TheHive

CSE 406 Project Report

Azizur Rahman Anik[1] K.M Fahim Shahriyar[2]

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

September 13, 2023

[1] Student ID: 1805115

[2] Student ID: 1805113

Introduction

TheHive is a scalable open source and free Security Incident Response Platform designed to make life easier for SOCs, CSIRTs, CERTs and any information security practitioner dealing with security incidents that need to be investigated and acted upon swiftly.

We can synchronize it with one or multiple MISP instances to start investigations out of MISP events. We can also export an investigation's results as a MISP event to help our peers detect and react to attacks we've dealt with. Additionally, when TheHive is used in conjunction with Cortex, security analysts and researchers can easily analyze tens if not hundred of observables.

Introduction continued

Collaboration is at the heart of TheHive. Multiple analysts from one organisations can work together on the same case simultaneously. For example, an analyst may deal with malware analysis while another may work on tracking C2 beaconing activity on proxy logs as soon as IOCs have been added by their coworker. Using TheHive's live stream, everyone can keep an eye on what's happening on the platform, in real time.

So the main purpose of using this tool is to detect any security incident quickly and analyze that incident in a collaborative platform to solve any security issue efficiently.

Source Code Architecture

Backend: TheHive's backend is Written in Scala.The backend is primarily based on the Play Framework.

Frontend: TheHive's frontend is built using AngularJS.

Database: TheHive primarily used the Elasticsearch search and analytics engine as its data store and indexing solution. Later it used Casandra, a distributed NoSQL database that is typically used for handling large volumes of structured and semi-structured data in a horizontally scalable and fault-tolerant manner

Documentation and Configuration: The project is typically well-documented, providing guidance for installation, configuration, and usage.Configuration files are used to customize the behavior of TheHive to suit an organization's specific needs.

APIs

APIs are available for following purposes.

1. Organization
2. User
3. Custom field
4. Case template
5. Alert
6. Case
7. task
8. Observable

Key components

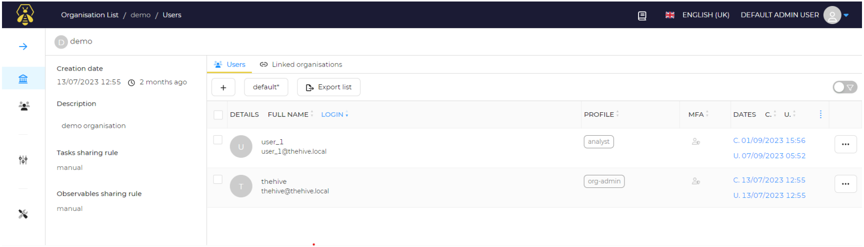
Key components of this tool are :

1. Organization
2. Case
3. Tasks
4. Observables

Organization

There are two types of account in TheHive.One is "Admin" and another is "User".Admin can create an organization and create users of that organization.The admin also can also assign role of each user in an organization.Those role reperesents the access permission of various components for a particular user of a orgnization.There can be three types of roles : Analyst,org-Admin,read-only.

Organization continued



Creation date
13/07/2023 12:55 2 months ago

Description
demo organisation

Tasks sharing rule
manual

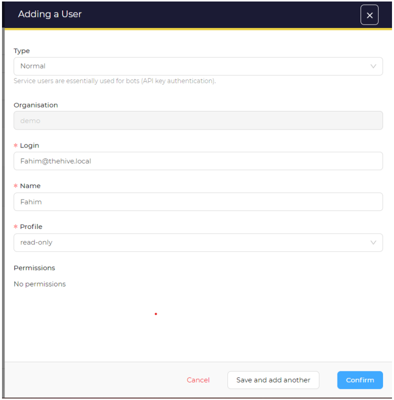
Observables sharing rule
manual

DETAILS	FULL NAME	LOGIN	PROFILE	MFA	DATES C. U.
U	user_1	user_1@thehive.local	analyst		C. 01/09/2023 15:56 U. 07/09/2023 05:52
T	thehive	thehive@thehive.local	org-admin		C. 13/07/2023 12:55 U. 13/07/2023 12:55

Figure: Organization dashboard

Here, in the above image an admin logged in whose name is "DEFAULT ADMIN USER" and he creates an orgnization named "demo" .In "demo" organization he creates two users.He can add more user by clicking "+" sign . After clicking "+" sign the following dialogbox will be shown to provide user information.After filling up the dialog box with user information and clicking on "Confirm" ,a new user will be added to organization

Organization continued



Adding a User

Type

Normal

Service users are essentially used for bots (API key authentication).

Organisation

demo

* Login

Fahim@thehive.local

* Name

Fahim

* Profile

read-only

Permissions

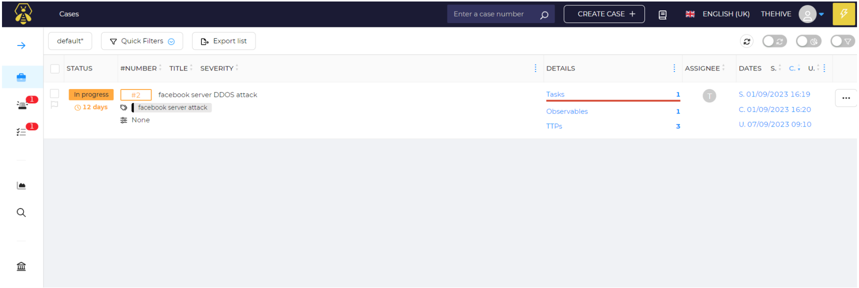
No permissions

Figure: Adding a user

Cases

Users of an organization with analyst or org-admin role can create cases at the response of any security incident and Other users can see the case and deal with the cases collaboratively.

After logging into an user account ,a user can see the list of cases of his organization .



STATUS	#NUMBER TITLE SEVERITY	DETAILS		ASSIGNEE	DATES S. C. U.
In progress 12 days	#2 facebook server DDOS attack facebook server attack None	Tasks Observables TTPs	1 1 3	T	S. 01/09/2023 16:19 C. 01/09/2023 16:20 U. 07/09/2023 09:10

Figure: User dashboard

Cases continued

To create a new case a user can click on "CREATE CASE +" button on the top and then the following dialogbox will be shown

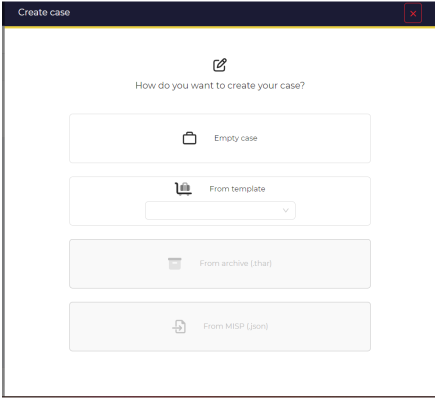
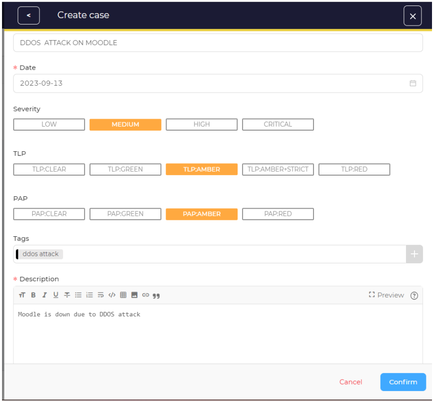


Figure: Choose case type(Empty or template)

Cases continued

From above user can select "EMPTY" to create a case from scratch or he can import a security event as a case from "MISP" after selecting "template" option

After selecting "EMPTY" the follwing dialog box will be shown



DDOS ATTACK ON MOODLE

* Date

2023-09-13

Severity

LOW [✓ MEDIUM] HIGH CRITICAL

TLP

TLP:CLEAR TLP:GREEN [✓ TLP:AMBER] TLP:AMBER+STRICT TLP:RED

PAP

PAP:CLEAR PAP:GREEN [✓ PAP:AMBER] PAP:RED

Tags

ddos attack

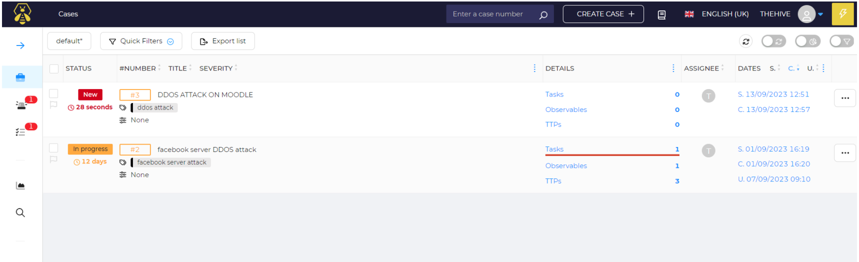
* Description

```
Moodle is down due to DDOS attack
```

Figure: Creating a case

Cases continued

Then after filling the dialog box with the information of security incident,when he clicks on ”Confirm” a new case will be added to its organization and the case will be seen by other users of this organization.

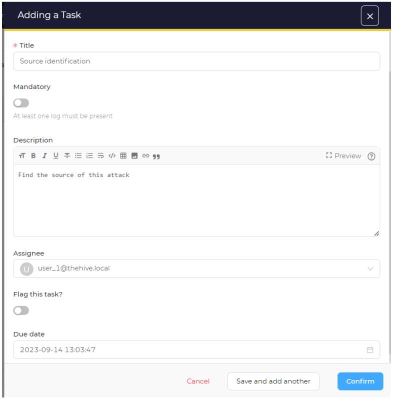


STATUS	#NUMBER	TITLE	SEVERITY	DETAILS		ASSIGNEE	DATES S. C. U.
New 28 seconds	#3	DDOS ATTACK ON MOODLE ddos attack None		Tasks Observables TTPs	0 0 0	T	S. 13/09/2023 12:51 C. 13/09/2023 12:57
In progress 12 days	#2	facebook server DDOS attack facebook server attack None		Tasks Observables TTPs	1 1 3	T	S. 01/09/2023 16:19 C. 01/09/2023 16:20 U. 07/09/2023 09:10

Figure: User dashboard(after creating a case)

Task

After creating a new case ,a user can create tasks which should be performed to resolve the case and assign those tasks to different users. So,For a particular case while adding a task we need to fill up the following dialogbox with necessary information about that task



Adding a Task

* Title: Source identification

Mandatory: ○

At least one log must be present

Description: Find the source of this attack

Assignee: user_1@thehive.local

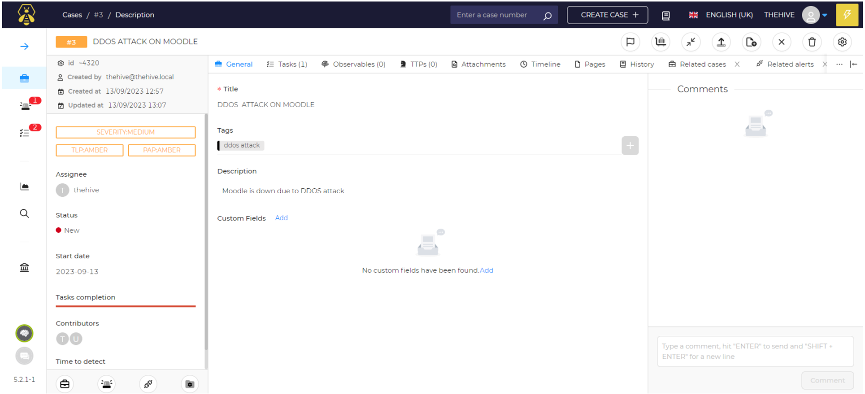
Flag this task?: ○

Due date: 2023-09-14 13:03:47

Figure: Adding a task

Task continued

Then after creating a task successfully the dashboard of a case under "Tasks" tab will look like below



#3 DDOS ATTACK ON MOODLE

id ~4320
Created by thehive@thehive.local
Created at 13/09/2023 12:57
Updated at 13/09/2023 13:07

SEVERITY:MEDIUM
TLP:AMBER PAP:AMBER

Assignee
thehive

Status
New

Start date
2023-09-13

Tasks completion

Contributors
T U

Time to detect

* Title
DDOS ATTACK ON MOODLE

Tags
ddos attack

Description
Moodle is down due to DDOS attack

Custom Fields Add

No custom fields have been found.Add

Type a comment, hit "ENTER" to send and "SHIFT + ENTER" for a new line

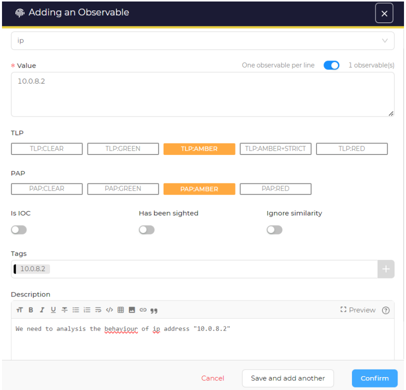
Figure: Case dashboard(after adding a new task)

Observable

Observables are the elements of a case on which the user(security analyst) will report their analysis(e.g. ip address, hash of malicious file)

Observable continued

For a case a user can add one or more observables. To add a new observable a user need to fill up the following dialog box.



Adding an Observable

ip

* Value: 10.0.8.2

One observable per line: on — 1 observable(s)

TLP: TLP:AMBER

PAP: PAP:AMBER

Is IOC: off

Has been sighted: off

Ignore similarity: off

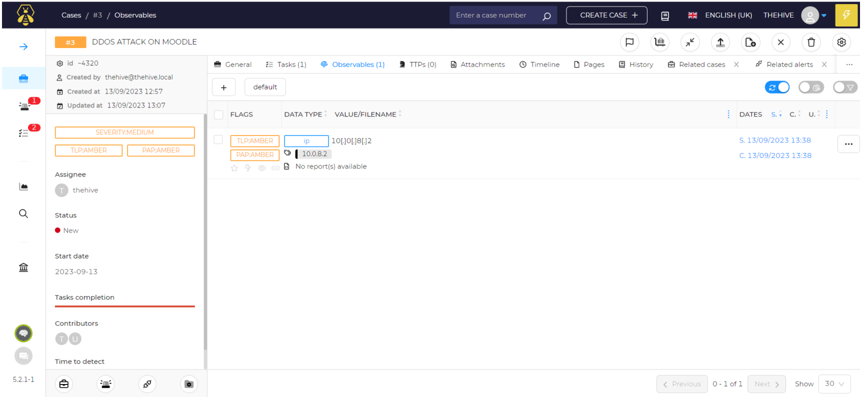
Tags: 10.0.8.2

Description: We need to analysis the behaviour of ip address "10.0.8.2"

Figure: Adding an observable

Observable continued

After adding an observable successfully, the dashboard of a case under "Observables" tab will look like below



#3 DDOS ATTACK ON MOODLE

id ~4320
Created by thehive@thehive.local
Created at 13/09/2023 12:57
Updated at 13/09/2023 13:07

SEVERITY:MEDIUM
TLP:AMBER PAP:AMBER

Assignee
thehive

Status
● New

Start date
2023-09-13

Tasks completion

Contributors
T U

Time to detect

FLAGS	DATA TYPE	VALUE/FILENAME	DATES
TLP:AMBER PAP:AMBER	ip	10[.]0[.]8[.]2 10.0.8.2 No report(s) available	S. 13/09/2023 13:38 C. 13/09/2023 13:38

‹ Previous 0 - 1 of 1 Next › Show 30

Figure: Case dashboard(after adding a new task)

Observable continued

Then after adding observables for a case ,the analysts can report their analysis on these observables by doing analysis manually or he can automate the process of analysis with the help of "CORTEX".

Cortex

Cortex is a software project that complements and extends the capabilities of TheHive, a security incident response platform. It serves as an automation and orchestration engine. It automates the execution of various analysis tasks and security operations related to incident response by making api calls to various threat intelligence feeds and collects their outputs.

Cortex: Key Features

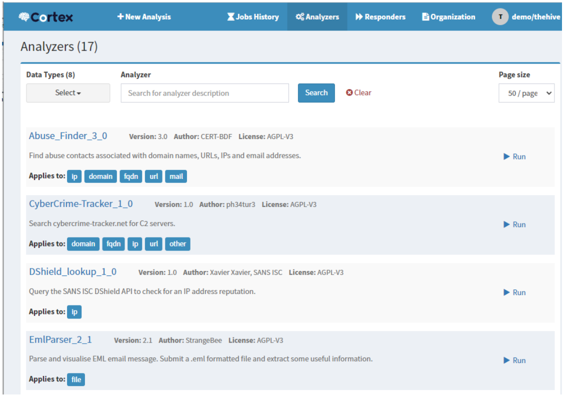
1. **Automation:** Cortex allows users to define and execute a wide range of actions, such as analyzing observables, querying threat intelligence feeds such as VirusTotal, CyberCrime-Tracker etc. and interacting with other security tools and services.
2. **Analyzer Integration:** Cortex includes a collection of analyzers, which are plugins, enabled by adding API key, can be used to analyze different types of observables, for example, IP addresses, urls, hashes etc. These analyzers can be integrated into TheHive through Cortex and automatically perform tasks like malware analysis, DNS lookups etc. The generated reports can be shared with other security analysts of the organization which saves analysts time and standardize the investigation process.

Cortex: Key Features continued

3. **Responder Integration:** Responders are plugins that can take action based on the analysis results. For example, if an analyzer detects a malicious URL, a responder can be configured to block the URL at the firewall or update an indicator of compromise blacklist.
4. **Extensibility:** Cortex allows organizations to develop custom analyzers and responders tailored to their specific needs. This flexibility makes it a valuable tool for organizations with unique security requirements.
5. **Integration with TheHive:** By integrating cortex with TheHive, it is easy to automate analysis and response actions into TheHive's case management and incident tracking workflows.

Cortex Analzers

We have used a traning VM which have total 216 analyzers available and 16 of them are enabled with API key. To enable a new Analyzer, we just need to add the API key for that. A snapshot of some of the Analyzers from Cortex is shown below.



Analyzers (17)

Data Types (8) | Analyzer: Search for analyzer description | Page size: 50 / page

Abuse_Finder_3_0 Version: 3.0 Author: CERT-BDF License: AGPL-V3

Find abuse contacts associated with domain names, URLs, IPs and email addresses.

Applies to: ip domain fqdn url mail

CyberCrime-Tracker_1_0 Version: 1.0 Author: ph34tur3 License: AGPL-V3

Search cybercrime-tracker.net for C2 servers.

Applies to: domain fqdn ip url other

DShield_lookup_1_0 Version: 1.0 Author: Xavier Xavier, SANS ISC License: AGPL-V3

Query the SANS ISC DShield API to check for an IP address reputation.

Applies to: ip

EmlParser_2_1 Version: 2.1 Author: StrangeBee License: AGPL-V3

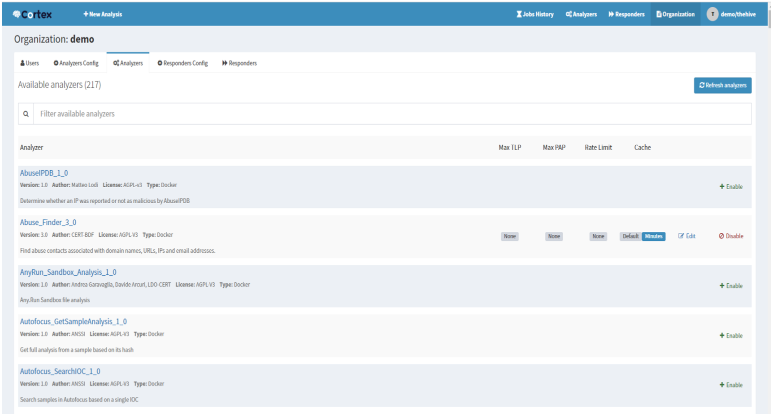
Parse and visualise EML email message. Submit a .eml formatted file and extract some useful information.

Applies to: file

Figure: Cortex Analyzers

Enabling An Analyzer

In the **Organization** tab of Cortex, all the analyzers that are available are provided. To enable an analyzer, press the enable button.



Organization: **demo**

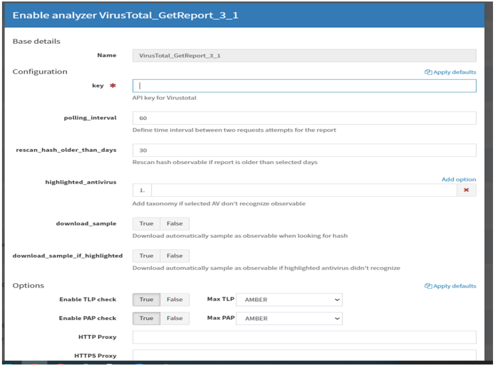
Available analyzers (217)

Analyzer	Max TLP	Max PAP	Rate Limit	Cache		
AbuseIPDB_1_0 **Version:** 1.0 **Author:** Matteo Lodi **License:** AGPL-v3 **Type:** Docker Determine whether an IP was reported or not as malicious by AbuseIPDB						+ Enable
Abuse_Finder_3_0 **Version:** 3.0 **Author:** CERT-BDF **License:** AGPL-V3 **Type:** Docker Find abuse contacts associated with domain names, URLs, IPs and email addresses.	None	None	None	Default Minutes	Edit	Disable
AnyRun_Sandbox_Analysis_1_0 **Version:** 1.0 **Author:** Andrea Garavaglia, Davide Arcuri, LDO-CERT **License:** AGPL-V3 **Type:** Docker Any.Run Sandbox file analysis						+ Enable
Autofocus_GetSampleAnalysis_1_0 **Version:** 1.0 **Author:** ANSSI **License:** AGPL-V3 **Type:** Docker Get full analysis from a sample based on its hash						+ Enable
Autofocus_SearchIOC_1_0 **Version:** 1.0 **Author:** ANSSI **License:** AGPL-V3 **Type:** Docker Search samples in Autofocus based on a single IOC						+ Enable

Figure: Enabling an Analyzer

Enabling An Analyzer continued

The following box will be shown after pressing the enable button. To enable an analyzer, go to it's website and get the API key and put it here in the **key** option.



Enable analyzer VirusTotal_GetReport_3_1

Base details

Name: VirusTotal_GetReport_3_1

Configuration

key *: |

API key for Virustotal

polling_interval: 60

Define time interval between two requests attempts for the report

rescan_hash_older_than_days: 30

Rescan hash observable if report is older than selected days

highlighted_antivirus: 1.

Add taxonomy if selected AV don't recognize observable

download_sample: True False

Download automatically sample as observable when looking for hash

download_sample_if_highlighted: True False

Download automatically sample as observable if highlighted antivirus didn't recognize

Options

Enable TLP check: [✓ True] False — Max TLP: AMBER

Enable PAP check: [✓ True] False — Max PAP: AMBER

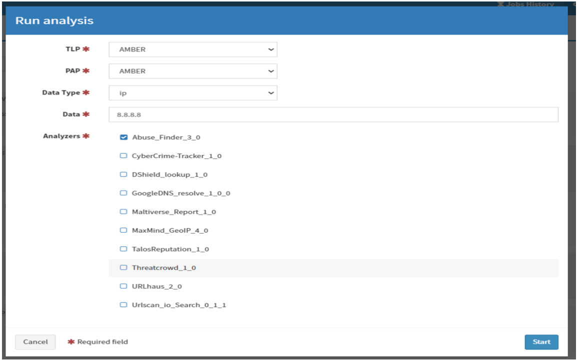
HTTP Proxy:

HTTPS Proxy:

Figure: Adding the API key

Running An Analyzer in Cortex

To run an analyzer, fill up the TLP, PAP, Data Type and Data and select the suitable analyzer accordingly. We can also select multiple analyzers for the same data.



Run analysis

TLP ✱ AMBER

PAP ✱ AMBER

Data Type ✱ ip

Data ✱ 8.8.8.8

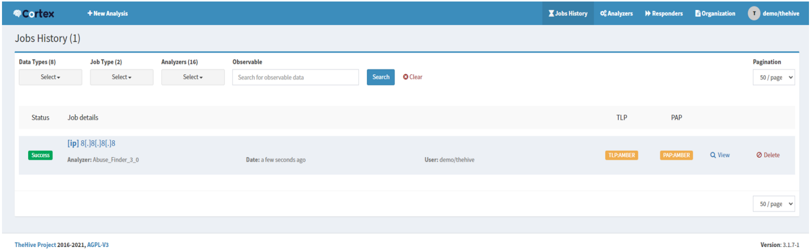
Analyzers ✱

- ☑ Abuse_Finder_3_0
- □ CyberCrime-Tracker_1_0
- □ DShield_lookup_1_0
- □ GoogleDNS_resolve_1_0_0
- □ Maltiverse_Report_1_0
- □ MaxMind_GeoIP_4_0
- □ TalosReputation_1_0
- □ Threatcrowd_1_0
- □ URLhaus_2_0
- □ Urlscan_io_Search_0_1_1

Figure: Running an Analyzer

Running An Analyzer in Cortex continued

The running log can be seen from the **Jobs History** in Cortex. If the status is **Success**, then it has successfully generated report by querying into that analyzer. If the status is **Failure**, then there may be a problem in data type or format or the server may be down.



Jobs History (1)

Status	Job details			TLP	PAP
Success	[ip] 8[.]8[.]8[.]8 Analyzer: Abuse_Finder_3_0	Date: a few seconds ago	User: demo/thehive	TLP:AMBER	PAP:AMBER

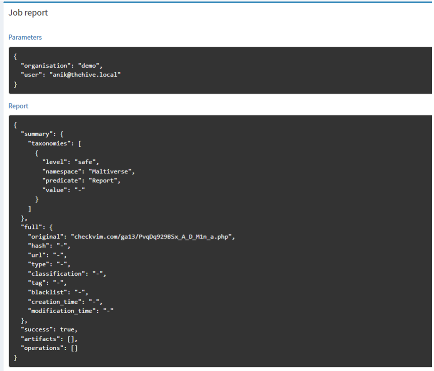
TheHive Project 2016-2021, AGPL-V3

Version: 3.1.7-1

Figure: Jobs history

Raw Report of Analyzer

By default in Cortex, the report generated by any analyzer is in JSON format which is not so human readable.



Job report

Parameters

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

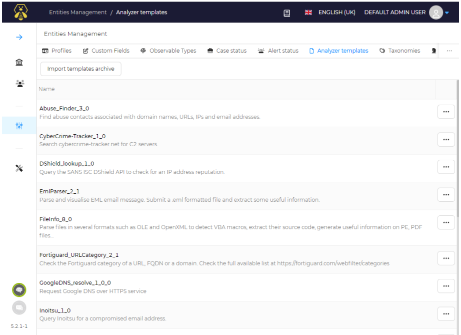
Report

```
{
  "summary": {
    "taxonomies": [
      {
        "level": "safe",
        "namespace": "Maltiverse",
        "predicate": "Report",
        "value": "-"
      }
    ]
  },
  "full": {
    "original": "checkvim.com/ga13/PvqDq929BSx_A_D_M1n_a.php",
    "hash": "-",
    "url": "-",
    "type": "-",
    "classification": "-",
    "tag": "-",
    "blacklist": "-",
    "creation_time": "-",
    "modification_time": "-"
  },
  "success": true,
  "artifacts": [],
  "operations": []
}
```

Figure: Raw report of the analyzer

Adding Templates From TheHive

To make the raw reports of Cortex more human readable, we can integrate the cortex with TheHive and add **templates** from admin account. In the traning vm, the cortex is integrated with TheHive. Therefore, we can analyze the observables from TheHive which will trigger the analyzer in Cortex.



Abuse_Finder_3_0
Find abuse contacts associated with domain names, URLs, IPs and email addresses.

CyberCrime-Tracker_1_0
Search cybercrime-tracker.net for C2 servers.

DShield_lookup_1_0
Query the SANS ISC DShield API to check for an IP address reputation.

EmlParser_2_1
Parse and visualise EML email message. Submit a .eml formatted file and extract some useful information.

FileInfo_8_0
Parse files in several formats such as OLE and OpenXML to detect VBA macros, extract their source code, generate useful information on PE, PDF files...

Fortiguard_URLCategory_2_1
Check the Fortiguard category of a URL, FQDN or a domain. Check the full available list at https://fortiguard.com/webfilter/categories

GoogleDNS_resolve_1_0_0
Request Google DNS over HTTPS service

Inoitsu_1_0
Query Inoitsu for a compromised email address.

Figure: Adding Templates from TheHive's Admin

Analyzing An Observable From TheHive

To analyze an observable from TheHive, we need to select an observable. Then among all the enabled analyzers, the ones that can analyze the selected data type will be shown. We can select one or more(up to all) analyzers and run which will then generate reports for the selected analyzers.

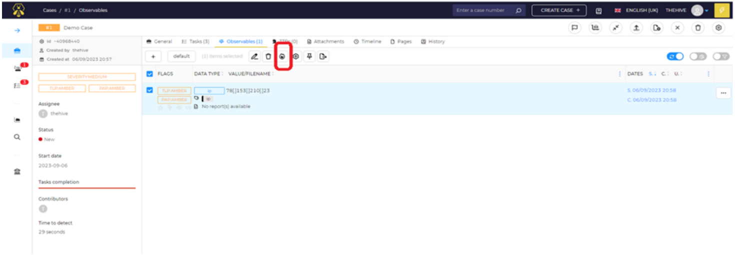
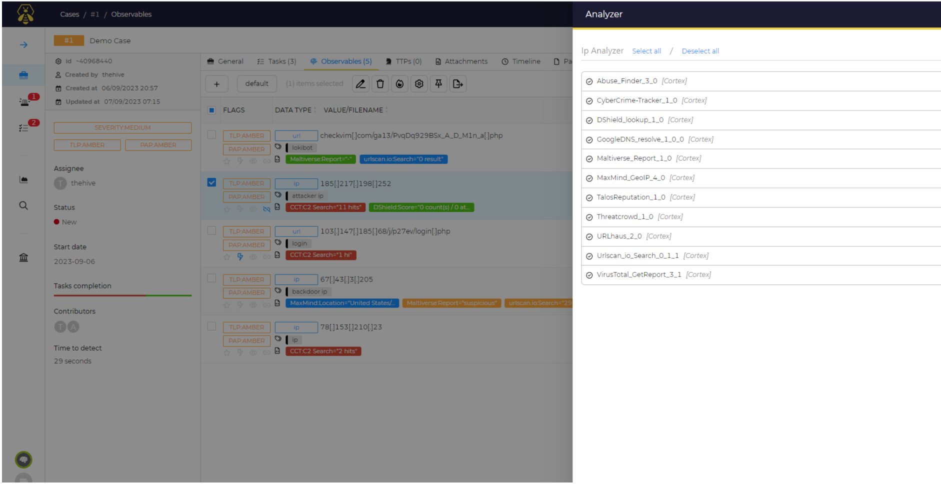


Figure: Analyzing an observable from TheHive

Analyzing An Observable From TheHive continued



Cases / #1 / Observables

#1 Demo Case

id ~40968440
Created by thehive
Created at 06/09/2023 20:57
Updated at 07/09/2023 07:15

SEVERITY:MEDIUM
TLP:AMBER PAP:AMBER

Assignee
thehive

Status
New

Start date
2023-09-06

Tasks completion

Contributors

Time to detect
29 seconds

☑	FLAGS	DATA TYPE	VALUE/FILENAME
□	TLP:AMBER PAP:AMBER	url	checkvim[.]com/ga13/PvqDq929BSx_A_D_M1n_a[.]php lokibot Maltiverse:Report="-" urlscan.io:Search="0 result"
☑	TLP:AMBER PAP:AMBER	ip	185[.]217[.]198[.]252 attacker ip CCT:C2 Search="11 hits" DShield:Score="0 count(s) / 0 at...
□	TLP:AMBER PAP:AMBER	url	103[.]147[.]185[.]68/j/p27ev/login[.]php login CCT:C2 Search="1 hi"
□	TLP:AMBER PAP:AMBER	ip	67[.]43[.]3[.]205 backdoor ip MaxMind:Location="United States/... Maltiverse:Report="suspicious" urlscan.io:Search="29
□	TLP:AMBER PAP:AMBER	ip	78[.]153[.]210[.]23 ip CCT:C2 Search="2 hits"

Analyzer

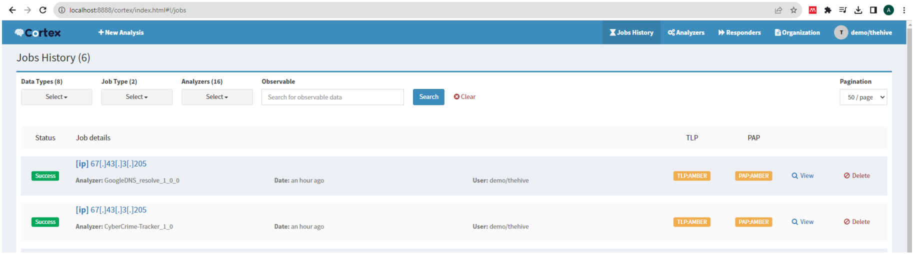
Ip Analyzer Select all / Deselect all

- ✓ Abuse_Finder_3_0 [Cortex]
- ✓ CyberCrime-Tracker_1_0 [Cortex]
- ✓ DShield_lookup_1_0 [Cortex]
- ✓ GoogleDNS_resolve_1_0_0 [Cortex]
- ✓ Maltiverse_Report_1_0 [Cortex]
- ✓ MaxMind_GeoIP_4_0 [Cortex]
- ✓ TalosReputation_1_0 [Cortex]
- ✓ Threatcrowd_1_0 [Cortex]
- ✓ URLhaus_2_0 [Cortex]
- ✓ Urlscan_io_Search_0_1_1 [Cortex]
- ✓ VirusTotal_GetReport_3_1 [Cortex]

Figure: Selecting the analyzer(s)

Analyzing An Observable From TheHive continued

Running an analyzer on an observable from TheHive automatically fires the analyzer from Cortex. The analysis report can be found in both Cortex and TheHive.



Jobs History (6)

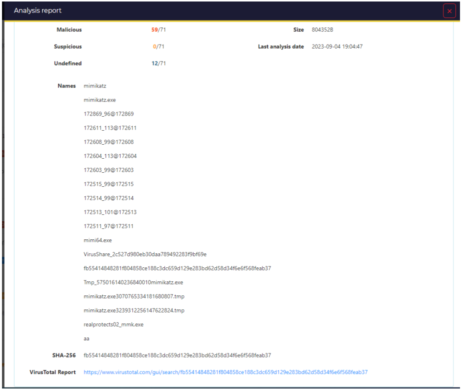
Data Types (8): Select
Job Type (2): Select
Analyzers (16): Select
Observable: Search for observable data
Search
Clear
Pagination: 50 / page

Status	Job details			TLP	PAP		
Success	[ip] 67[.]43[.]3[.]205 **Analyzer:** GoogleDNS_resolve_1_0_0	**Date:** an hour ago	**User:** demo/thehive	TLP:AMBER	PAP:AMBER	View	Delete
Success	[ip] 67[.]43[.]3[.]205 **Analyzer:** CyberCrime-Tracker_1_0	**Date:** an hour ago	**User:** demo/thehive	TLP:AMBER	PAP:AMBER	View	Delete

Figure: Running log of the analyzer

Analyzer Report: VirusTotal

We have analyzed a malicious hash : fb55414848281f804858ce188c3dc659d129e283bd62d58d34f6e6f568feab37 which was collected from the VirusTotal website. By running the VirusTotal analyzer for this observable, we get the following report.



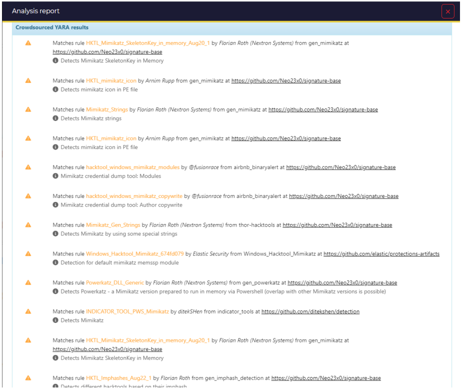
Analysis report

Malicious	59/71	Size	804352B
Suspicious	0/71	Last analysis date	2023-09-04 19:04:47
Undefined	12/71		

Names	mimikatz mimikatz.exe 172869_96@172869 172611_113@172611 172608_99@172608 172604_113@172604 172603_99@172603 172515_99@172515 172514_99@172514 172513_101@172513 172511_97@172511 mimi64.exe VirusShare_2c527d980eb30daa789492283f9bf69e fb55414848281f804858ce188c3dc659d129e283bd62d58d34f6e6f568feab37 Tmp_575016140236840010mimikatz.exe mimikatz.exe3070765334181680807.tmp mimikatz.exe3239312256147622824.tmp realprotects02_mmk.exe aa
SHA-256	fb55414848281f804858ce188c3dc659d129e283bd62d58d34f6e6f568feab37
VirusTotal Report	https://www.virustotal.com/gui/search/fb55414848281f804858ce188c3dc659d129e283bd62d58d34f6e6f568feab37

Figure: VirusTotal Report

Analyzer Report: VirusTotal continued



Analysis report

Crowdsourced YARA results

⚠ Matches rule HKTL_Mimikatz_SkeletonKey_in_memory_Aug20_1 by *Florian Roth (Nextron Systems)* from gen_mimikatz at https://github.com/Neo23x0/signature-base
ℹ Detects Mimikatz SkeletonKey in Memory

⚠ Matches rule HKTL_mimikatz_icon by *Arnim Rupp* from gen_mimikatz at https://github.com/Neo23x0/signature-base
ℹ Detects mimikatz icon in PE file

⚠ Matches rule Mimikatz_Strings by *Florian Roth (Nextron Systems)* from gen_mimikatz at https://github.com/Neo23x0/signature-base
ℹ Detects Mimikatz strings

⚠ Matches rule HKTL_mimikatz_icon by *Arnim Rupp* from gen_mimikatz at https://github.com/Neo23x0/signature-base
ℹ Detects mimikatz icon in PE file

⚠ Matches rule hacktool_windows_mimikatz_modules by *@fusionrace* from airbnb_binaryalert at https://github.com/Neo23x0/signature-base
ℹ Mimikatz credential dump tool: Modules

⚠ Matches rule hacktool_windows_mimikatz_copywrite by *@fusionrace* from airbnb_binaryalert at https://github.com/Neo23x0/signature-base
ℹ Mimikatz credential dump tool: Author copywrite

⚠ Matches rule Mimikatz_Gen_Strings by *Florian Roth (Nextron Systems)* from thor-hacktools at https://github.com/Neo23x0/signature-base
ℹ Detects Mimikatz by using some special strings

⚠ Matches rule Windows_Hacktool_Mimikatz_674fd079 by *Elastic Security* from Windows_Hacktool_Mimikatz at https://github.com/elastic/protections-artifacts
ℹ Detection for default mimikatz memssp module

⚠ Matches rule Powerkatz_DLL_Generic by *Florian Roth (Nextron Systems)* from gen_powerkatz at https://github.com/Neo23x0/signature-base
ℹ Detects Powerkatz - a Mimikatz version prepared to run in memory via Powershell (overlap with other Mimikatz versions is possible)

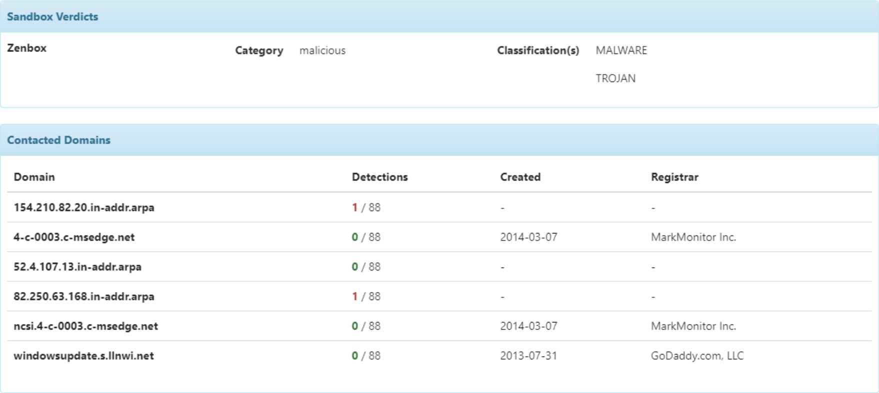
⚠ Matches rule INDICATOR_TOOL_PWS_Mimikatz by *ditekSHen* from indicator_tools at https://github.com/ditekshen/detection
ℹ Detects Mimikatz

⚠ Matches rule HKTL_Mimikatz_SkeletonKey_in_memory_Aug20_1 by *Florian Roth (Nextron Systems)* from gen_mimikatz at https://github.com/Neo23x0/signature-base
ℹ Detects Mimikatz SkeletonKey in Memory

⚠ Matches rule HKTL_Imphashes_Aug22_1 by *Florian Roth* from gen_imphash_detection at https://github.com/Neo23x0/signature-base
ℹ Detects different hacktools based on their imphash

Figure: VirusTotal Report

Analyzer Report: VirusTotal continued



Sandbox Verdicts

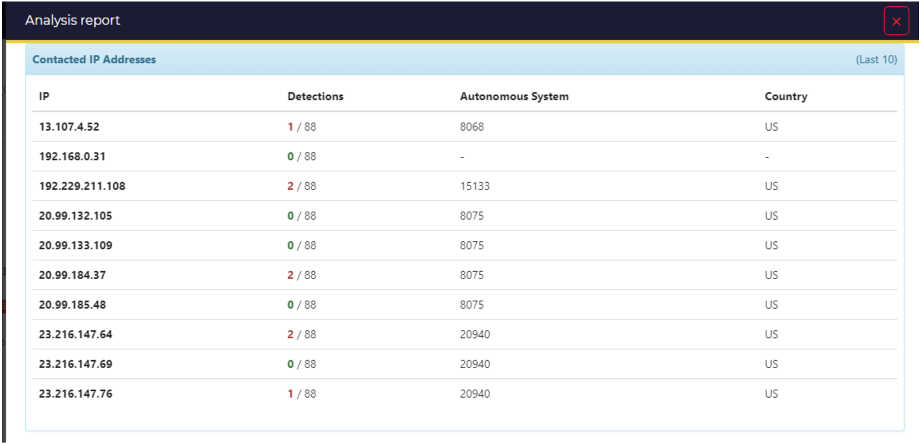
Zenbox **Category** malicious **Classification(s)** MALWARE
TROJAN

Contacted Domains

Domain	Detections	Created	Registrar
154.210.82.20.in-addr.arpa	1 / 88	-	-
4-c-0003.c-msedge.net	0 / 88	2014-03-07	MarkMonitor Inc.
52.4.107.13.in-addr.arpa	0 / 88	-	-
82.250.63.168.in-addr.arpa	1 / 88	-	-
ncsi.4-c-0003.c-msedge.net	0 / 88	2014-03-07	MarkMonitor Inc.
windowsupdate.s.llnwi.net	0 / 88	2013-07-31	GoDaddy.com, LLC

Figure: VirusTotal Report

Analyzer Report: VirusTotal continued



Analysis report

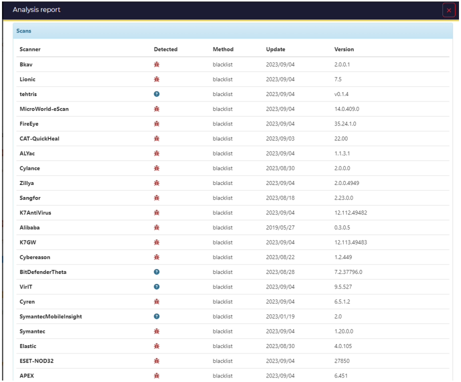
Contacted IP Addresses (Last 10)

IP	Detections	Autonomous System	Country
13.107.4.52	1 / 88	8068	US
192.168.0.31	0 / 88	-	-
192.229.211.108	2 / 88	15133	US
20.99.132.105	0 / 88	8075	US
20.99.133.109	0 / 88	8075	US
20.99.184.37	2 / 88	8075	US
20.99.185.48	0 / 88	8075	US
23.216.147.64	2 / 88	20940	US
23.216.147.69	0 / 88	20940	US
23.216.147.76	1 / 88	20940	US

Figure: VirusTotal Report

Analyzer Report: VirusTotal continued

Here, it is showing the list of different security report website where some of them have already detected and marked this hash as malicious



Analysis report

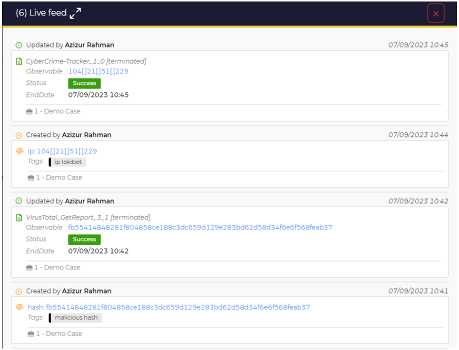
Scans

Scanner	Detected	Method	Update	Version
Bkav	🐞	blacklist	2023/09/04	2.0.0.1
Lionic	🐞	blacklist	2023/09/04	7.5
tehtris	?	blacklist	2023/09/04	v0.1.4
MicroWorld-eScan	🐞	blacklist	2023/09/04	14.0.409.0
FireEye	🐞	blacklist	2023/09/04	35.24.1.0
CAT-QuickHeal	🐞	blacklist	2023/09/03	22.00
ALYac	🐞	blacklist	2023/09/04	1.1.3.1
Cylance	🐞	blacklist	2023/08/30	2.0.0.0
Zillya	🐞	blacklist	2023/09/04	2.0.0.4949
Sangfor	🐞	blacklist	2023/08/18	2.23.0.0
K7AntiVirus	🐞	blacklist	2023/09/04	12.112.49482
Alibaba	🐞	blacklist	2019/05/27	0.3.0.5
K7GW	🐞	blacklist	2023/09/04	12.113.49483
Cybereason	🐞	blacklist	2023/08/22	1.2.449
BitDefenderTheta	?	blacklist	2023/08/28	7.2.37796.0
VirIT	?	blacklist	2023/09/04	9.5.527
Cyren	🐞	blacklist	2023/09/04	6.5.1.2
SymantecMobileInsight	?	blacklist	2023/01/19	2.0
Symantec	🐞	blacklist	2023/09/04	1.20.0.0
Elastic	🐞	blacklist	2023/08/30	4.0.105
ESET-NOD32	🐞	blacklist	2023/09/04	27850
APEX	🐞	blacklist	2023/09/04	6.451

Figure: VirusTotal Report

Live Feed

The observables that are analyzed from TheHive via cortex can be seen by other analysts of the organization through Live Feed. If the analysis is done from Cortex, then it cannot be seen by other analysts. Thus, running analyzers from TheHive provides instant updates to all the analysts which help them to be up-to-date with the case progress.



(6) Live feed

Updated by **Azizur Rahman** 07/09/2023 10:45

CyberCrime-Tracker_1_0 [terminated]
Observable 104[]21[]51[]229
Status Success
EndDate 07/09/2023 10:45
1 - Demo Case

Created by **Azizur Rahman** 07/09/2023 10:44

ip: 104[]21[]51[]229
Tags ip lokibot
1 - Demo Case

Updated by **Azizur Rahman** 07/09/2023 10:42

VirusTotal_GetReport_3_1 [terminated]
Observable fb55414848281f804858ce188c3dc659d129e283bd62d58d34f6e6f568feab37
Status Success
EndDate 07/09/2023 10:42
1 - Demo Case

Created by **Azizur Rahman** 07/09/2023 10:41

hash: fb55414848281f804858ce188c3dc659d129e283bd62d58d34f6e6f568feab37
Tags malicious hash
1 - Demo Case

Figure: Live Feed

Conclusion Remark

Cortex, integrated seamlessly into TheHive, empowers security professionals with a powerful arsenal of analyzers and responders, enhancing the platform's capabilities to detect, investigate, and respond to threats effectively. By harnessing the versatility and extensibility of Cortex, organizations can take their incident response to new heights, bolstering their cyber security posture in an ever-evolving threat landscape.As we wrap up our discussion on Cortex in TheHive, it is clear that this partnership is a game-changer for security teams, empowering them to detect, analyze, and mitigate threats more effectively than ever before.