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 assingned 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 assingned to one or more user(like github issue)

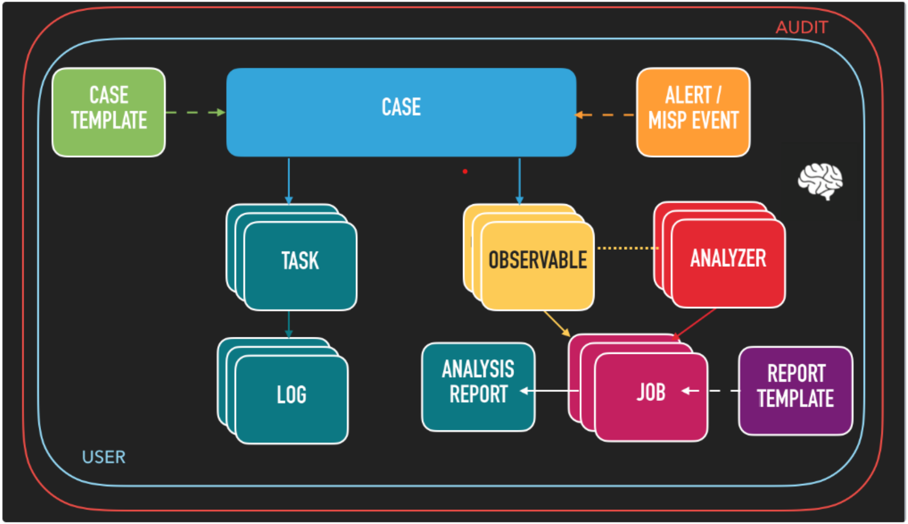
Key concepts

- **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 assingned 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 assingned to one or more user(like github issue)

General Workflow of TheHive



Two key Features

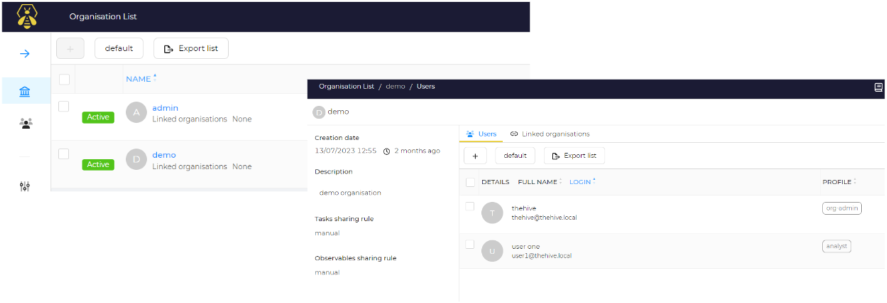
- Creating organizations, and assigning tasks to users
- Using observables to analyze and respond to security incidents

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



	NAME
Active	admin Linked organisations None
Active	demo Linked organisations None

demo

Creation date

13/07/2023 12:55 2 months ago

Description

demo organisation

Tasks sharing rule

manual

Observables sharing rule

manual

DETAILS	FULL NAME	LOGIN	PROFILE
T	thehive	thehive@thehive.local	org-admin
U	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)