

The Hive Security Tool

Sumaiya Seaha, 1905033

Fariha Zaman Aurin, 1905049

Debjany Ghosh Aronno, 1905053

Department of CSE

Bangladesh University of Engineering & Technology

March 6, 2024

Table of contents

- 1 Introduction
- 2 Architecture
- 3 Key Concepts
- 4 Workflow
- 5 Core Features
- 6 Demonstration

Table of contents

- 1 Introduction
- 2 Architecture
- 3 Key Concepts
- 4 Workflow
- 5 Core Features
- 6 Demonstration

Unveiling TheHive: Your Security Ally

- Welcome to THE HIVE – Your Security Incident Response Wing!
- Just like GitHub brings developers together, TheHive unites security analysts in a collaborative heaven.
- Picture this: THE HIVE seamlessly integrates with powerhouse tools like CORTEX and MISP, automating the analysis of security incidents with unmatched precision and efficiency.

Why TheHive?

Rapid Detection, Collective Analysis: Swiftly identify and collaboratively dissect security incidents, ensuring efficient resolution of any security challenge.

Unveiling TheHive: Your Security Ally

- Welcome to THE HIVE – Your Security Incident Response Wing!
- Just like GitHub brings developers together, TheHive unites security analysts in a collaborative heaven.
- Picture this: THE HIVE seamlessly integrates with powerhouse tools like CORTEX and MISP, automating the analysis of security incidents with unmatched precision and efficiency.

Why TheHive?

Rapid Detection, Collective Analysis: Swiftly identify and collaboratively dissect security incidents, ensuring efficient resolution of any security challenge.

Unveiling TheHive: Your Security Ally

- Welcome to THE HIVE – Your Security Incident Response Wing!
- Just like GitHub brings developers together, TheHive unites security analysts in a collaborative heaven.
- Picture this: **THE HIVE** seamlessly integrates with powerhouse tools like **CORTEX** and **MISP**, automating the analysis of security incidents with unmatched precision and efficiency.

Why TheHive?

Rapid Detection, Collective Analysis: Swiftly identify and collaboratively dissect security incidents, ensuring efficient resolution of any security challenge.

Unveiling TheHive: Your Security Ally

- Welcome to THE HIVE – Your Security Incident Response Wing!
- Just like GitHub brings developers together, TheHive unites security analysts in a collaborative heaven.
- Picture this: **THE HIVE** seamlessly integrates with powerhouse tools like **CORTEX** and **MISP**, automating the analysis of security incidents with unmatched precision and efficiency.

Why TheHive?

Rapid Detection, Collective Analysis: Swiftly identify and collaboratively dissect security incidents, ensuring efficient resolution of any security challenge.

Table of contents

- 1 Introduction
- 2 Architecture**
- 3 Key Concepts
- 4 Workflow
- 5 Core Features
- 6 Demonstration

TheHive's Architecture Overview

1. Frontend

- User interface where analysts interact.
- Developed using AngularJS and Bootstrap.
- Control panel for managing cases, tasks, and observables.

2. Backend

- Core logic and heavy lifting.
- Implemented in Scala, Akka, Play Framework, and Slick.
- Ensures smooth processing of data and communication with the frontend.

TheHive's Architecture Overview

1. Frontend

- User interface where analysts interact.
- Developed using AngularJS and Bootstrap.
- Control panel for managing cases, tasks, and observables.

2. Backend

- Core logic and heavy lifting.
- Implemented in Scala, Akka, Play Framework, and Slick.
- Ensures smooth processing of data and communication with the frontend.

TheHive's Architecture Overview Contd.

3. Cortex

- Real-time analytics platform.
- Enhances intelligence with Scala, Akka, Play Framework, and Python.
- Analyzes data from the backend, adding an extra layer of insight.

4. Storage

- Essential memory bank for TheHive.
- Utilizes Elasticsearch, a distributed database.
- Stores all data securely for efficient retrieval.

Overview

Cortex is an integral component that enhances the capabilities of TheHive by providing real-time analytics and active response capabilities. It is used to process data from the backend, analyze observables, and perform actions on those observables, such as blocking an IP address or quarantining a file.

TheHive's Architecture Overview Contd.

3. Cortex

- Real-time analytics platform.
- Enhances intelligence with Scala, Akka, Play Framework, and Python.
- Analyzes data from the backend, adding an extra layer of insight.

4. Storage

- Essential memory bank for TheHive.
- Utilizes Elasticsearch, a distributed database.
- Stores all data securely for efficient retrieval.

Overview

Cortex is an integral component that enhances the capabilities of TheHive by providing real-time analytics and active response capabilities. It is used to process data from the backend, analyze observables, and perform actions on those observables, such as blocking an IP address or quarantining a file.

TheHive's Architecture Overview Contd.

3. Cortex

- Real-time analytics platform.
- Enhances intelligence with Scala, Akka, Play Framework, and Python.
- Analyzes data from the backend, adding an extra layer of insight.

4. Storage

- Essential memory bank for TheHive.
- Utilizes Elasticsearch, a distributed database.
- Stores all data securely for efficient retrieval.

Overview

Cortex is an integral component that enhances the capabilities of TheHive by providing real-time analytics and active response capabilities. It is used to process data from the backend, analyze observables, and perform actions on those observables, such as blocking an IP address or quarantining a file.

TheHive's Architecture - Continued

How It Works

The frontend serves as the user's window into TheHive, allowing for seamless interaction with cases and tasks. The backend, powered by Scala and Akka, processes the user's commands and orchestrates the entire operation.

Cortex, the analytical powerhouse, brings real-time insights to the table, using a combination of Scala, Akka, Play Framework, and Python. It acts like a smart assistant, enriching the analysis process.

The storage layer, backed by Elasticsearch, ensures that every piece of data is securely stored and easily retrievable. Think of it as TheHive's reliable memory bank, storing information for future reference.

TheHive's Architecture - Continued

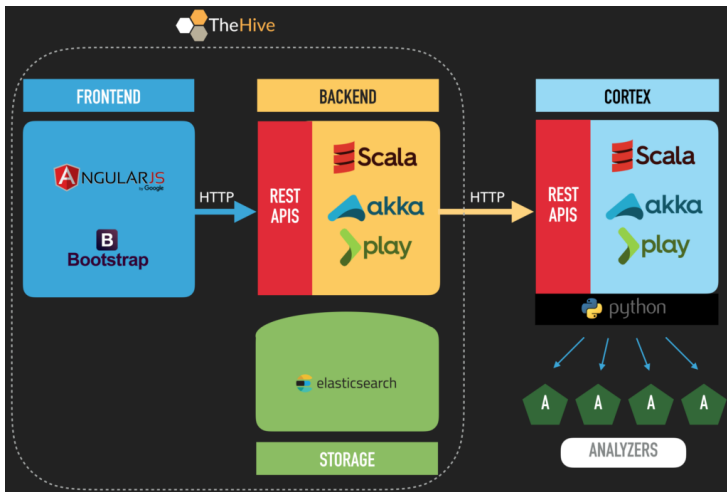


Figure: Overview of TheHive's Architecture

Table of contents

- 1 Introduction
- 2 Architecture
- 3 Key Concepts**
- 4 Workflow
- 5 Core Features
- 6 Demonstration

Key Concepts in TheHive

- **User:** TheHive supports two main user types – **Admin** and **User**.
- **Organization:** Admins can create organizations and manage users within them. Organizations group multiple users who collaborate on specific types of security incidents.
- **Case:** Users within an organization can create cases to document and manage incidents. Each case represents a specific security incident.
- **Task:** For each case, there can be one or more tasks aimed at resolving the incident. Tasks are similar to issues on platforms like GitHub and can be assigned to one or more users.

Key Concepts in TheHive

- **User:** TheHive supports two main user types – **Admin** and **User**.
- **Organization:** Admins can create organizations and manage users within them. Organizations group multiple users who collaborate on specific types of security incidents.
- **Case:** Users within an organization can create cases to document and manage incidents. Each case represents a specific security incident.
- **Task:** For each case, there can be one or more tasks aimed at resolving the incident. Tasks are similar to issues on platforms like GitHub and can be assigned to one or more users.

Key Concepts in TheHive

- **User:** TheHive supports two main user types – **Admin** and **User**.
- **Organization:** Admins can create organizations and manage users within them. Organizations group multiple users who collaborate on specific types of security incidents.
- **Case:** Users within an organization can create cases to document and manage incidents. Each case represents a specific security incident.
- **Task:** For each case, there can be one or more tasks aimed at resolving the incident. Tasks are similar to issues on platforms like GitHub and can be assigned to one or more users.

Key Concepts in TheHive

- **User:** TheHive supports two main user types – **Admin** and **User**.
- **Organization:** Admins can create organizations and manage users within them. Organizations group multiple users who collaborate on specific types of security incidents.
- **Case:** Users within an organization can create cases to document and manage incidents. Each case represents a specific security incident.
- **Task:** For each case, there can be one or more tasks aimed at resolving the incident. Tasks are similar to issues on platforms like GitHub and can be assigned to one or more users.

Key Concepts (Contd.)

- **Observables:** Data points representing relevant information in an investigation, such as IP addresses, domains, or hashes.
- **Analyzers and Responders:** Automation mechanisms for analyzing and responding to observables using external tools.
- **Alerts:** Notifications generated by external tools or manually created to flag potential security incidents.
- **Dashboards:** Overview pages providing insights into ongoing cases, tasks, and other metrics.

Key Concepts (Contd.)

- **Observables:** Data points representing relevant information in an investigation, such as IP addresses, domains, or hashes.
- **Analyzers and Responders:** Automation mechanisms for analyzing and responding to observables using external tools.
- **Alerts:** Notifications generated by external tools or manually created to flag potential security incidents.
- **Dashboards:** Overview pages providing insights into ongoing cases, tasks, and other metrics.

Key Concepts (Contd.)

- **Observables:** Data points representing relevant information in an investigation, such as IP addresses, domains, or hashes.
- **Analyzers and Responders:** Automation mechanisms for analyzing and responding to observables using external tools.
- **Alerts:** Notifications generated by external tools or manually created to flag potential security incidents.
- **Dashboards:** Overview pages providing insights into ongoing cases, tasks, and other metrics.

Key Concepts (Contd.)

- **Observables:** Data points representing relevant information in an investigation, such as IP addresses, domains, or hashes.
- **Analyzers and Responders:** Automation mechanisms for analyzing and responding to observables using external tools.
- **Alerts:** Notifications generated by external tools or manually created to flag potential security incidents.
- **Dashboards:** Overview pages providing insights into ongoing cases, tasks, and other metrics.

Table of contents

- 1 Introduction
- 2 Architecture
- 3 Key Concepts
- 4 Workflow**
- 5 Core Features
- 6 Demonstration

General Workflow of TheHive

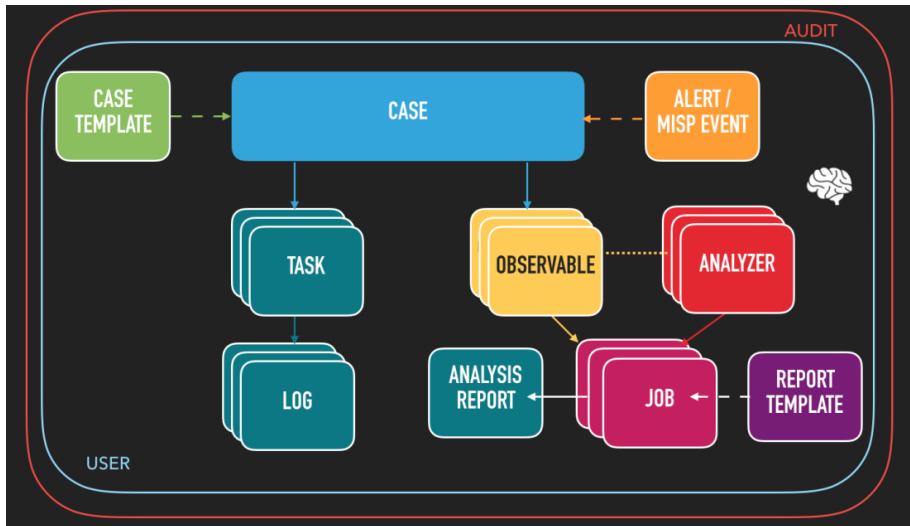


Table of contents

- 1 Introduction
- 2 Architecture
- 3 Key Concepts
- 4 Workflow
- 5 Core Features**
- 6 Demonstration

Features of TheHive

1 Case Management:

- Create cases to document and manage incidents.
- Assign cases to analysts or teams for resolution.

2 Task Assignment:

- Assign tasks and responsibilities within cases.
- Ensure organized and efficient incident response.

3 Alerts and Notifications:

- Receive alerts to notify analysts of potential security incidents.
- Stay informed and respond promptly.

Features of TheHive

① Case Management:

- Create cases to document and manage incidents.
- Assign cases to analysts or teams for resolution.

② Task Assignment:

- Assign tasks and responsibilities within cases.
- Ensure organized and efficient incident response.

③ Alerts and Notifications:

- Receive alerts to notify analysts of potential security incidents.
- Stay informed and respond promptly.

Features of TheHive

① Case Management:

- Create cases to document and manage incidents.
- Assign cases to analysts or teams for resolution.

② Task Assignment:

- Assign tasks and responsibilities within cases.
- Ensure organized and efficient incident response.

③ Alerts and Notifications:

- Receive alerts to notify analysts of potential security incidents.
- Stay informed and respond promptly.

Features of TheHive (Contd)

4 Observable Analysis:

- Document and analyze potential threats with observables.
- Utilize Cortex for real-time observable analysis.

5 Analyzer Integration:

- Use various analyzers to gather additional information.
- Enhance incident response with automated analysis.

6 Information Sharing:

- Tight integration with MISP for sharing threat intelligence.
- Import/export cases and synchronize observables with MISP.

Features of TheHive (Contd)

4 Observable Analysis:

- Document and analyze potential threats with observables.
- Utilize Cortex for real-time observable analysis.

5 Analyzer Integration:

- Use various analyzers to gather additional information.
- Enhance incident response with automated analysis.

6 Information Sharing:

- Tight integration with MISP for sharing threat intelligence.
- Import/export cases and synchronize observables with MISP.

Features of TheHive (Contd)

4 Observable Analysis:

- Document and analyze potential threats with observables.
- Utilize Cortex for real-time observable analysis.

5 Analyzer Integration:

- Use various analyzers to gather additional information.
- Enhance incident response with automated analysis.

6 Information Sharing:

- Tight integration with MISP for sharing threat intelligence.
- Import/export cases and synchronize observables with MISP.

Table of contents

- 1 Introduction
- 2 Architecture
- 3 Key Concepts
- 4 Workflow
- 5 Core Features
- 6 Demonstration**

Two key Features

- Case management
- Observable analysis with Cortex integration

Two key Features

- Case management
- Observable analysis with Cortex integration

Demonstration

Live Demonstration

Demonstration of feature One

Creating A case

The screenshot shows the 'Create case' form in The Hive Security Tool. The form is titled 'Create case' and includes the following fields and options:

- Title:** Worm infection
- Date:** 22/02/2024 06:04
- Severity:** LOW (selected), MEDIUM, HIGH, CRITICAL
- TLP:** TLP:CLEAR, TLP:GREEN, TLP:AMBER (selected), TLP:AMBER+STRICT, TLP:RED
- DAD:** DAD:CLEAR, DAD:GREEN, DAD:AMBER (selected), DAD:RED
- Tags:** CERT XLMalicious-coder/worm
- Description:** Worm infection

At the bottom of the form, there are buttons for 'Cancel' and 'Confirm'. A watermark 'Activate Windows Go to Settings to activate Windows.' is visible in the bottom right corner.

Demonstration of feature One (Contd.)

After Successful Creation of A case

The screenshot displays the 'Cases' section of The Hive Security Tool. The interface includes a top navigation bar with a search input 'Enter a case number', a 'CREATE CASE+' button, and language/region settings (ENGLISH (UK), BOB). Below the navigation bar, there are tabs for 'default', 'Quick Filters', and 'Export list'. The main content area shows a list of cases with columns for STATUS, SEVERITY, #NUMBER, TITLE, DETAILS, ASSIGNEE, and DATES. Two cases are visible:

STATUS	SEVERITY	#NUMBER	TITLE	DETAILS	ASSIGNEE	DATES
In progress	High	#2	DDOS ATTACK ON MOODLE	Tasks: 1, Observables: 1, TTPs: 0, Linked Alerts: 0	A	S: 22/02/2024 06:18, C: 22/02/2024 06:26, U: 22/02/2024 06:39
New	Low	#1	Worm infection	Tasks: 0, Observables: 0, TTPs: 0, Linked Alerts: 0	B	S: 22/02/2024 06:04, C: 22/02/2024 06:06

The interface also features a sidebar with navigation icons and a bottom status bar showing '5.2.11-1'. An 'Activate Windows' watermark is visible in the bottom right corner.

Demonstration of feature One (Contd.)

Adding a Task to a case and assign a User to it

Adding a Task

At least one log must be present

Description

⌵ B I U ↶ ☰ ☷ ⌨ ↗ ↻ 🔍

Find the Source of this attack

Preview ?

Assignee

Alice@thehive.local

Demonstration of feature One (Contd.)

After Task Assignment

The screenshot shows the The Hive Security Tool interface after a task has been assigned. The top navigation bar includes a search bar, a 'CREATE CASE+' button, and user information (ENGLISH (UK), BOB). The main header displays the case name '#2 DDOS ATTACK ON MOODLE' and various action icons.

The left sidebar contains a list of cases, with the selected case '#2' highlighted. Below the case list, the 'Assignee' is set to 'Bob', the 'Status' is 'New', and the 'Start date' is '22/02/2024 06:18'. A 'Tasks completion' progress bar is shown at the bottom of the sidebar.

The main content area shows the 'Tasks' tab for the selected case. It displays a table with the following columns: TASK, DETAILS, ASSIGNEE, DATES, S., C., U., and I. The table contains one task: 'Source Identification', assigned to 'Bob', with a due date of '22/02/2024 06:29'. The task is marked as 'Activity' and has a 'Due date in 14 days' indicator.

The bottom of the interface features a 'Go to Settings to activate Windows' message and a pagination bar showing '0 - 1 of 1' items.

Demonstration of Feature Two :Observables

- Observables are pieces of information related to a security incident.
- Observables can be added to cases in TheHive.
- 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)

Demonstration of Feature Two :Observables

- Observables are pieces of information related to a security incident.
- Observables can be added to cases in TheHive.
- 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)

Demonstration of Feature Two :Observables

- Observables are pieces of information related to a security incident.
- Observables can be added to cases in TheHive.
- 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)

Demonstration of Feature Two :Observables

- Observables are pieces of information related to a security incident.
- Observables can be added to cases in TheHive.
- 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)

Demonstration of feature Two (Contd.)

Creating An Observable

The screenshot displays the Hive Security Tool interface. The main window shows a case titled "#2 DDOS ATTACK ON MOODLE" with details such as ID -8440, created by bob@thehive.local, and status New. A modal dialog titled "Adding an Observable" is open, allowing the user to create a new observable. The dialog includes fields for Type (set to "ip") and Value (set to "10.0.8.2"). It also features a "One observable per line" toggle (checked) and a "1 observable(s)" indicator. Below these fields are sections for TLP (TLP-CLEAR, TLP-GREEN, TLP-AMBER, TLP-AMBER+STRICT, TLP-RED) and PAP (PAP-CLEAR, PAP-GREEN, PAP-AMBER, PAP-RED) labels. There are also checkboxes for "Is IOC", "Has been sighted", and "Ignore similarity". At the bottom, there is a "Tags" field with "10.0.8.2" entered. The dialog has "Cancel", "Save and add another", and "Confirm" buttons. An "Activate Windows" watermark is visible in the bottom right corner of the dialog.

Demonstration of feature Two (Contd.)

Addition of an Observable to a Case

The screenshot displays the The Hive Security Tool interface. The top navigation bar shows 'Workspaces' and 'Applications'. The main header indicates the current date and time: 'Mar 6 9:15 PM'. The browser address bar shows the URL 'localhost:9000/cases/~8040464/observables'. The left sidebar contains a navigation menu with icons for 'Cases', 'Observables', 'Tasks', 'Attachments', 'Timeline', 'Pages', and 'History'. The main content area is titled 'Cases / #1 / Observables' and includes a 'CREATE CASE +' button. Below this, there is a table of observables. The table has columns for 'id', 'created by', 'created at', 'updated at', 'severity', 'type', 'value', 'date', and 'action'. The first row shows an observable with id '~8040464', created by 'alice', and a severity of 'SEVERITY MEDIUM'. The second row shows an observable with id 'TLP:AMBER', created by 'alice', and a severity of 'TLP:AMBER'. The third row shows an observable with id 'PAP:AMBER', created by 'alice', and a severity of 'PAP:AMBER'. The fourth row shows an observable with id 'hash', created by 'alice', and a severity of 'hash'. The fifth row shows an observable with id 'virus', created by 'alice', and a severity of 'virus'. The sixth row shows an observable with id 'V1:CertReport~7 contacted domain...', created by 'alice', and a severity of 'V1:CertReport~61776'. The bottom status bar shows '5.2.11-1' and navigation controls.

id	created by	created at	updated at	severity	type	value	date	action
~8040464	alice	06/03/2024 18:40	06/03/2024 18:46	SEVERITY MEDIUM				
TLP:AMBER	alice			TLP:AMBER				
PAP:AMBER	alice			PAP:AMBER				
hash	alice			hash		fb55414848281fb04858ce188c3dc659d129e283bd62d58d34fe6f568feab37	5. 06/03/2024 18:46	
virus	alice			virus		V1:CertReport~7 contacted domain...	06/03/2024 18:46	
V1:CertReport~7 contacted domain...	alice			V1:CertReport~61776				

Demonstration of feature Two (Contd.)

Finally we can See the observables in a Case Like this

The screenshot displays the The Hive Security Tool interface. The top navigation bar includes a search bar, a 'CREATE CASE+' button, and language/user settings. The main content area shows a list of cases with columns for STATUS, SEVERITY, #NUMBER, TITLE, DETAILS, ASSIGNEE, and DATES. Two cases are visible:

STATUS	SEVERITY	#NUMBER	TITLE	DETAILS	ASSIGNEE	DATES
In progress 13 minutes	High	#2	DDOS ATTACK ON MOODLE	Tasks: 1 Observables: 1 TTPs: 0 Linked Alerts: 0	A	S: 22/02/2024 06:18 C: 22/02/2024 06:26 U: 22/02/2024 06:39
New 33 minutes	Medium	#1	Worm infection	Tasks: 0 Observables: 0 TTPs: 0 Linked Alerts: 0	B	S: 22/02/2024 06:04 C: 22/02/2024 06:06

The interface also includes a sidebar with navigation icons and a bottom status bar showing '5.2.11-1'.

Summary

- TheHive is a collaborative Security Incident Response Platform.
- Features include case management, observable analysis, and active response.
- The architecture comprises a sleek frontend, robust backend, Cortex analytics, reliable storage, and powerful analyzers.
- Key concepts involve users, organizations, cases, and tasks.
- Analyzers enhance intelligence, while responders enable active responses.

Thank You!

Thank you for your attention!

Any questions or discussions are welcome.