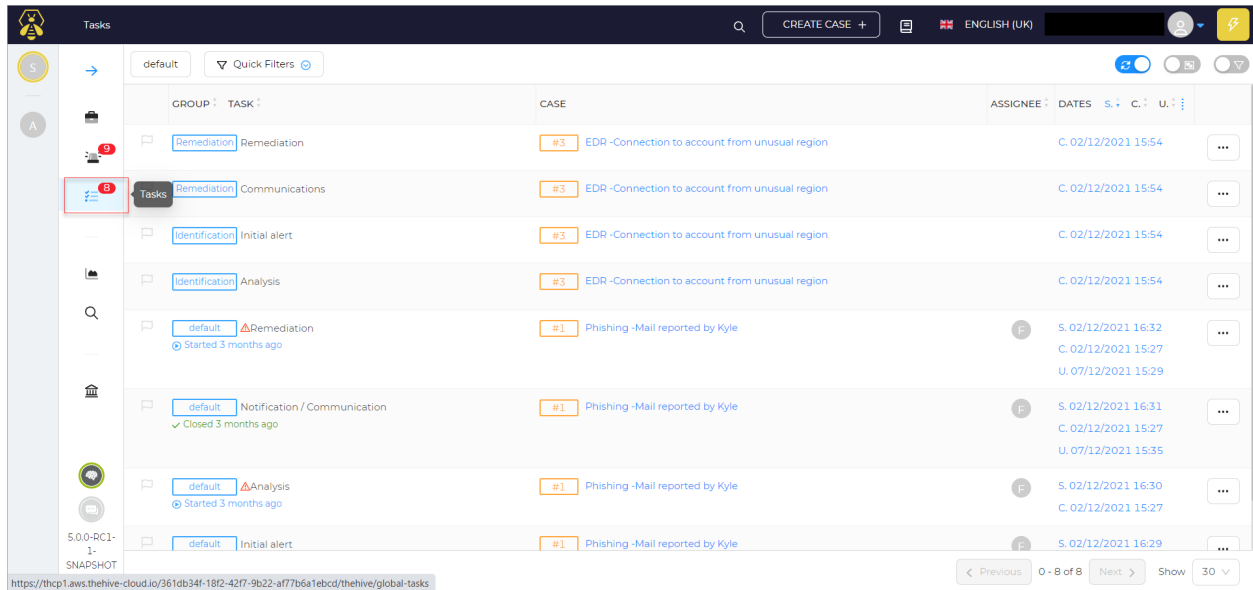
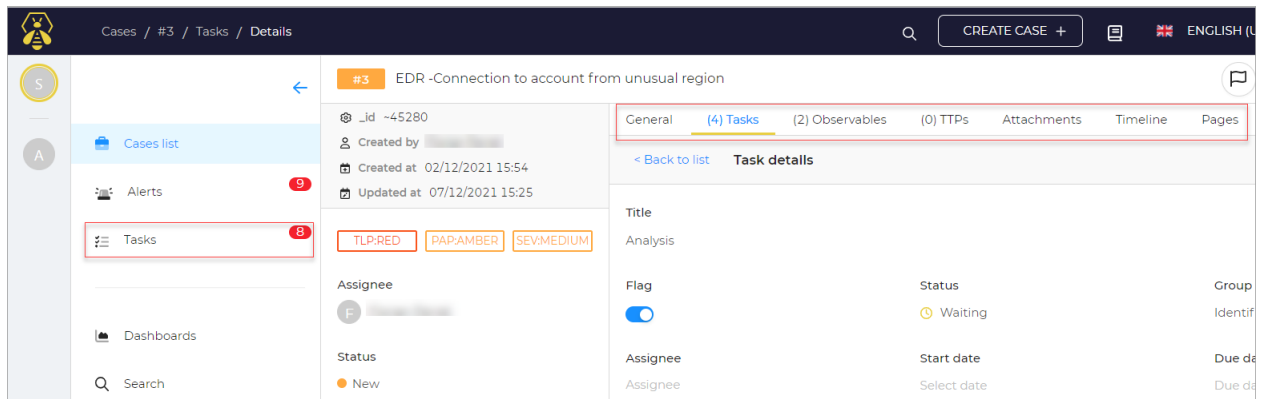


Figure 18: task list

The details are displayed



- Preview

To preview the task details:

On the list of tasks page, there is a Preview button corresponding to the specific task name.

Click the Preview option.

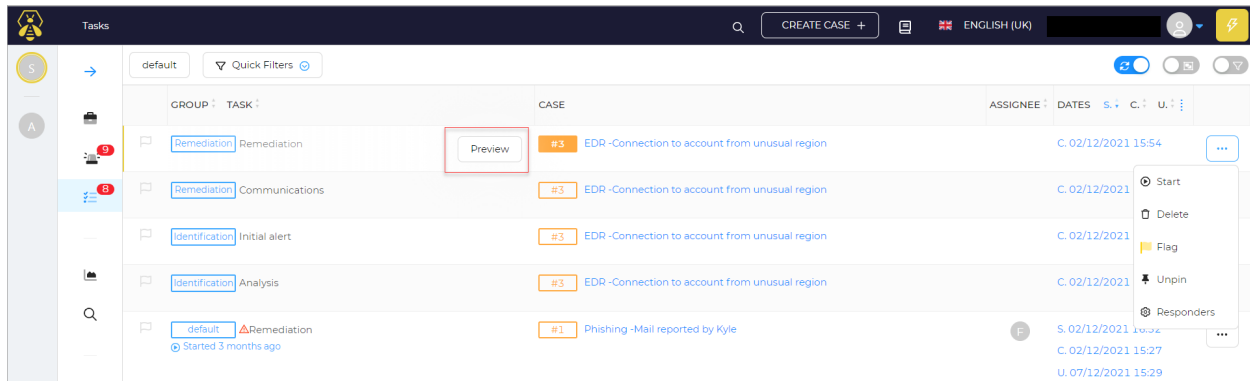


Figure 19: task list

The task details preview window opens.

1805047-Ashfaqur Rahman
1805052-Hasan Masum

- Actions

Actions

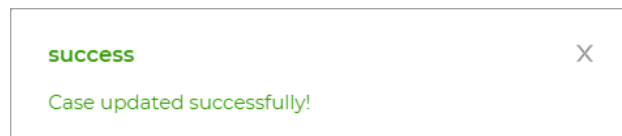
You can make use of any of the available actions.

<input type="checkbox"/>	STATUS	#NUMBER	TITLE	SEVERITY	⋮	DETAILS	⋮	ASSIGNEE	DATES	S. ⬆	C. ⬆	U. ⬆	⋮
<input type="checkbox"/>	New	#3	case-2-malicious ip attack			Tasks	2	T	S. 07/09/2023 13:07				⋮
	7 days	ip				Observables	2		C. 07/09/2023 13:07				
		None				TTPs	0		U. 14/09/2023 13:07				
<input type="checkbox"/>	New	#1	Test			Tasks	3	T	S. 23/08/2023 13:07				⋮
	22 days	hunting				Observables	2		C. 23/08/2023 13:07				
		Hits				TTPs	1		U. 07/09/2023 13:07				

Apply case template
 Flag case(s)
 Close case(s)
 Responders

Flag/Unflag

Click the Flag/Unflag option to either flag or unflag a case. A pop-up message appears



Close case

Click the Close option to remove a case A new window opens.

- Select Status from the list.
- Change the Summary
- Click the Close tasks and case button.

Close case #1

This case contains the following open or unassigned tasks. Closing the case will permanently remove the unassigned ones. This action cannot be undone.

Task	Date	Assignee
<div>defaultAnalysis</div> <div>Started 3 months ago</div>	02/12/2021 15:27	F
<div>defaultRemediation</div> <div>Started 3 months ago</div>	02/12/2021 15:27	F

Status *

InProgress

Summary *

⌵

B

I

U

↶

☰

☷

🔍

≡

</>

📱

🖼️

🔗

Preview ?

Close summary

Cancel

Close tasks and Case

Figure 20: Closing a case

5.3 Observables

5.3.1 Create Case Observables

In a TheHive case, observables can be declared. Open the Observables list (Case > Observables) to create an observable. You must have permission to administer cases.

The Add observable icon is located on the Observables tab:

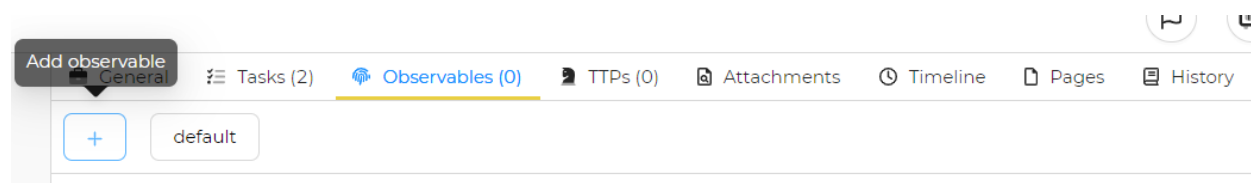


Figure 21: Adding observables

In the pop-up, you are invited to fill the observable(s) details:

- Type *: The **observable dataType** (e.g.: ip, hash, domain, ...)
- Value *: Your observable value (e.g.: 8.8.8.8)
 - One observable per line: Create one observable per line inserted in value field.
 - One single multiline observable: Create one observable, no matter the number of lines (useful for long URLs for example).
- TLP *: Define here the way the information should be shared.
- Is IOC: Check it if this observable is considered as Indicator of Compromission.
- Has been sighted: Has this observable been sighted on your information system.
- Ignore for similarity: Do not correlate this observable with other similar observables.
- Tags **: Tag your observable with insightful information.
- Description **: Description of the observable.

 A screenshot of the 'Adding an Observable' pop-up form. The form has a title bar with a close button. It contains several sections:

- Type**: A dropdown menu with 'ip' selected.
- Value**: A text area containing '103.94.135.159'. To the right, there's a toggle for 'One observable per line' (checked) and '1 observable(s)'.
- TLP**: A row of buttons: 'TLP-CLEAR', 'TLP-GREEN', 'TLP-AMBER' (selected), 'TLP-AMBER-STRICT', and 'TLP-RED'.
- PAP**: A row of buttons: 'PAP-CLEAR', 'PAP-GREEN', 'PAP-AMBER' (selected), and 'PAP-RED'.
- Is IOC**: A toggle switch (unchecked).
- Has been sighted**: A toggle switch (checked).
- Ignore similarity**: A toggle switch (unchecked).
- Tags**: A text input field containing 'not malicious'.
- Description**: A rich text editor with a toolbar and a preview button. The text 'Hello world!' is entered.

 At the bottom, there are three buttons: 'Cancel', 'Save and add another', and 'Confirm'.

Figure 22: Creating observables

Finally, click on Create Observable(s)

5.3.2 Run analyzers

In TheHive4 you can run analyzers on observables.

To run an analyzer, you must have the manageAnalyse permission

From an observable page

You can trigger an analyzer on a single observable from it's page (Case \rightarrow Observables \rightarrow Observable).

In the Analysis section, you'll find every analyzers available for your organisation and compatible with the observable dataType:

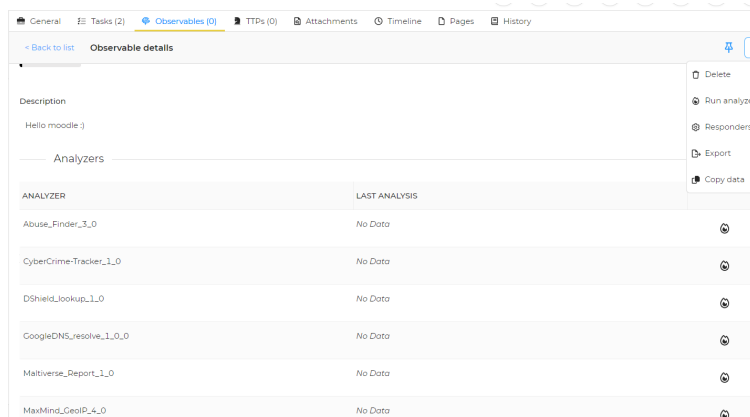


Figure 23: Available analyzers

From the observables list

You can also trigger one or more analyzers on one or more observables from the Observables list (Case \rightarrow Observables).

On the left side of the Observables list, you have checkboxes to select which observables to act on. You can even select all of them using the checkbox that is at the very top of the Observables list:

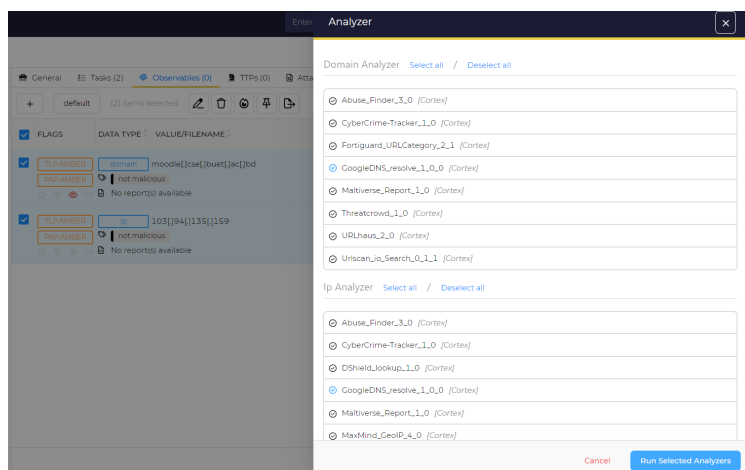


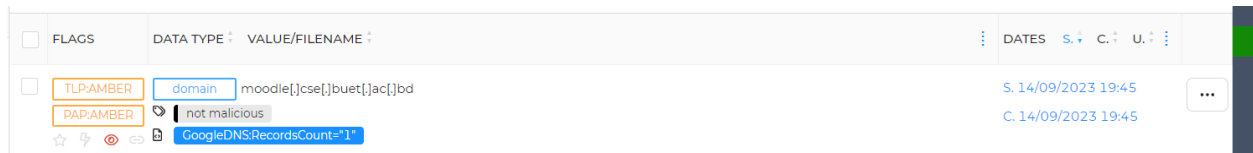
Figure 24: Running analyzers from observables list

Consult analyzers report

Once the analyzer has been triggered and the job terminated, you can consult the Job report directly within TheHive.

Short report

In the Observables list (Case *i* Observables), you have access to a short report:

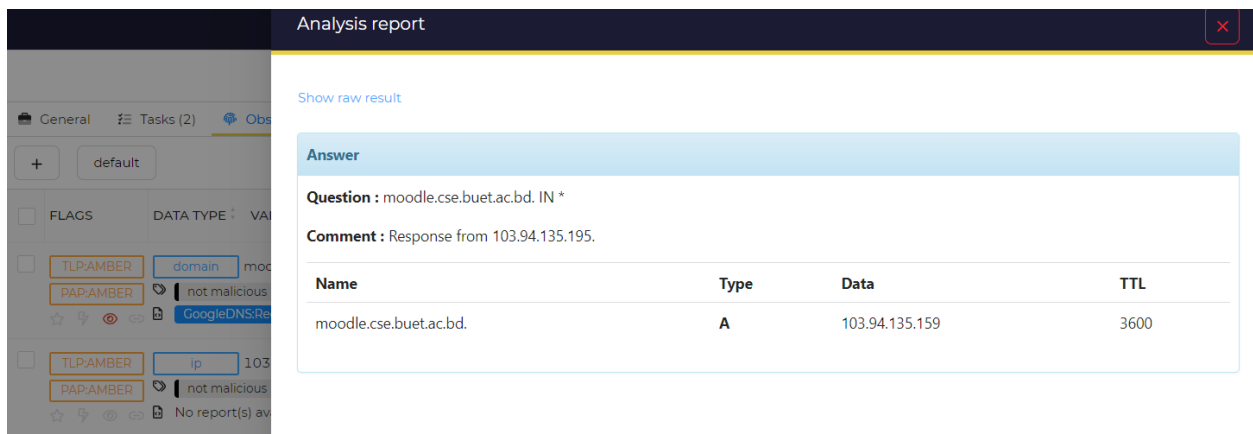


<input type="checkbox"/>	FLAGS	DATA TYPE	VALUE/FILENAME	DATES	
<input type="checkbox"/>	TLP:AMBER	domain	moodle[.]cse[.]bu[.]et[.]ac[.]bd	S. 14/09/2023 19:45	...
	PAP:AMBER	not malicious		C. 14/09/2023 19:45	
			GoogleDNS:RecordsCount="1"		

Figure 25: Short report

Long report

On the Observable page (Case *i* Observables *i* Observable), in the Analysis table, you can consult an HTML-formatted long report by clicking on the analysis link:



Analysis report			
Show raw result			
Answer			
Question : moodle.cse.bu[.]et[.]ac[.]bd. IN *			
Comment : Response from 103.94.135.195.			
Name	Type	Data	TTL
moodle.cse.bu[.]et[.]ac[.]bd.	A	103.94.135.159	3600

Figure 26: Long report

References

- [1] TheHive Project GitHub repository: <https://github.com/TheHive-Project/TheHive>
- [2] TheHive Project documentation: <https://docs.thehive-project.org/thehive/>
- [3] The hive official guide: <https://docs.strangebee.com/thehive/setup/>