

The Hive Security Tool

Sumaiya Seaha, 1905033

Fariha Zaman Aurin, 1905049

Debjany Ghosh Aronno, 1905053

Department of CSE

Bangladesh University of Engineering & Technology

March 9, 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

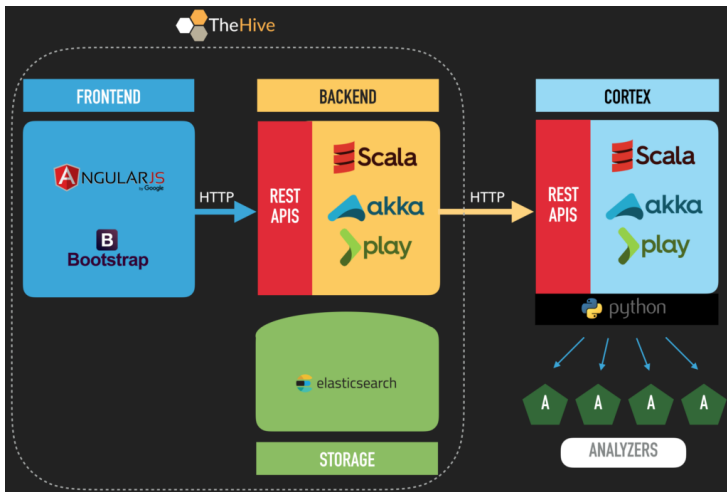


Figure: Overview of TheHive's Architecture

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

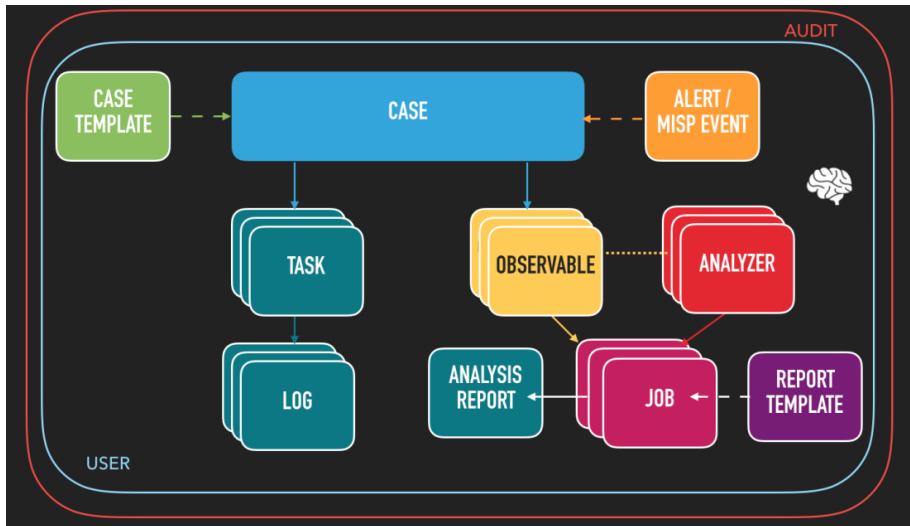


Table of contents

- 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

Create case

* Title
Worm infection

* Date
22/02/2024 06:04

Severity

TLP

DAD

Tags

* Description
 Worm infection

Tasks Custom fields Pages

Activate Windows
Go to Settings to activate Windows.

Cancel Confirm

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/user settings. Below the navigation bar, there are tabs for 'default', 'Quick Filters', and 'Export list'. The main area shows a table of cases with columns for STATUS, SEVERITY, #NUMBER, TITLE, DETAILS, ASSIGNEE, and DATES. Two cases are listed:

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	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

At the bottom of the interface, there is a '5.2.11-1' version indicator and a Windows watermark: 'Activate Windows. Go to Settings to activate Windows.' with navigation buttons for 'Previous', '0 - 2 of 2', 'Next', 'Show', and '30'.

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

A

alice@thehive.local

▼

Demonstration of feature One (Contd.)

After Task Assignment

The screenshot displays the 'Cases / #1 / Task' view in The Hive Security Tool. The main panel shows a task titled 'suspicious hash analysis' with a task ID of 'id -8040464'. The task was created by 'alice@thehive.local' on '06/03/2024 18:40' and updated at '06/03/2024 18:46'. The task is assigned to 'alice' and has a status of 'New'. The start date is '06/03/2024 18:38'. The task completion is shown as a red progress bar. The task description is 'run analyser on this hash' with a due date of 'Due date in 4 days'. The task is listed in the 'TASKS' table with columns: TASK, ORDER, DETAILS, ASSIGNEE, DATES, S, C, U. The task is assigned to 'alice' and has a due date of '06/03/2024 18:42'. The task is listed in the 'TASKS' table with columns: TASK, ORDER, DETAILS, ASSIGNEE, DATES, S, C, U.

General | Tasks (1) | Observables (1) | TTPs (0) | Attachments | Timeline | Pages | History

default Quick Filters Export list

TASK: ORDER

DETAILS

ASSIGNEE DATES S C U

Activity 0 06/03/2024 18:42

Assignee: alice

Status: New

Start date: 06/03/2024 18:38

Tasks completion

Contributors

Time to detect: 3 minutes

5.2.10-1

Previous 0 / 1 of 1 Next Show 30

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 a status of New. A modal dialog titled "Adding an Observable" is open, allowing the user to add 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, there 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.)

Finally we can See the observables in a Case Like this

The screenshot displays the 'Observables' tab for a case named 'Unauthorized access'. The interface includes a sidebar with navigation icons and a main content area. The case details on the left show ID -4132984, created by alice@thehive.local, and updated at 06/03/2024 19:57. The main area lists two observables:

FLAGS	DATA TYPE	VALUE/FILENAME	DATES
TLP:AMBER PAP:AMBER	IP	8[]8[]8[]8	S. 06/03/2024 20:05 C. 06/03/2024 20:05
TLP:GREEN PAP:GREEN	IP	10[]10[]1[]1	S. 06/03/2024 19:57 C. 06/03/2024 19:57

Below the observables, it states 'No report(s) available'. The bottom of the interface shows navigation controls for the case, including 'Previous', '0 - 2 of 2', 'Next', 'Show', and '30'.

Demonstration of feature Two (Contd.)

Applying analyzer

TheHive + New Case My tasks 1 Waiting tasks 1 Alerts 1 All Dashboards Search

Case # 13 - Demo Case

pranta 08/05/22 16:37 2 minutes

Details Tasks 1 Observations

1 selected observable + Add observable(s)

Filters + Add a filter

Analyzer observable(s)

Select the analyzers you want to run on the selected observables.

hash analyzers Select all / Deselect all

- ☒ VirusTotal_GetReport_3_0
- ☐ Hashdd_Detail_2_0
- ☐ Urlscan_io_Search_0_1_1
- ☐ Malwares_GetReport_1_0
- ☐ Cyberprotect_ThreatScore_3_0

Cancel Run selected analyzers

List of observables (2 of 2) (1 selected)

Flags	Type	Value/Filename	Dates	S	v	C	U	Actions
<input checked="" type="checkbox"/>	hash	A593C024778F860F299C8B7D4A5B1E48ECC3C1E51583EAAF1BF73E9747403EC4	S. 08/05/22 16:39					
		malicious file	C. 08/05/22 16:39					
		No reports available						

Demonstration of feature Two (Contd.)

Analysis result

The screenshot displays the The Hive Security Tool interface for a case titled "suspicious hash analysis". The interface is divided into several sections:

- Header:** Shows "Cases / #1 / Observables", a search bar for "Enter a case number", a "CREATE CASE +" button, and user information "ENGLISH (UK) ALICE".
- Left Sidebar:** Contains navigation icons and a list of cases. The current case is highlighted.
- Case Details (Left Panel):**
 - ID:** -B040464
 - Created by:** alice
 - Created at:** 06/03/2024 18:40
 - Updated at:** 06/03/2024 18:46
 - Severity:** MEDIUM
 - Assignee:** alice
 - Status:** New
 - Start date:** 06/03/2024 18:38
 - Tasks completion:** (Progress bar)
 - Contributors:** (List)
 - Time to detect:** 3 minutes
- Observables (Main Panel):**
 - General:** default
 - Flags:** (List)
 - Data Type:** VALUE/FILENAME
 - Observables:**
 - TLP:AMBER:** hash: fb55414b482b1f044958ce180c3dc659d129e283bd62d58d34f6e6568feab37
 - PAP:AMBER:** virus: VT:GaiReport*7 contacted domain... VT:GaiReport*61776
 - DATES:** S: 06/03/2024 18:46, C: 06/03/2024 18:46

Demonstration of feature Two (Contd.)

Analysis report

The screenshot displays the 'Analysis report' window in The Hive Security Tool. The left sidebar shows the case details for 'suspicious hash analysis', including its ID, creation and update timestamps, and a list of tasks. The main panel is divided into two sections: 'Observables extracted from analysis report' and a 'Summary' table.

Observables extracted from analysis report

TYPE	VALUE
other	import "pe" /import "hash" rule MAL_Malware_imp hash_Mar23_1 [meta ... [detection:YARA] rule:gen_imp hash_detection]
other	import "pe" rule INDICATOR_TOOL_IPWS_LaZagne [meta: author = "Stek... [detection:YARA] rule:indicator_tool]
other	import "pe" / Mimikatz / rule Mimikatz_Memory_Rule_1_APT [meta: ... [detection:YARA] rule:gen_mimikatz]
other	rule Windows_Hacktool_Mimikatz_1388212a [meta: author = "Elastic Se... [detection:YARA] rule:etWindows_Hacktool_Mimikatz]
other	/ Yara Rule Set Author [see the author field in the rules] Date: 2017... [detection:YARA] rule:set.yara]

[Show raw result](#)

Summary

Category	Count	Size	Last analysis date
Malicious	61/72	8043528	2024-02-25 06:39:28
Suspicious	9/72		
Undefined	11/72		

Names

- %SystemRoot%\System32\cmd.exe
- mimikatz
- mimikatz.exe

Demonstration of feature Two (Contd.)

Job details in Cortex(Job report in JSON format)

The screenshot displays the Cortex web interface. The top navigation bar includes the Cortex logo, a '+ New Analysis' button, and links for 'Jobs History', 'Analyzers', 'Responders', 'Organization', and a user profile 'demo/alice'. The main content area is titled 'Job details' and features a sidebar on the left with job metadata and a main panel on the right showing the job report in JSON format.

Job details sidebar:

- Artifact:** VirusTotal_GetReport_3_1
- Hash:** [HASH] f5554148482b1f804858ce188c3dc659d129e283bd62d58d34f6ef568feab37
- Date:** 9 minutes ago
- TLP:** TLP:AMBER
- PAP:** PAP:AMBER
- Status:** Success
- Report summary:** VT:GetReport-"61/76" VT:GetReport-"7 contacted domain(s)"

Job report (JSON format):

```
{
  "organisation": "demo",
  "user": "alice@thehive.local"
}

{
  "summary": {
    "taxonomies": [
      {
        "level": "malicious",
        "namespace": "VT",
        "predicate": "GetReport",
        "value": "61/76"
      },
      {
        "level": "malicious",
        "namespace": "VT",
        "predicate": "GetReport",
        "value": "7 contacted domain(s)"
      }
    ]
  },
  "full": {
    "type": "file",
    "attributes": {
      "type.tape": {
        "executable",
        "windows",
        "win32",
        "pe",
        "..."
      }
    }
  }
}
```

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.