CSE406-Computer Security Sessional
Report on TheHive - an open source and free Security Incident Response Platform

1905102: Shafiul Haque

1905116: Md. Sayeeduzzaman

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

March 9, 20

Contents

1 Introduction

TheHive is an open source and free securit y 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 any one can access, review, or contribute to it. In this rep ort, we will provide a high level overview of the main modules.

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 in to several modules and packages , each with a specific purpose and functionality. Figure 1 shows the structure of the source code

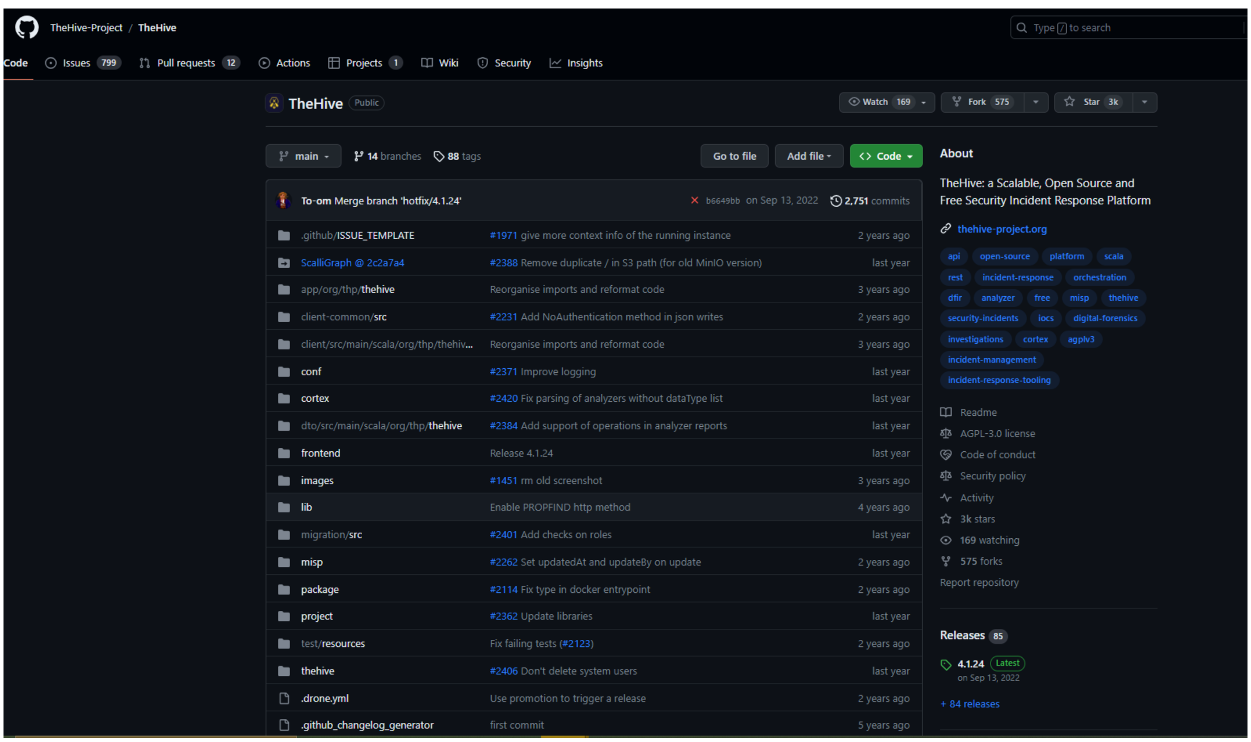


Figure 1: The structure of the source code of TheHive

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 TheHive App , TheHive Module, and TheHive Config .
- 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 op erations for the datamodels, 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 con tains the co de for the web-based user interfac e 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 Dash boardPage, CasePage, TaskP age, 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, Notification Service, UserService, and Organisation Service.

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 pack age contains the case classes and objects that represent the data models of Cortex, such as Analyzer, Job, Report, Responder, Action, 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, 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 TheHiv e. 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 even ts, 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 suc h as IP an d 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 Th e Hive or from alternative SIRP platforms, custom scripts or MISP .
- Active response : Cortex also enables users to perform activ e response actions on observables, such as blocking an IP ad dress , 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 with in 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 adm n and assigned to case templates or individual cases.

4.2 Cases

Cases are the security incidents that need to be investigated and handled b y analysts using The Hive security to ol. Cases can have various attributes, such as title, description, severity , start date, end date, tasks, and observables. Cases can also b e 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 b y 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

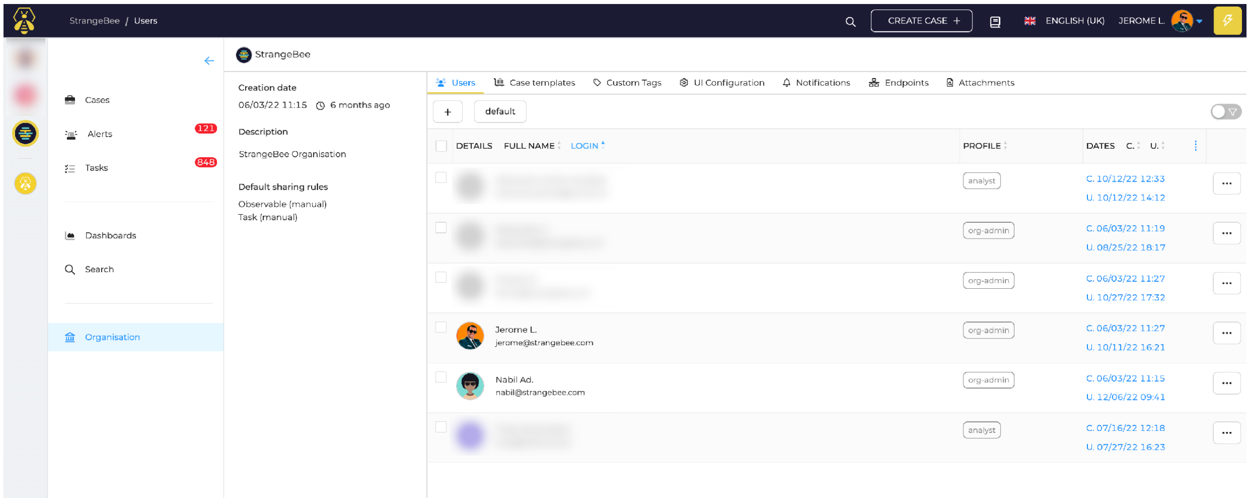
5.1.1 Manage Users

List of Users

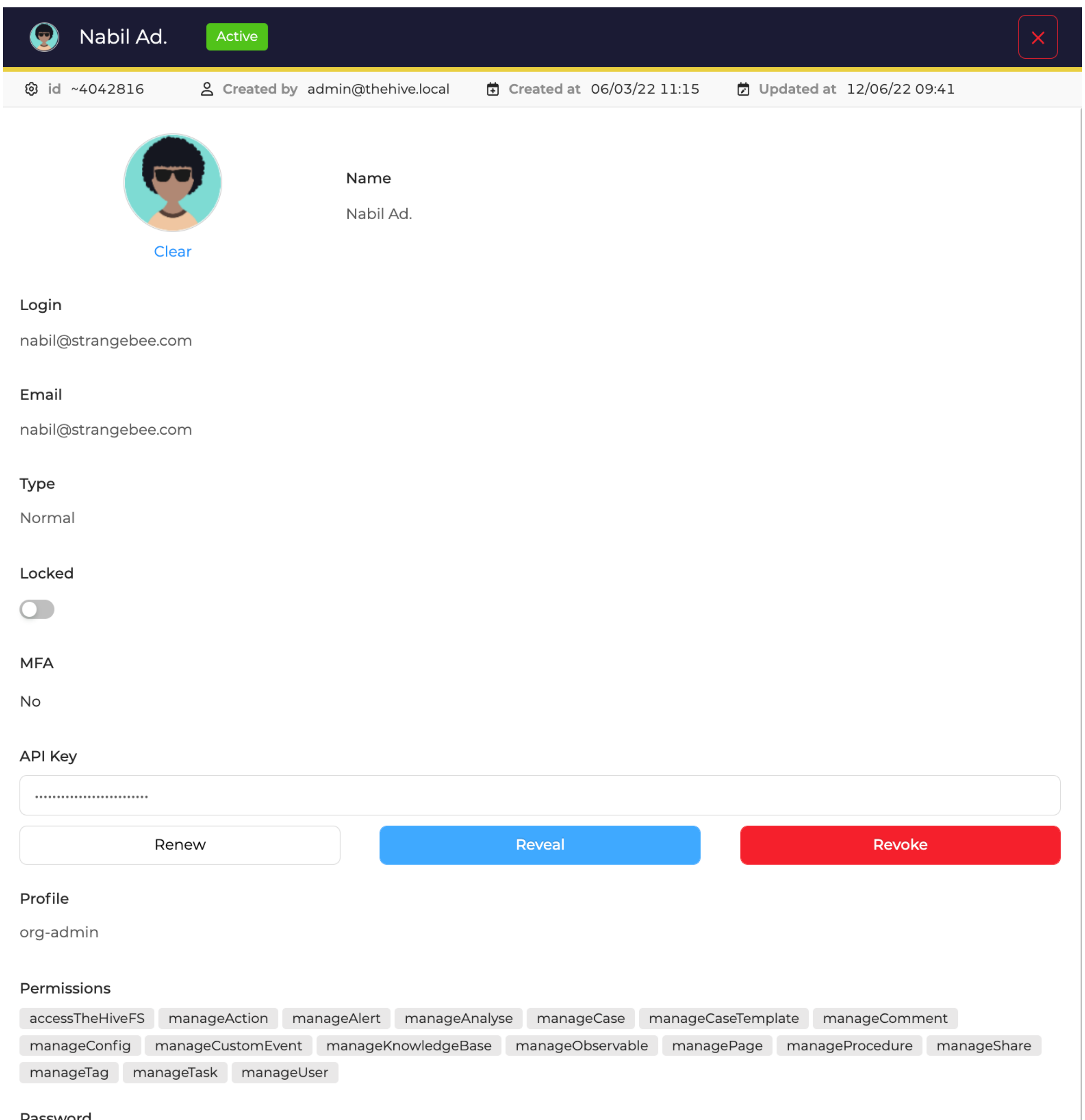
To see a list of people in your organization, click on Organisation in the menu on the left. Users is the first tab.

User information

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


StrangeBee / Users
CREATE CASE +
ENGLISH (UK)
JEROME L.
Cases
Alerts
121
Tasks
848
Dashboards
Search
Organisation
StrangeBee
Creation date
06/03/22 11:15
6 months ago
Description
StrangeBee Organisation
Default sharing rules
Observable (manual)
Task (manual)
Users
Case templates
Custom Tags
UI Configuration
Notifications
Endpoints
Attachments
default
DETAILS
FULL NAME
LOGIN
PROFILE
DATES
C.
U.
analyst
C. 10/12/22 12:33
U. 10/12/22 14:12
org-admin
C. 06/03/22 11:19
U. 08/25/22 18:17
org-admin
C. 06/03/22 11:27
U. 10/27/22 17:32
Jerome L.
jerome@strangebee.com
org-admin
C. 06/03/22 11:27
U. 10/11/22 16:21
Nabil Ad.
nabil@strangebee.com
org-admin
C. 06/03/22 11:15
U. 12/06/22 09:41
analyst
C. 07/16/22 12:18
U. 07/27/22 16:23

Figure

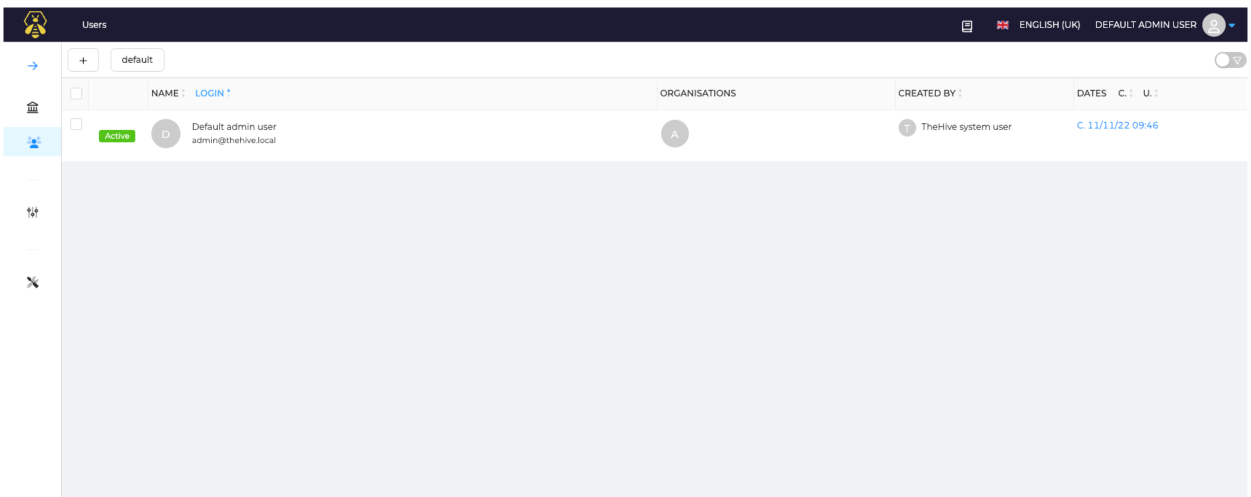

Nabil Ad.
Active
id ~4042816
Created by admin@thehive.local
Created at 06/03/22 11:15
Updated at 12/06/22 09:41
Clear
Name
Nabil Ad.
Login
nabil@strangebee.com
Email
nabil@strangebee.com
Type
Normal
Locked
MFA
No
API Key
Renew
Reveal
Revoke
Profile
org-admin
Permissions
accessTheHiveFS
manageAction
manageAlert
manageAnalyse
manageCase
manageCaseTemplate
manageComment
manageConfig
manageCustomEvent
manageKnowledgeBase
manageObservable
managePage
manageProcedure
manageShare
manageTag
manageTask
manageUser

Configuration parameters

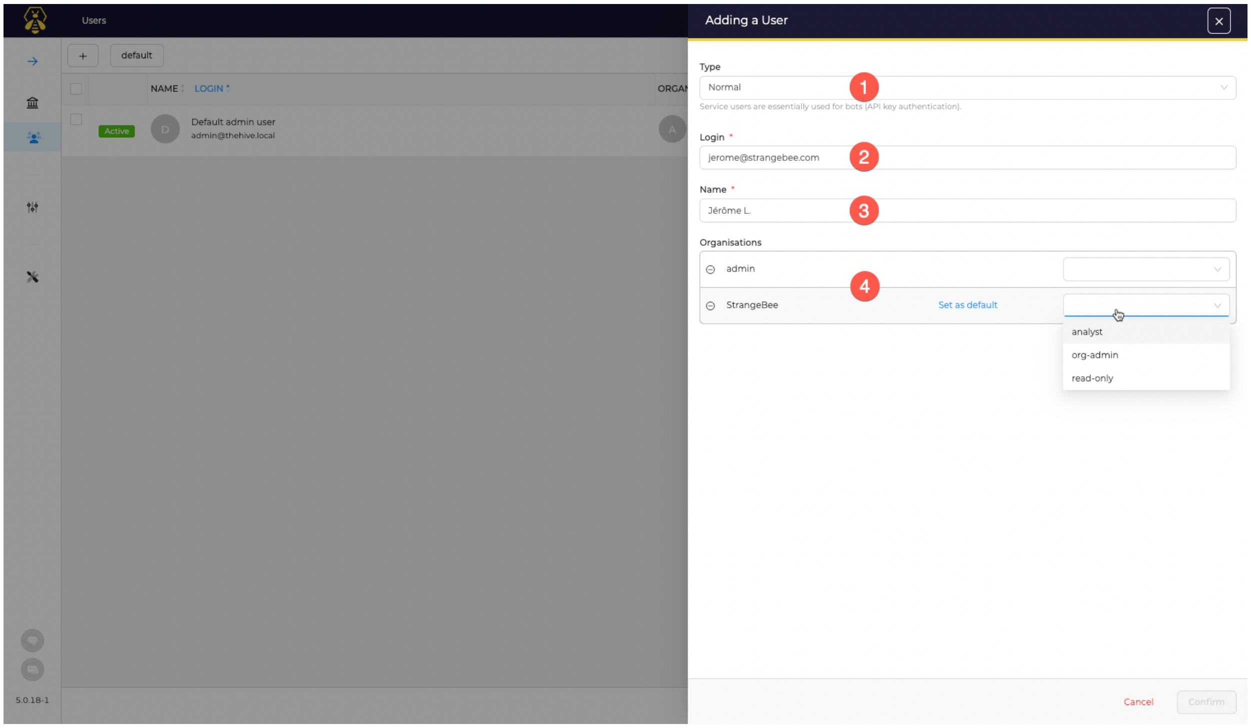
- Avatar : Up date the avatar associated with the user by drag and drop a new file (PNG or JPG files).
- Login : User login
- Email : email address for the account. This is used to send notifications or reset password links to users. Login is used if no email is filled there
- Type : Typ e of the account. 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 up date 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

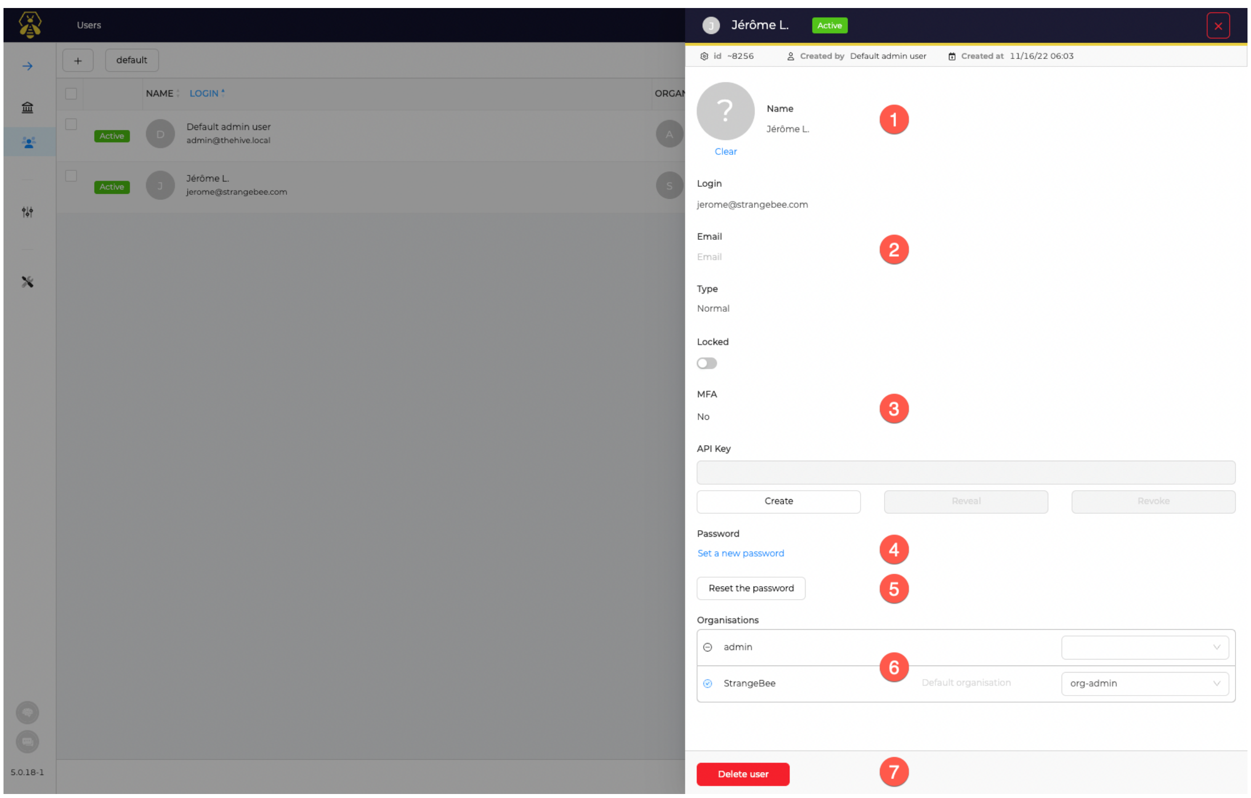
org-admin



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



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



5.1.2 Templates

- Case

List of Case Templates

Access

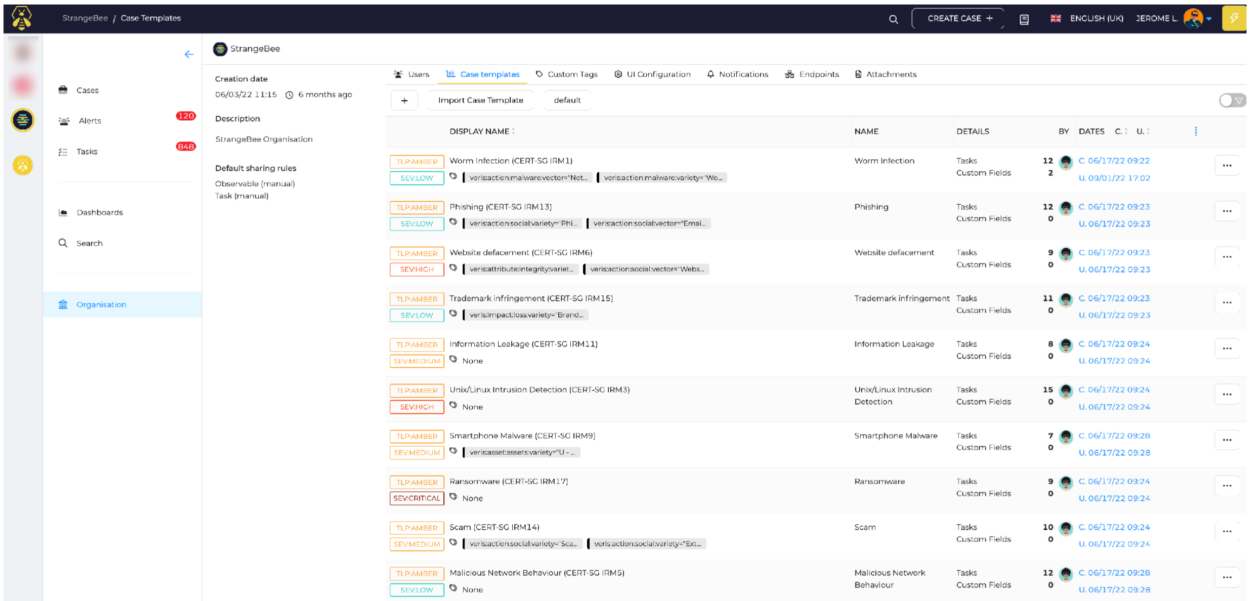


Figure 4: List of case templates

New Case template

Click the + button to create a new Case template.

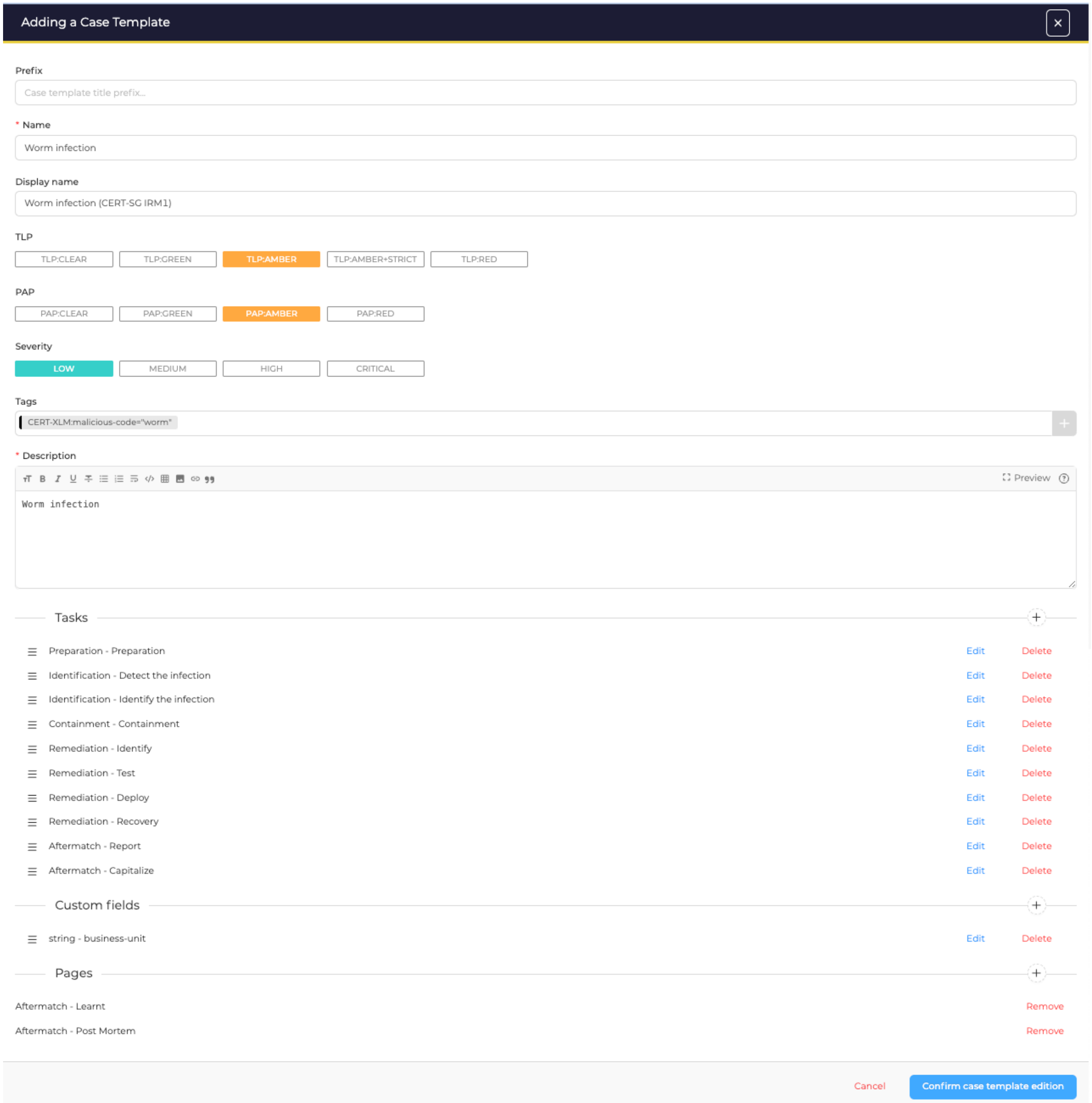


Figure 5: New case template

Configuration parameters

- **Prefix : String that will b e 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 o f 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 b e 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

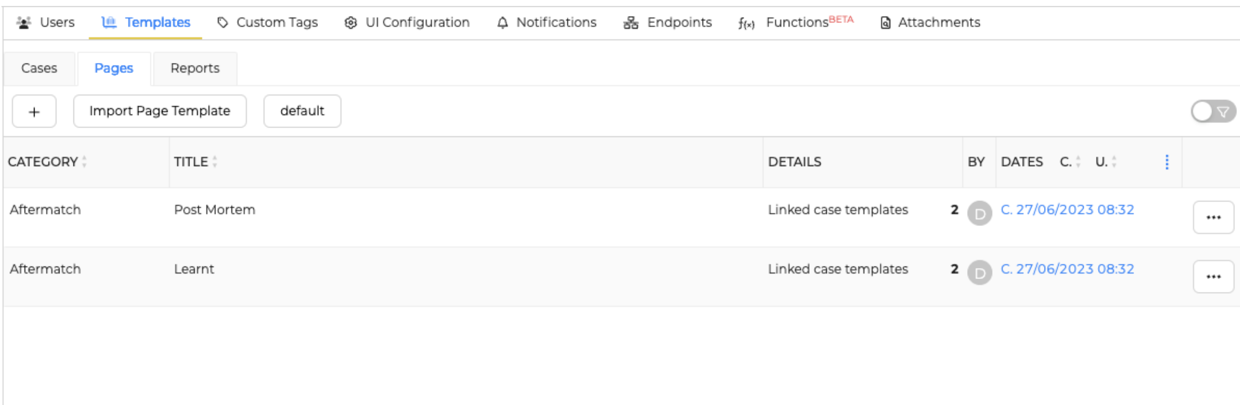


Figure 6: List of pages templates

New Case template

Click the + button to create a new Page template.

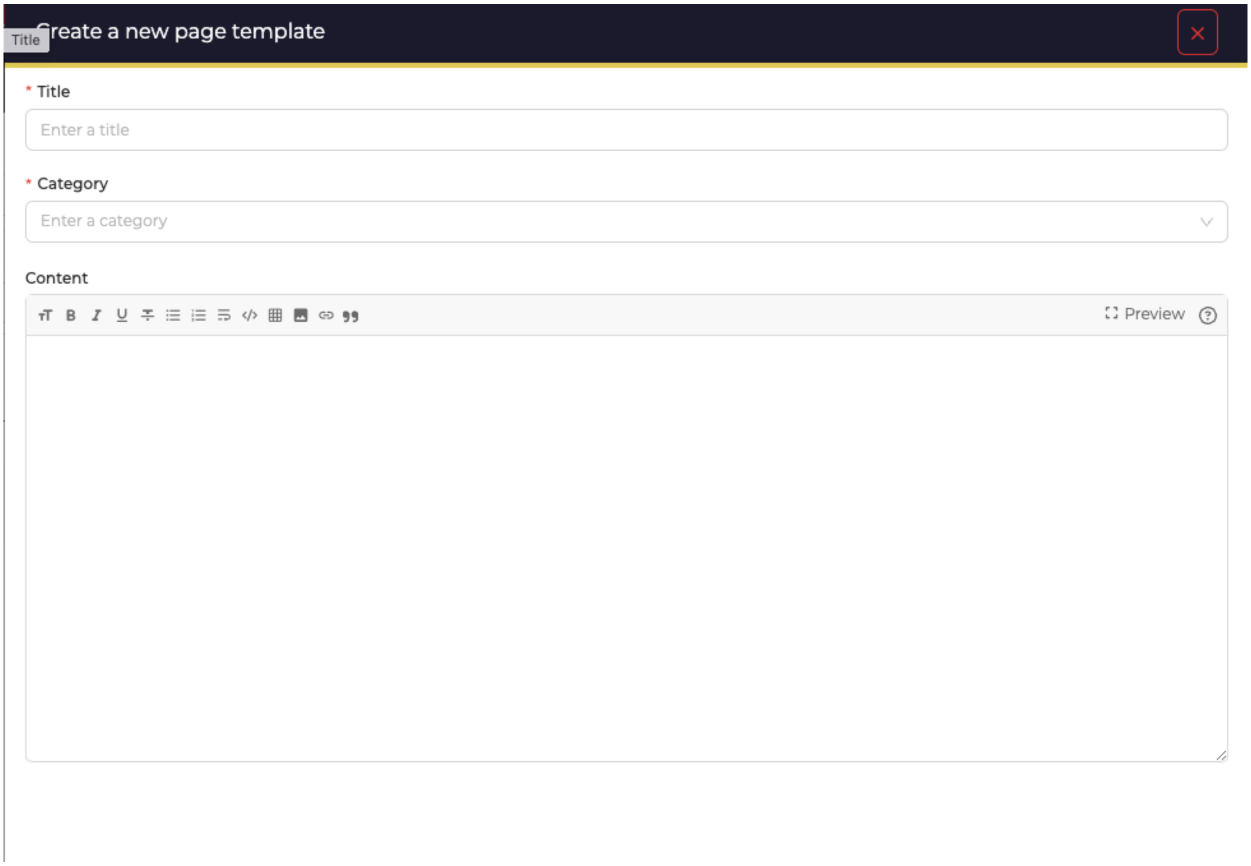


Figure 7: New P age template

Configuration parameters

- **Title : Page template title. Used to identify the Page template with the API. Al s o 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 conten t 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 T

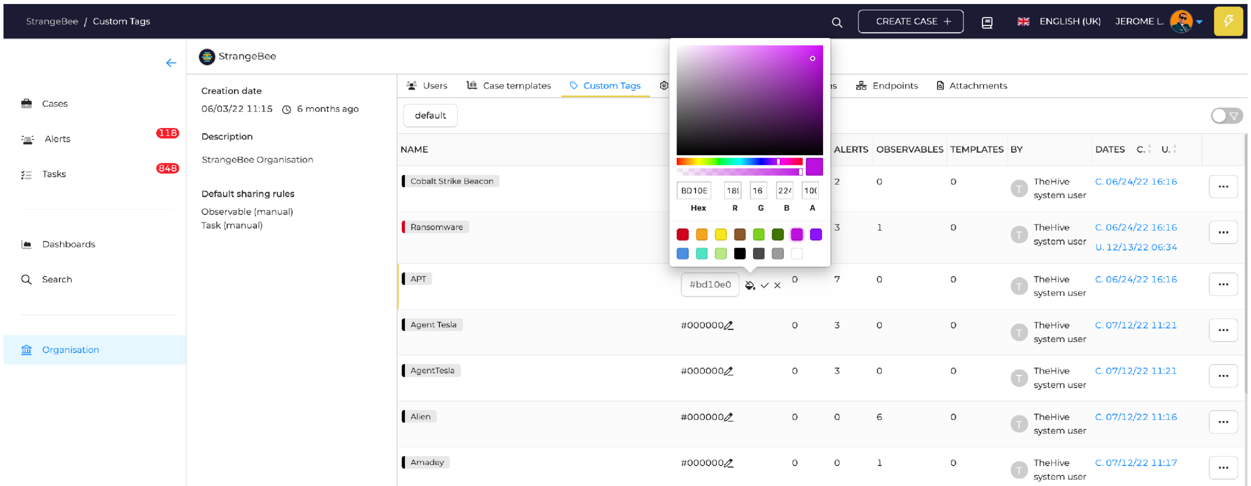


Figure 8: Custom tags

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 and 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

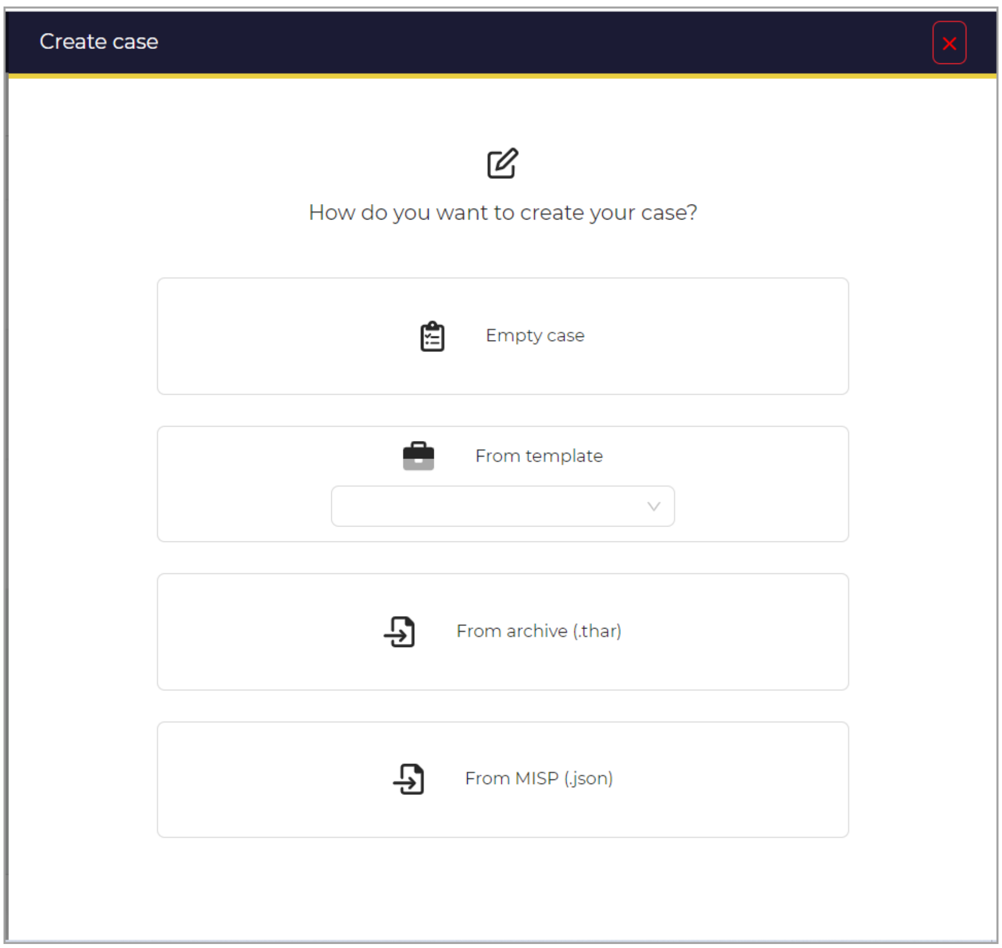


Figure 10: create case

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/Am b er/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).**
-

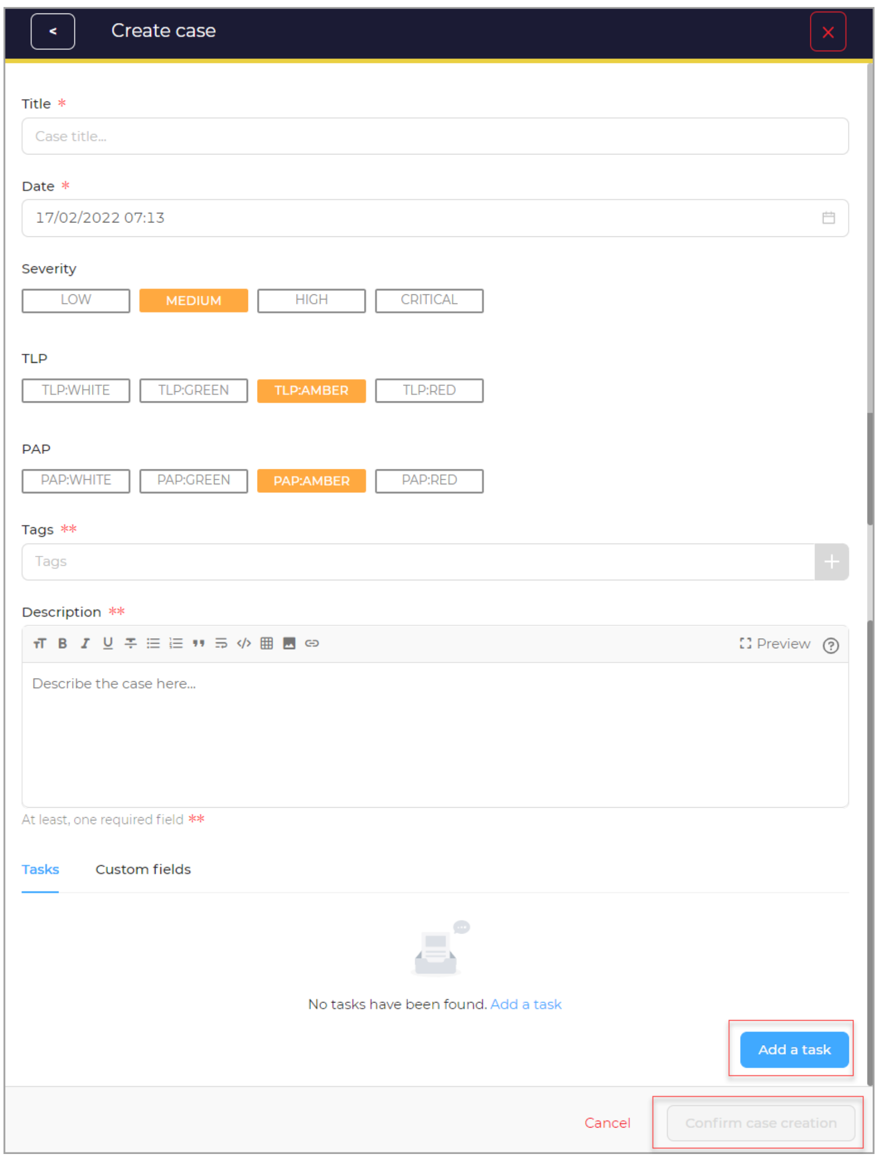


Figure 11: create empty case

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 T ask 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.)
-

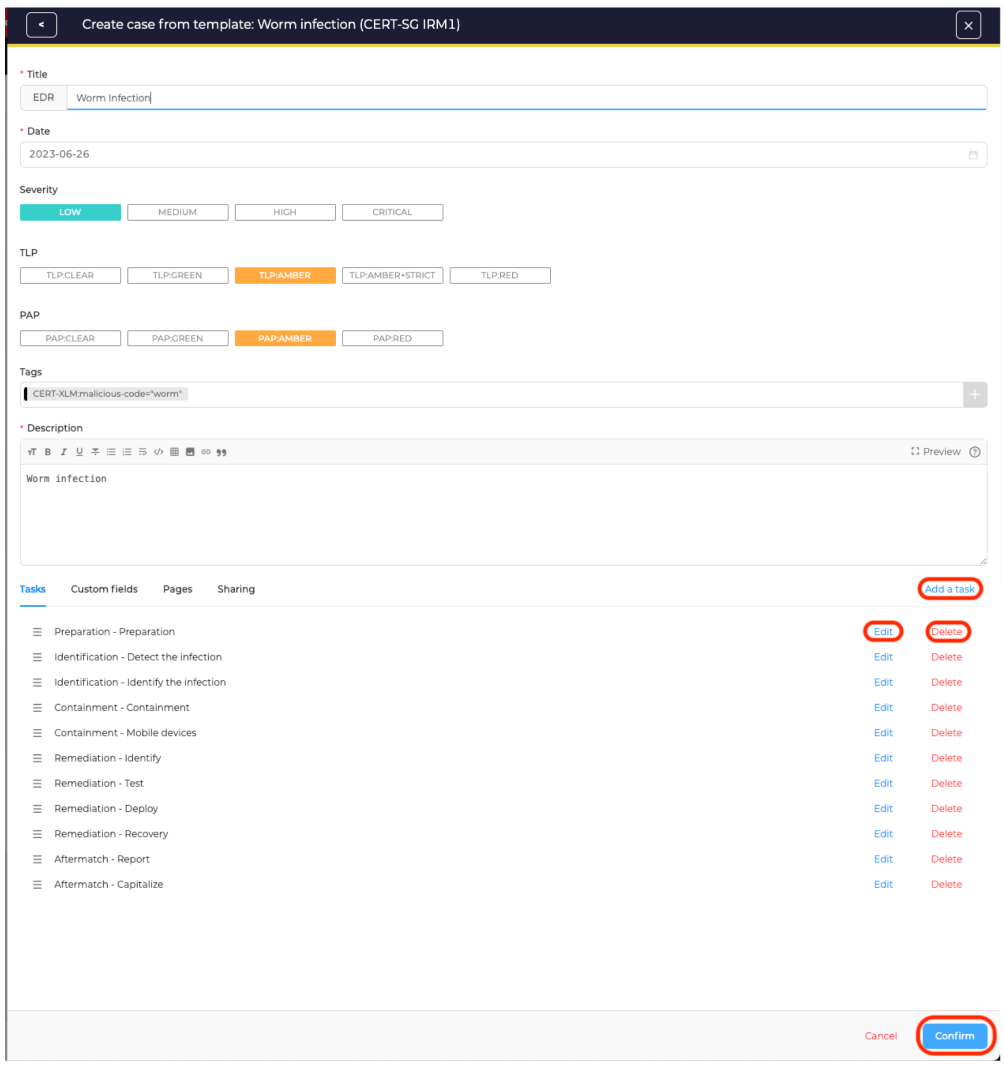


Figure 12: create case from template

- 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

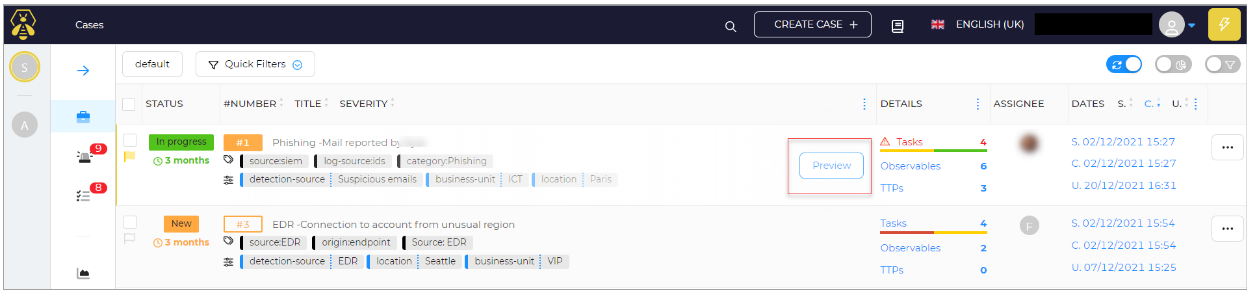
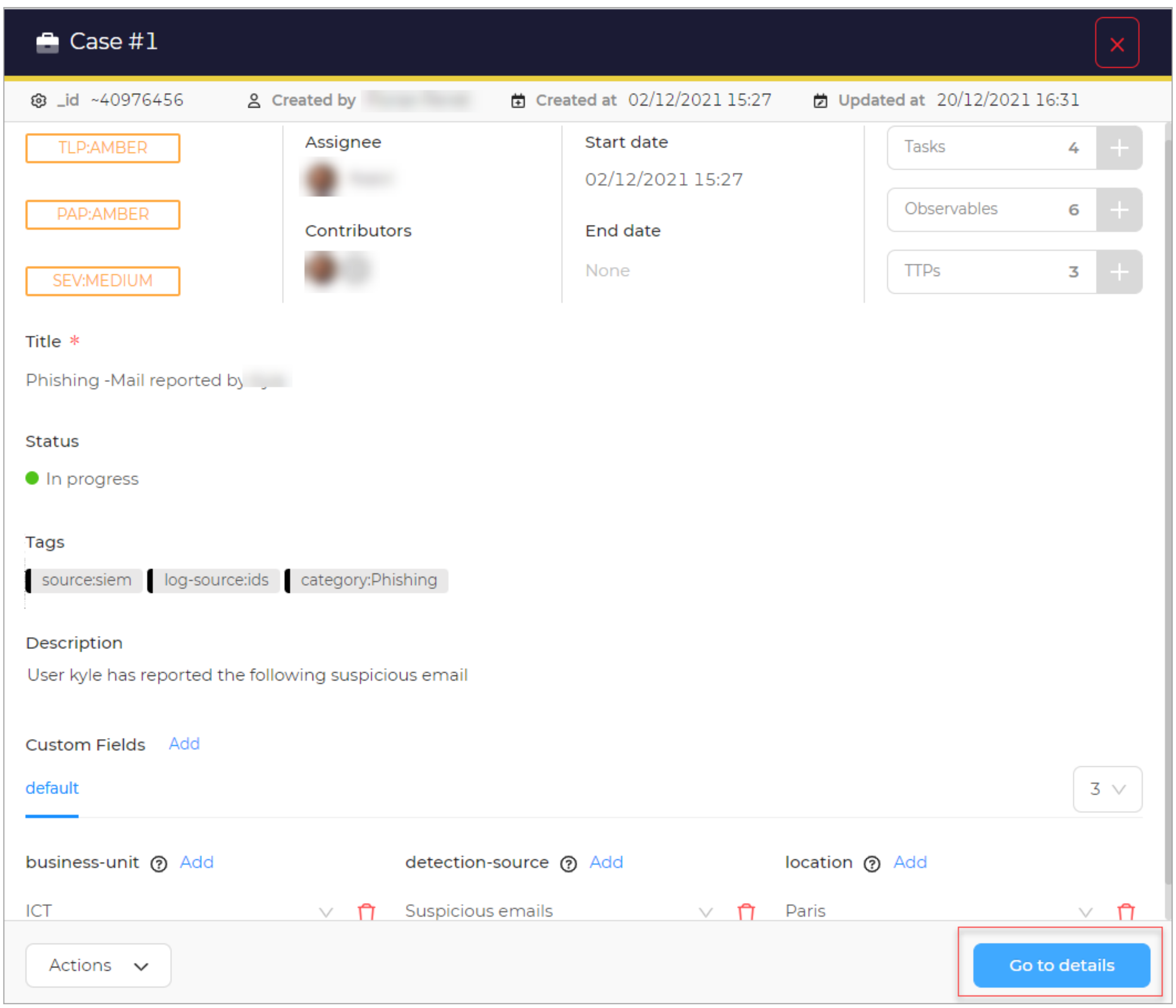


Figure 13: case list

The case details preview window opens.



- 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.**
-

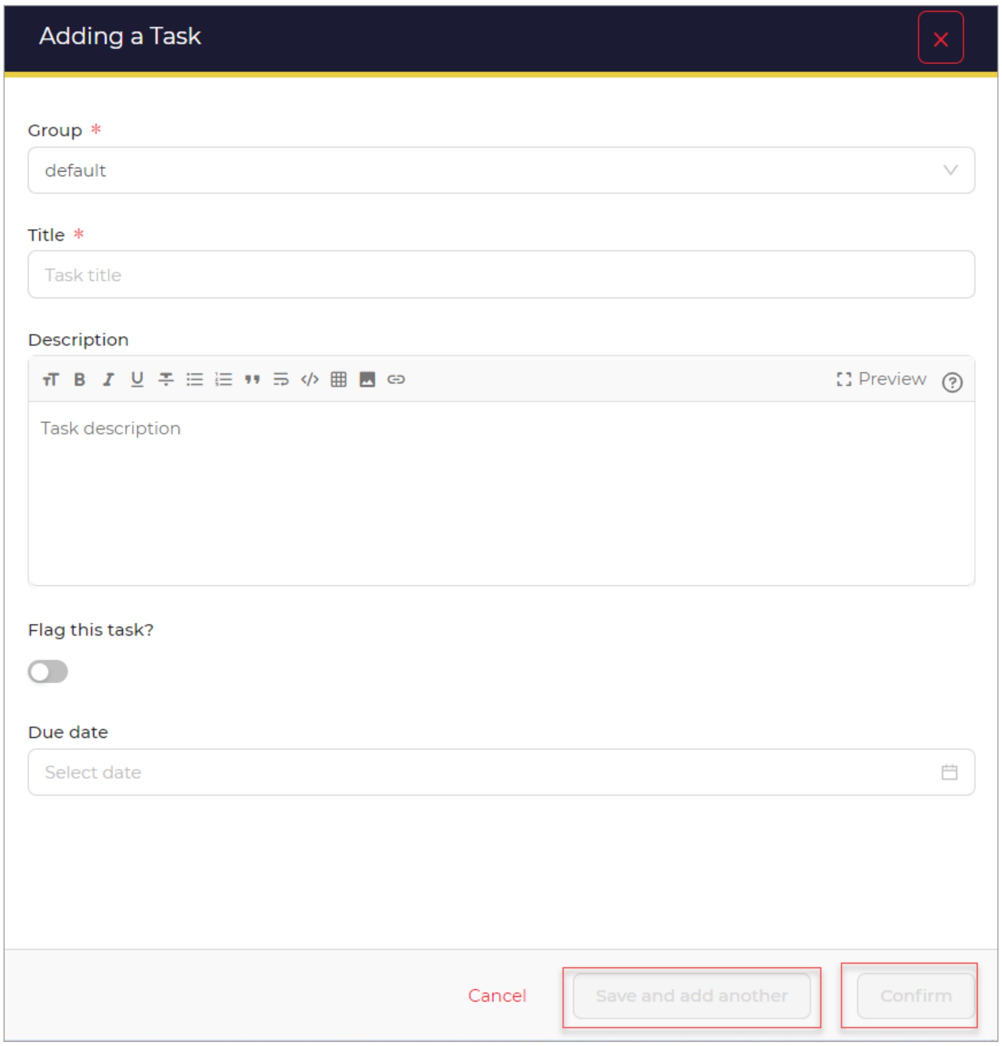


Figure 14: add a task

Add tags

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

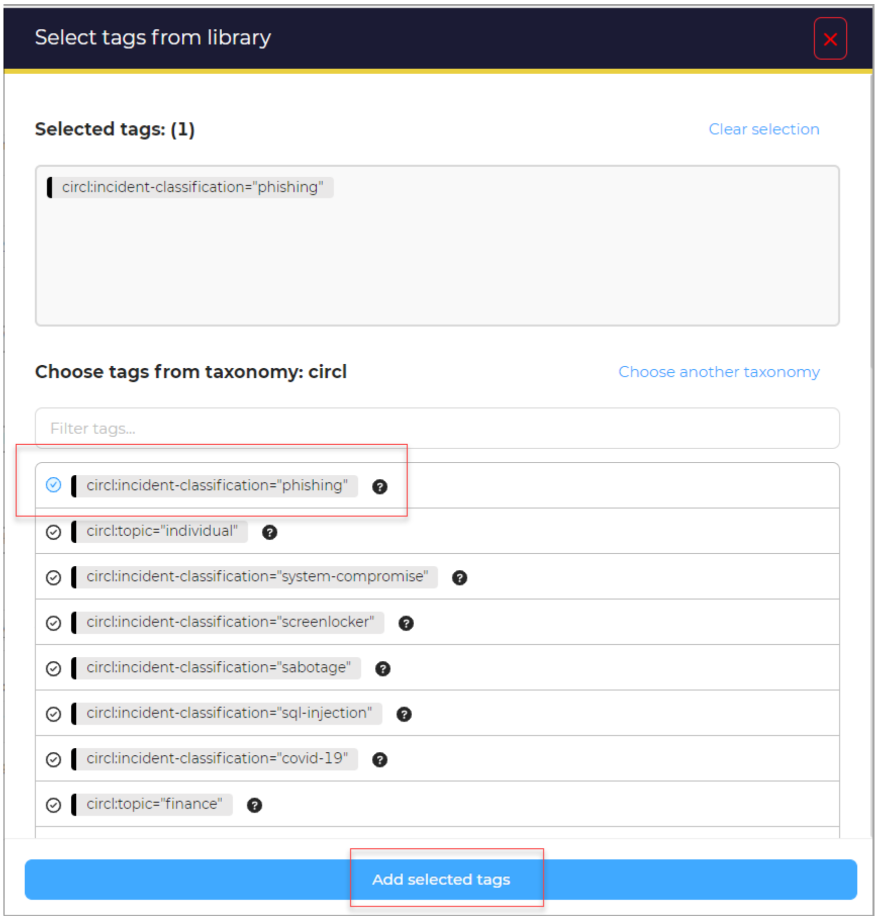


Figure 15: add tags

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.**

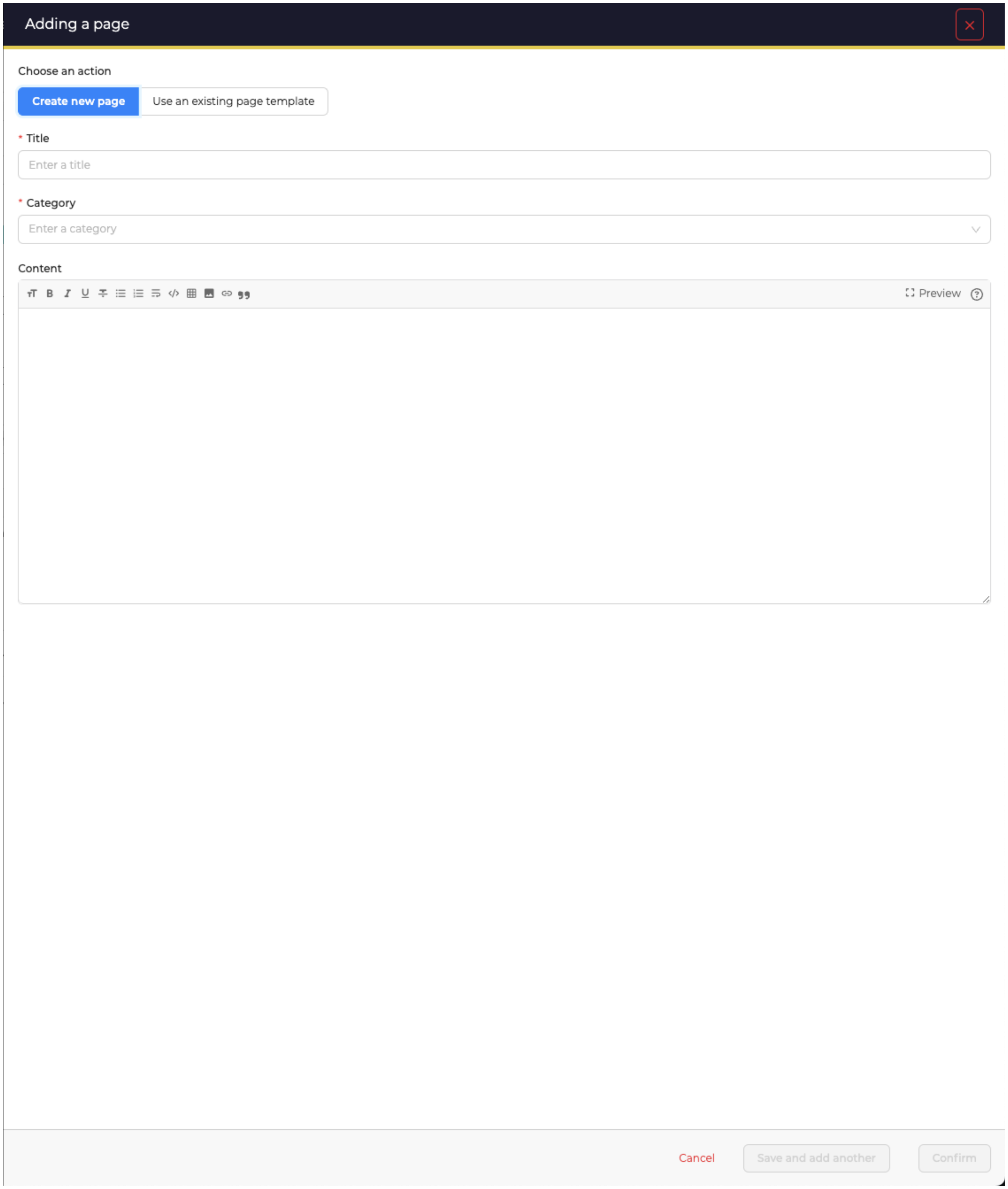


Figure 16: add a new page

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.

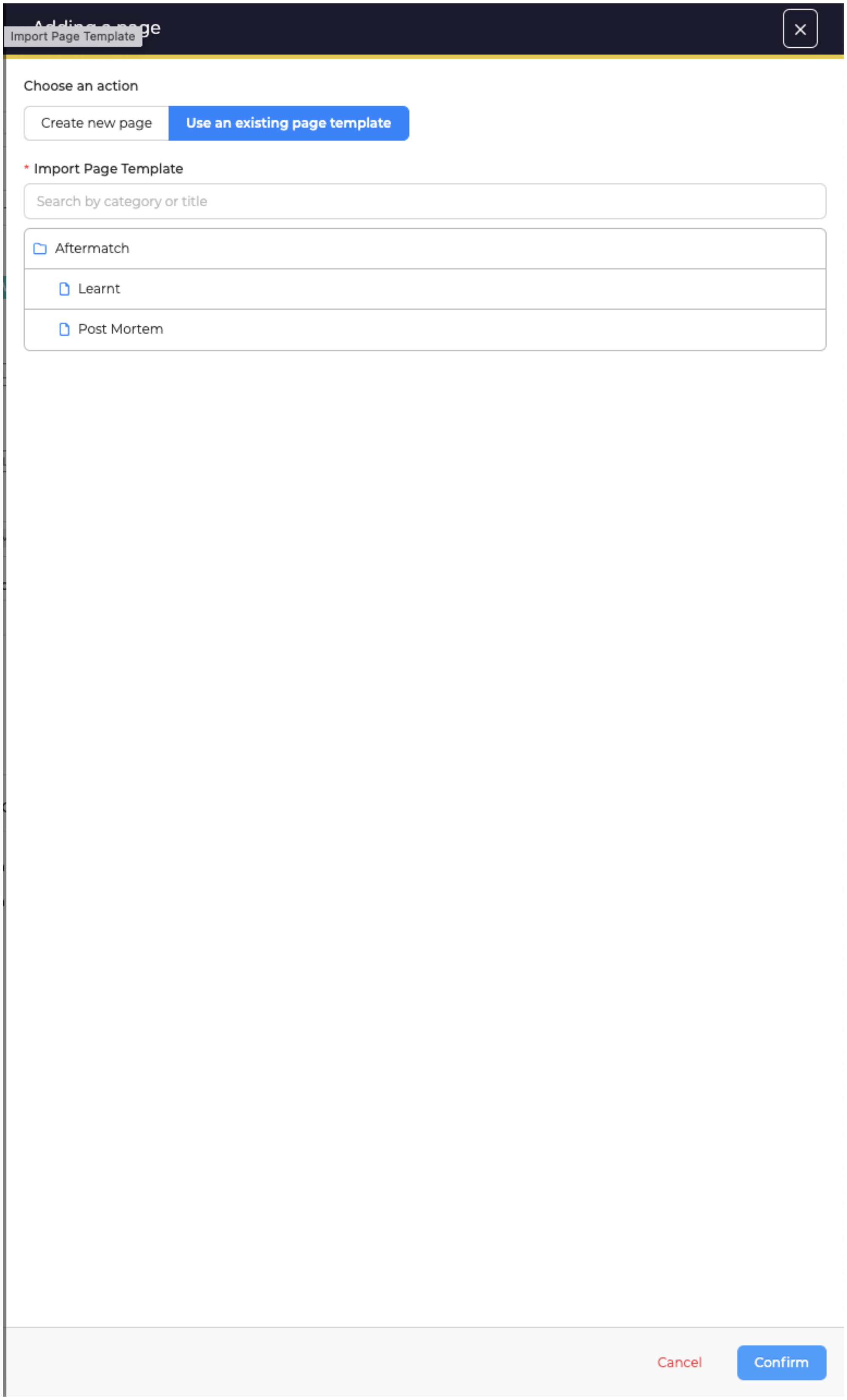


Figure 17: with an existing page

5.2.2 Tasks

- About

To view task details

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

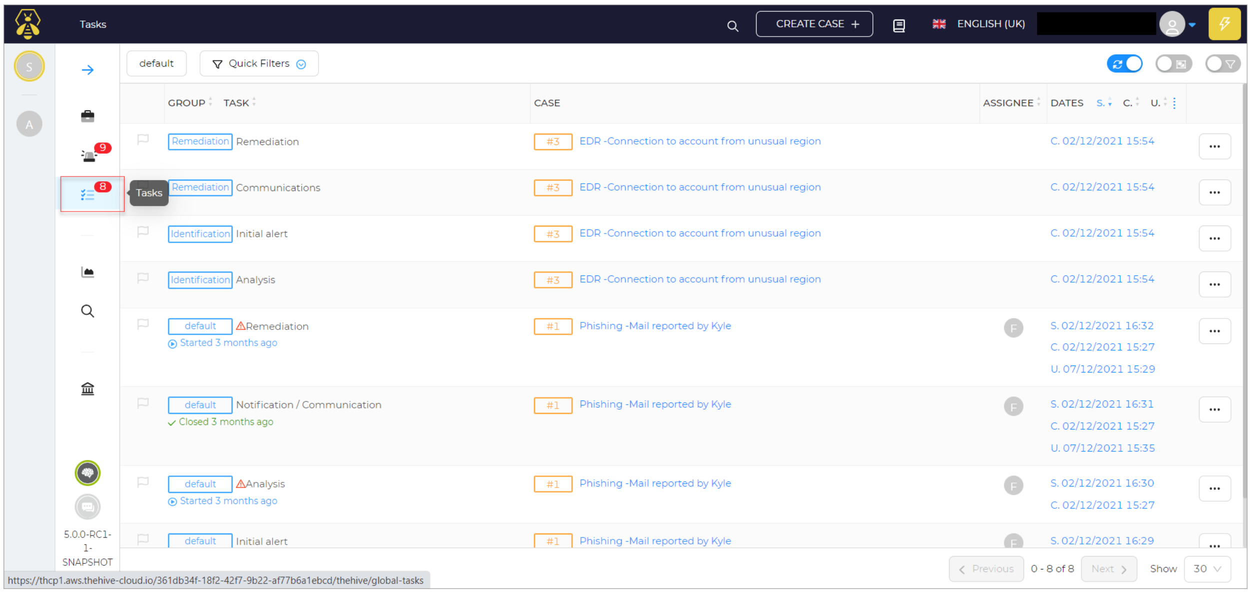
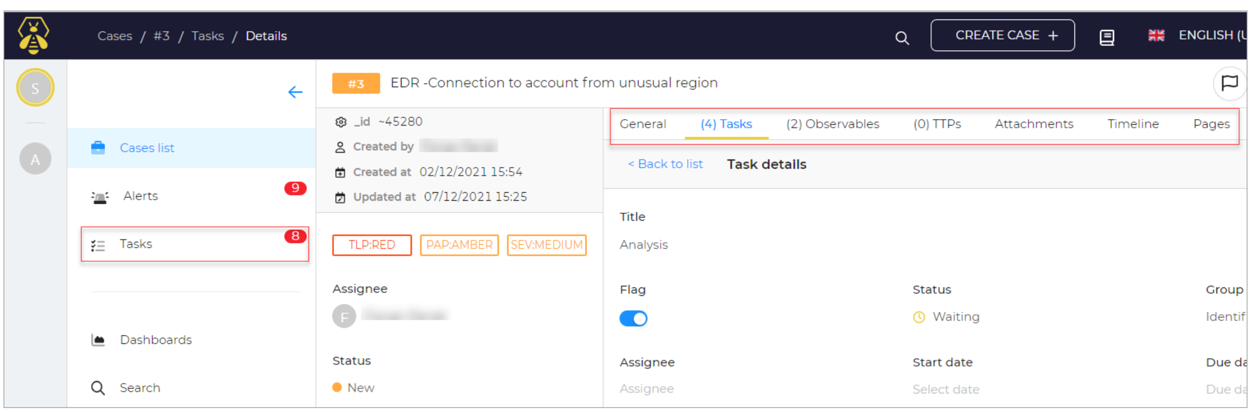


Figure 18: task list

The details:



- 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

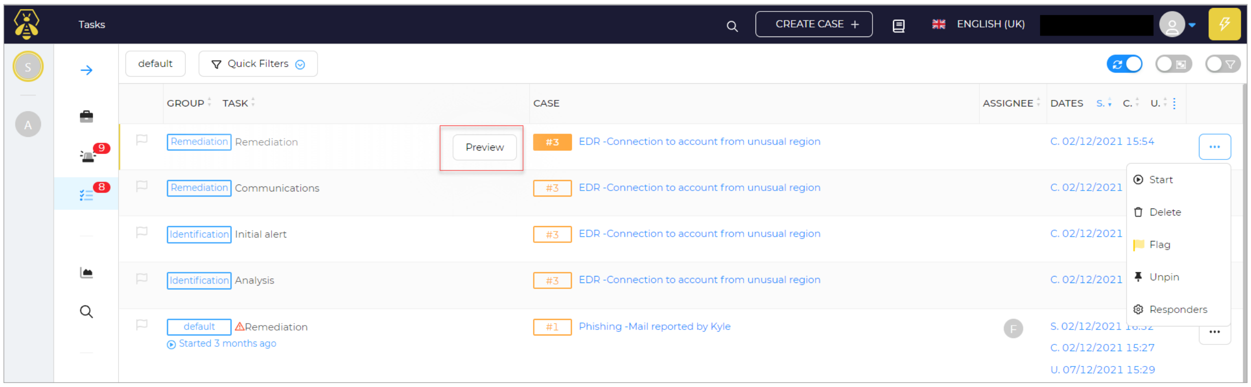
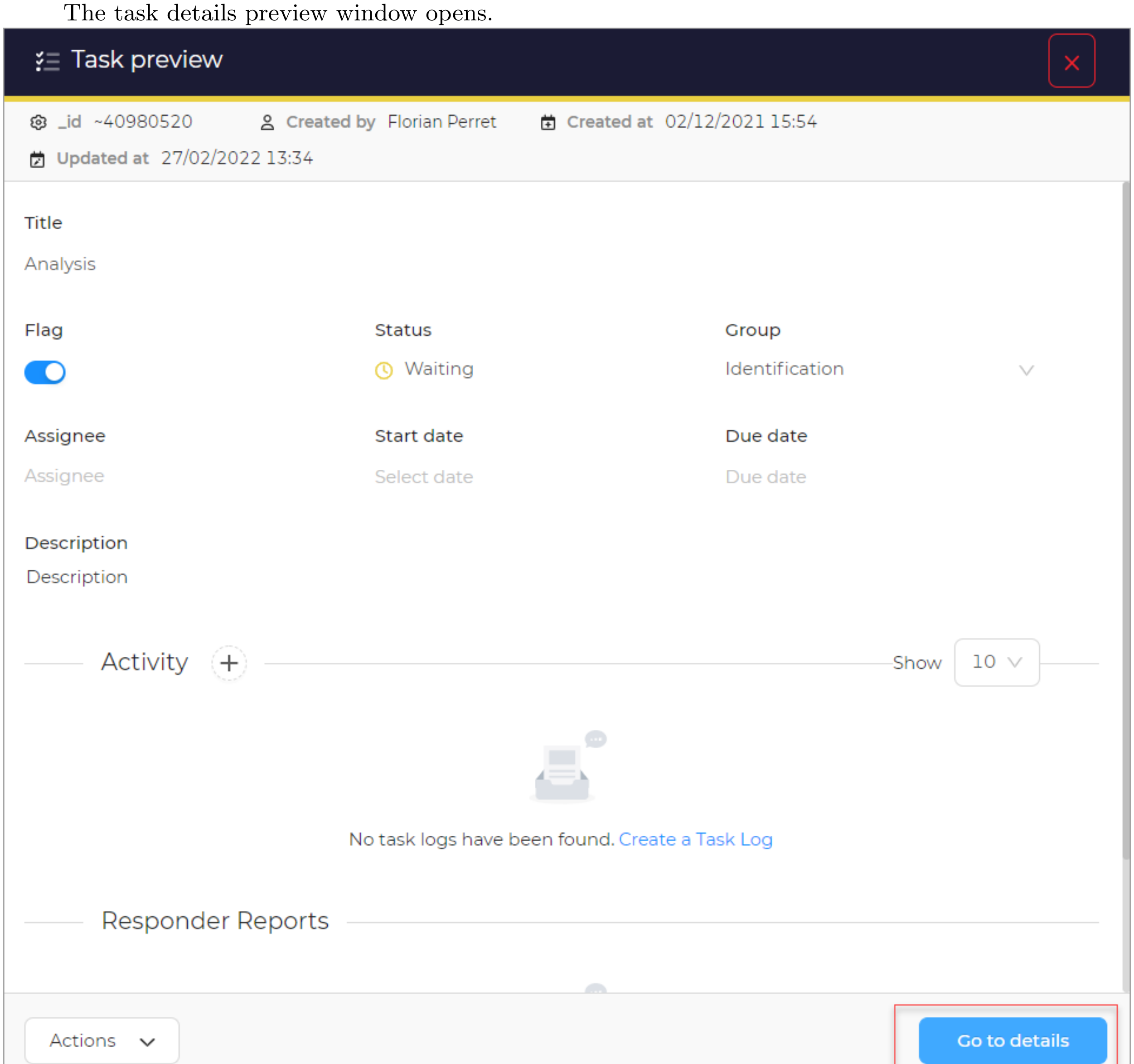


Figure 19: task list

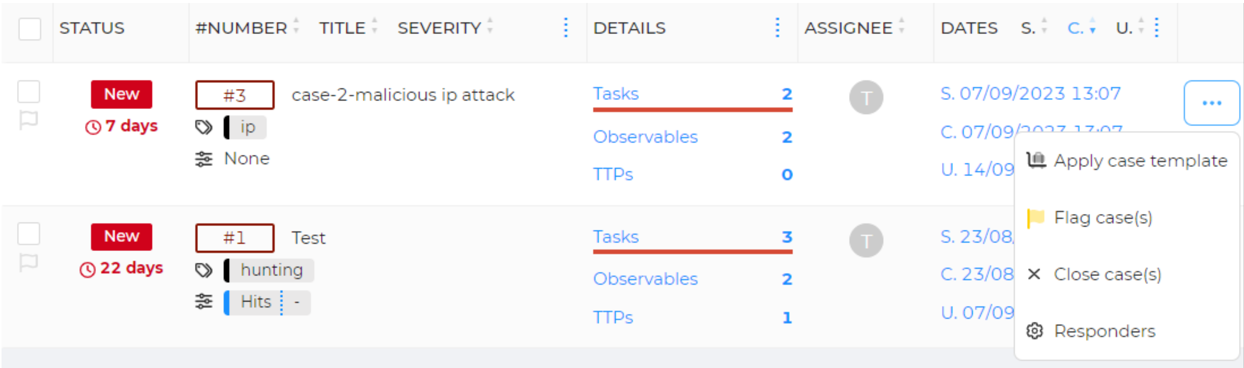
The task details preview window opens.



- Actions

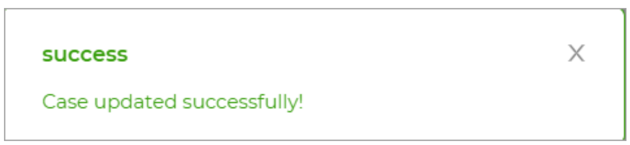
Actions

You can make use of any of the available actions



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.**

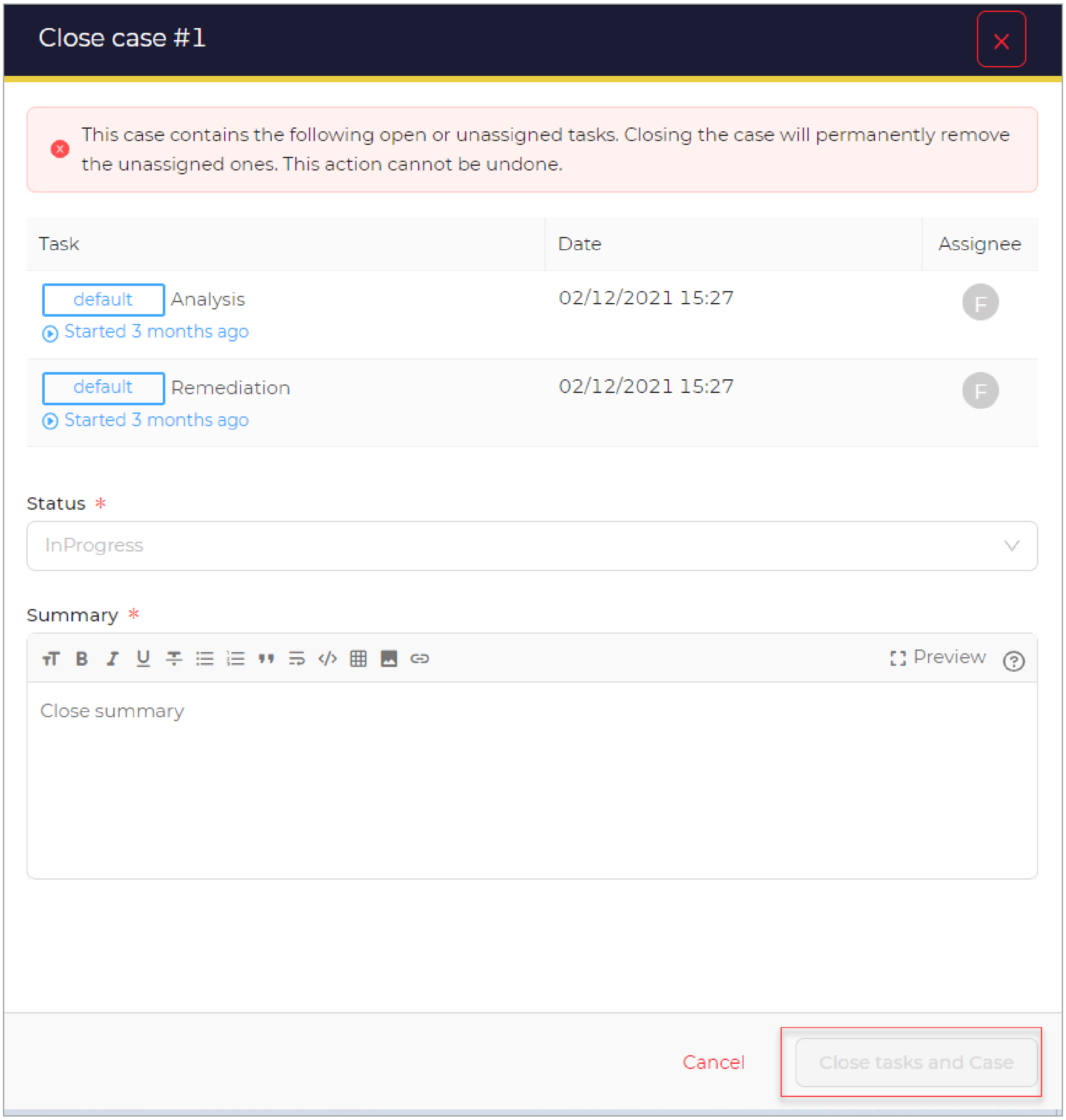


Figure 20: Closing a case

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:

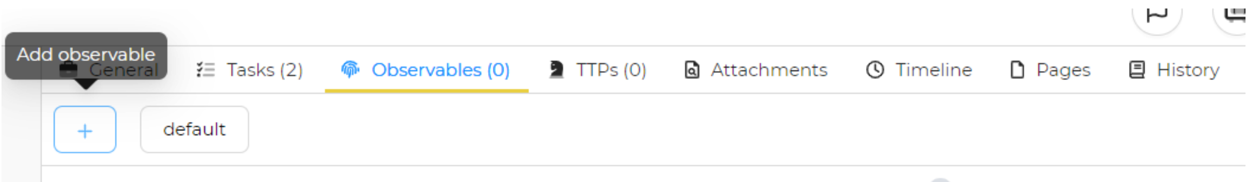


Figure 21: Adding obserables

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 p er 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 y our information system.
- Ignore for similarity: Do not correlate this observable with other similar observables.
- Tags **: Tag your observable with insightful information.
-

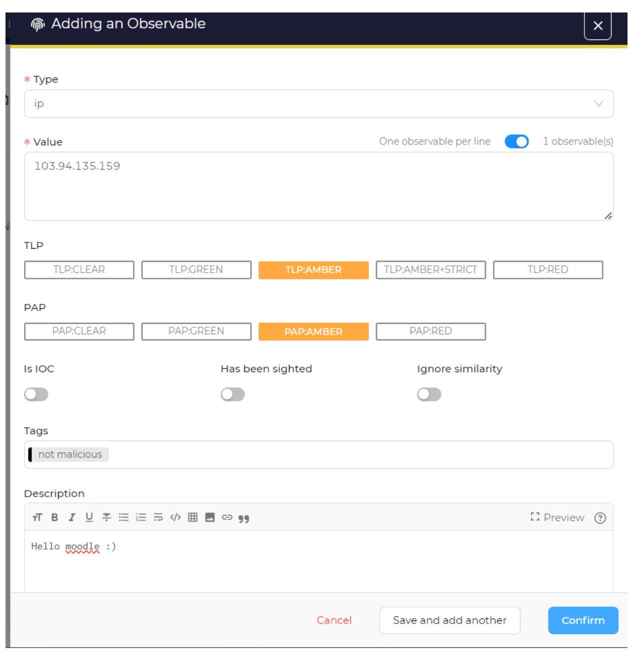


Figure 22: Creating observables

Finally , click on Create Observable(s)

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 ofiicial guide: https://docs.strangebee.com/thehive/setup/