



# The Hive Security Tool

Md. Sayeed Hasan Ovi Sanju Basak  
1805065 1805064

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

September 12, 2023

# Introduction

- **THE HIVE** is a Security Incident Response Platform.
- It is a collaborative platform for the security analysts (like github )
- This tool can be integrated with other security tools (such as **CORTEX** and **MISP**) to automate the process of analyzing the security incidents more accurately and efficiently.

## Purpose of using this Tool:

To detect any security incident quickly and analyze that incident in a collaborative platform to solve any security issue efficiently

# Introduction

- **THE HIVE** is a Security Incident Response Platform.
- It is a collaborative platform for the security analysts (like github )
- This tool can be integrated with other security tools (such as **CORTEX** and **MISP**) to automate the process of analyzing the security incidents more accurately and efficiently.

## Purpose of using this Tool:

To detect any security incident quickly and analyze that incident in a collaborative platform to solve any security issue efficiently

# Introduction

- **THE HIVE** is a Security Incident Response Platform.
- It is a collaborative platform for the security analysts (like github )
- This tool can be integrated with other security tools (such as **CORTEX** and **MISP**) to automate the process of analyzing the security incidents more accurately and efficiently.

## Purpose of using this Tool:

To detect any security incident quickly and analyze that incident in a collaborative platform to solve any security issue efficiently

# Introduction

- **THE HIVE** is a Security Incident Response Platform.
- It is a collaborative platform for the security analysts (like github )
- This tool can be integrated with other security tools (such as **CORTEX** and **MISP**) to automate the process of analyzing the security incidents more accurately and efficiently.

## Purpose of using this Tool:

To detect any security incident quickly and analyze that incident in a collaborative platform to solve any security issue efficiently

# Key concepts

- **Type of users** : Admin and user
- **Organization** : Admin can create an organization and create users .In an organization there are multiple users who deal with a particular type of security incident
- **Case** : A user of an organization can create a case for a particular incident
- **Task** : For each case there can be one or more task to solve that particular incident .each task can assigned to one or more user(like github issue)

# Key concepts

- **Type of users** : Admin and user
- **Organization** : Admin can create an organization and create users .In an organization there are multiple users who deal with a particular type of security incident
- **Case** : A user of an organization can create a case for a particular incident
- **Task** : For each case there can be one or more task to solve that particular incident .each task can assigned to one or more user(like github issue)

# Key concepts

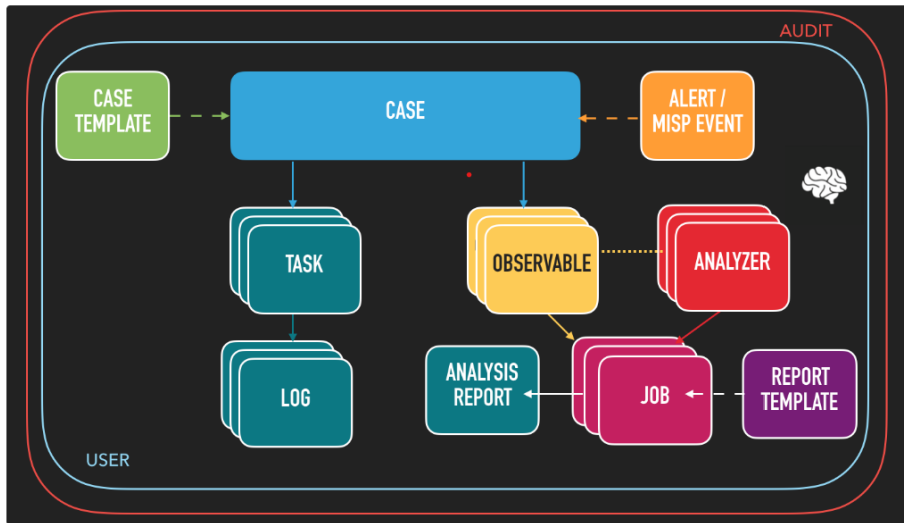
- **Type of users** : Admin and user
- **Organization** : Admin can create an organization and create users .In an organization there are multiple users who deal with a particular type of security incident
- **Case** : A user of an organization can create a case for a particular incident
- **Task** : For each case there can be one or more task to solve that particular incident .each task can assigned to one or more user(like github issue)



# Key concepts

- **Type of users** : Admin and user
- **Organization** : Admin can create an organization and create users .In an organization there are multiple users who deal with a particular type of security incident
- **Case** : A user of an organization can create a case for a particular incident
- **Task** : For each case there can be one or more task to solve that particular incident .each task can assigned to one or more user(like github issue)

# General Workflow of TheHive



# Two key Features

- Creating organizations, and assigning tasks to users
- Using observables to analyze and respond to security incidents

# Two key Features

- Creating organizations, and assigning tasks to users
- Using observables to analyze and respond to security incidents

# Demonstration of feature One

## Creating organizations and assigning tasks to users

The screenshot displays the 'Organisation List' interface in The Hive Security Tool. The main panel shows a list of organizations with columns for selection, name, status, and linked organizations. Two organizations are listed: 'admin' and 'demo', both with an 'Active' status and 'None' linked organizations. A sidebar on the left contains navigation icons for home, users, and other functions. A top navigation bar includes a '+', 'default', and 'Export list' button. A secondary panel on the right shows the 'demo' organization details, including creation date (13/07/2023 12:55), description ('demo organisation'), task sharing rule ('manual'), and observables sharing rule ('manual'). Below this, the 'Users' section lists two users: 'thehive' (th@hive.local) with role 'org-admin' and 'user one' (user1@thehive.local) with role 'analyst'.

	NAME	Active	Linked organisations
<input type="checkbox"/>	admin	Active	None
<input type="checkbox"/>	demo	Active	None

	Users	Linked organisations
<input type="checkbox"/>	thehive th@hive.local	org-admin
<input type="checkbox"/>	user one user1@thehive.local	analyst

# Observables

- Observables are pieces of information related to a security incident.
- Observables can be added to cases in TheHive.
- Observables can be analyzed using Cortex.
- Observables have different types, such as url, mail subject, or registry key.
- Here the user (security analysts) will report their analysis.(e.g. IP address , hash of malicious files )

# Observables

- Observables are pieces of information related to a security incident.
- Observables can be added to cases in TheHive.
- Observables can be analyzed using Cortex.
- Observables have different types, such as url, mail subject, or registry key.
- Here the user (security analysts) will report their analysis.(e.g. IP address , hash of malicious files )

# Observables

- Observables are pieces of information related to a security incident.
- Observables can be added to cases in TheHive.
- Observables can be analyzed using Cortex.
- Observables have different types, such as url, mail subject, or registry key.
- Here the user (security analysts) will report their analysis.(e.g. IP address , hash of malicious files )



# Observables

- Observables are pieces of information related to a security incident.
- Observables can be added to cases in TheHive.
- Observables can be analyzed using Cortex.
- Observables have different types, such as url, mail subject, or registry key.
- Here the user (security analysts) will report their analysis.(e.g. IP address , hash of malicious files )

# Observables

- Observables are pieces of information related to a security incident.
- Observables can be added to cases in TheHive.
- Observables can be analyzed using Cortex.
- Observables have different types, such as url, mail subject, or registry key.
- Here the user (security analysts) will report their analysis.(e.g. IP address , hash of malicious files )