Security Incident Response with TheHive Project

Cláudia Maia
Masters in Information Security
up201905492@fe.up.pt

Pedro Ferreira
Masters in Information Security
up202209372@fc.up.pt

Rui Gonçalves
Masters in Information Security
up202209376@fc.up.pt

***Abstract*—In order to prevent, detect and know how to handle with cyber attacks, organizations and companies have the need to contract or have a Security Operations Center that works with a computer security incident response team, to deal with problems of security arising from tecnologies. In order to simplify and help the communication between the SOC members, CSIRT and CERT we are going to explore in this project a security incident response platform, named TheHive. This project has the following structure: Introduction (I); TheHive Project (II); Implementation (III); and Conclusion (IV).**

***Index Terms*—Incident Response, SOC, CSIRT, Cybersecurity, Handle events, Analize, Tracking and document.**

I. Introduction

A. SOC:

A Security Operations Center (SOC) is a centralized function that is responsible for enterprise cybersecurity. It employs people, processes, and technology to monitor, prevent, detect, analyze, and respond to cyber threats in real time. SOC teams are in charge of monitoring and protecting the organization's assets (intellectual property, personnel data, business systems, and brand integrity), so they take in telemetry from across an organization's IT infrastructure, including its networks, devices, appliances, and information stores, wherever those assets are. The SOC is usually led by a SOC manager, and may include incident responders, SOC Analysts (tiers 1, 2 and 3), threat hunters (in proactive SOCs) and incident response manager(s). The SOC reports to the CISO (chief information security officer), who in turn reports to either the CIO or directly to the CEO.

B. CSIRT:

A computer security incident response team (CSIRT), is a group of IT professionals that provides an organization (i.e. a SOC) with services and support surrounding the assessment, management and prevention of cybersecurity-related emergencies, as well as coordination of incident response efforts. The main goal of a CSIRT is to respond to computer security incidents quickly and efficiently, thus regaining control and minimizing damage, so SOC staff work close with it to ensure security issues are addressed quickly upon discovery. This involves following National Institute of Standards and Technology's (NIST) four phases of incident response: preparation, detection and analysis, containment, eradication and recovery, post-incident activity. To do so, CSIRTs may take on many responsibilities, including the following: create and update incident response plans; maintain and communicate information to internal and external entities; identify, assess and analyze incidents; coordinate and communicate response efforts; remediate incidents; report on incidents; manage audits; review security policies; and recommend changes to prevent future incidents.

II. TheHive Project

For this project we integrated Elasticsearch, Cortex and TheHive.

Elasticsearch, based on the Lucene library, provides a distributed, multitenant-capable full-text search engine with an HTTP web interface and schema-free JSON documents, to access and search for any stored information.

Cortex is an open source and free software that has been created by TheHive Project for analyzing observables that have been collected, at scale. Observables, such as IP and email addresses, URLs, domain names, files or hashes, can be analyzed individually or in bulk mode using a Web interface, it can also be automated on account of the Cortex REST API.

TheHive is an open source Security Incident Response Platform (SIRP) designed to help and support SOCs, CSIRTs, CERTs and any information security practitioner dealing with security incidents that need to be investigated and acted upon swiftly. It is tightly integrated with MISP (Malware Information Sharing Platform) and can be synchronized with one or multiple MISP instances to start investigations out of MISP events. It can also export an investigation's results as a MISP event to help detect and react to attacks that were already dealt with. Additionally, when TheHive is integrated with Cortex, security analysts and researchers can easily and quickly analyze observables. TheHive is scalable and used to:

- Collaborate: Multiple SOC and CERT analysts can collaborate on investigations simultaneously. TheHive has a built-in live stream that makes real time information of new or existing cases, tasks, observables and IOCs be available to all team members. Special notifications allow users to handle or assign new tasks, and preview new MISP events and alerts from multiple sources such as email reports, CTI providers and SIEMs, so they can then import and investigate them right away.
- Elaborate: Users can create cases and associated tasks using templates made according to their needs, by adding metrics and custom fields (as we are going to demonstrate in the next section). Furthermore analysts can record their progress, attach pieces of evidence, add tags and import

password-protected ZIP archives containing malware or suspicious data without opening them.

- Act: Users can add observables to each case or import them directly from a MISP event or any alert sent to the platform, so they can quickly triage and filter them. Integrating Cortex, and its analyzers and responders, users speed up their investigation and contain threats. As soon as investigations are completed, IOCs are exported to one or several MISP instances.

Thehive has a very intuitive and user friendly platform, to help the platform administrator, this user will be responsible for creating all the users that will have access to the platform. The users in our case were created taking into account the organization of the SOC, Tier1, Tier2, Tier3, SOC Manager, Security Engineers. To share information about alerts they have an alert function or they can receive alerts from an intrusion detection system (IDS), from misp or from logs. Cases can be created from scratch by adding all information manually, entering a title, severity level, date and description. When the case is created the next step is to create tasks for the case where it is described what the task consists of and to whom it is assigned, here comes the importance of the correct creation of users, so that each task is assigned to the responsible user. Thehive has the feature of creating case templates to automate case creation where we can create not just cases but all the tasks that are relevant to that case. These templates come about as a result of alerts that have already occurred and/or common cases.

III. Implementation

For the implementation of our setup with TheHive Project and the required dependencies, we used Docker. Docker is an open-source, container-based technology for automated creation, fast deployment, and reliable execution of software/code that enables building, shipping, and distributing containers into an environment.

Giving our use-case and to easily manage different containers and other configurations we also used the docker-compose tool which helps to define and share multi-container applications with the creation of a YAML file to define the services (with the required configurations) and network allowing us with a single command to instantiate our full environment.

A. TheHive Project

After executing the *docker-compose up* command, the services and network specified in our *docker-compose.yml* file are created and started. The configurations adressed below were all done from TheHive and Cortex web interfaces.

After accesing both web interfaces, first, we must update both cortex and TheHive databases. This ensures that its schema is up-to-date, then retrieves previous data (if any) and update its format for the new schema. Both tools use ElasticSearch to store users, organizations and analyzers configuration. After this first step is completed, we can proceed to create our TheHive Administrator account.

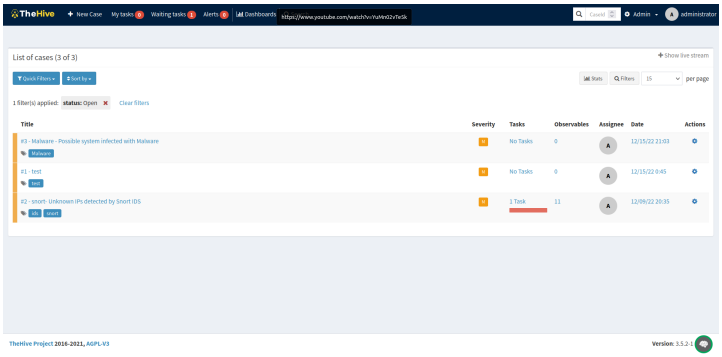

Fig. 1. TheHive Project Interface

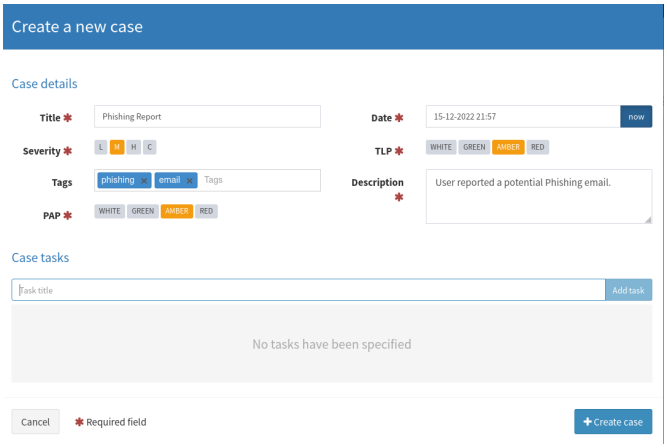

Fig. 2. Phishing case example

This admin account has (by default) read, write and admin roles that enable full control of organizations and users that are added into the platform and also control of the cases that were created by any user. For this reason it is obviously recommended to create multiple accounts with only the needed permissions for each department of the SOC.

After login as Admin into TheHive platform we are presented with the interface in the Fig. 1.

To give an example of a real case in TheHive Project, one is going to be presented next.

In a real scenario it is recommend to have a high number of case templates to, as quickly as possible, create a case from an alert that just appeared in TheHive. The templates created can be directly saved into TheHive, making them available for immediate usage or exported into *json* file format. Another thing to keep in mind is that cases can be continuosly updated, so it is better to first create the case with information collected and, later, update it when new observables are discovered or new tasks that need to be assigned to members of the SOC. For the purpose of this demonstration we are going to show how a case of a possible phishing attempt can be handled.

The case that will be created have the information specified in Fig. 2.

Now that the case is created, tasks can be assigned. Because our example is a phishing attempt, it makes sense to know

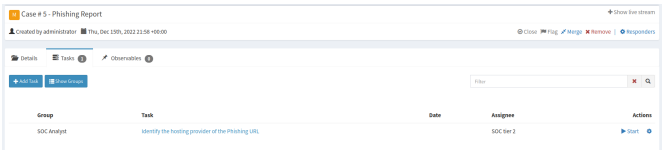

Fig. 3. Task Example of the Phishing case

the hosting provider of the malicious website. A task can be assigned to a SOC Analyst to do this job as it is represented in Fig. 3.

We can also make our case more complete by adding some observables in the observables section. In our case the observables could be the URL of the phishing website or the corresponding IP address.

B. Cortex

Similar to TheHive, Cortex also requires a Administrator account to create and manage multiple organizations, manage the associated users and give them different roles.

According to the official documentation [9], the default cortex organization cannot be used for any other purpose than managing global administrators (users with the superAdmin role), organizations and their associated users. It cannot be used to enable/disable or configure analyzers. Therefore, a new organization must be created as well as some users that belong to the new Organization.

After the new Organization was added, all the cortex following Cortex configurations will be done using one the newly created user that belongs to the organization and has the role *orgadmin*.

Before detailing which Analyzers and how they were configured in Cortex, it is important to explain what they are and what they need to function.

Analyzers allow analysts and security researchers to analyze observables (from TheHive cases for example) and IOCs such as domain names, IP addresses, hashes, files or URLs. Some of this Analyzers require special access while others necessitate a valid service subscription or product license. In our case, the Analyzers implemented required API keys that were obtained in the services websites.

For Cortex being able to run Analyzers, the official documentation [**?**] states that in order to use docker service the docker socket must be bound into Cortex container. Moreover, as Cortex shares files with analyzers, a folder must be bound between them.

Cortex can instantiate docker container by using the docker socket */var/run/docker.sock*. In order to make job file visible to analyzer docker, Cortex needs to know both folders (parameters –job-directory and -docker-job-directory). If all the configurations are setup correctly, cortex will successfully pull an image of the analyzers available in Docker Hub to do the Job reports that will be detailed above.

C. Cortex Analyzers implementation and results

The Cortex Neurons Analyzers that we chose were from VirusTotal and MalwareBazaar. Both of them required an API

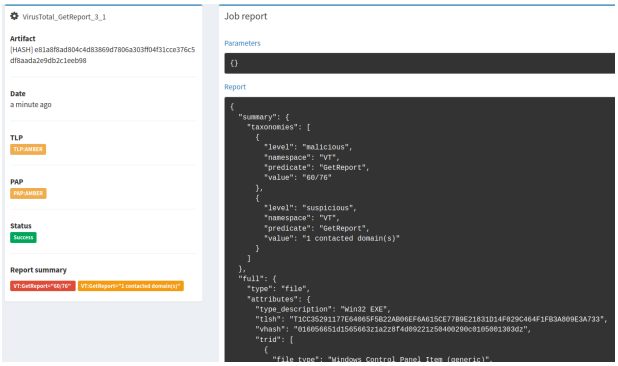

Fig. 4. VirusTotal analyzer report for Hive Ransomware IOC

key (available after creating an account in their websites) to be able to function.

VirusTotal is a platform to analyze suspicious files, domains, IPs, URLs, hashes, and others to detect malware and other breaches, automatically sharing them with the security community. The Cortex program uses VirusTotal API v3 and can run VirusTotal services on the following datatypes: file, hash, domain, Fully Qualified Domain Name (FQDN), IP and URL.

The three enabled Analyzers related to VirusTotal were:

- VirusTotal_GetReport, that gets the latest VirusTotal report for a file, hash, domain or an IP address.
- VirusTotal_Scan, which uses VirusTotal to scan a file or URL.
- VirusTotal_Rescan, that uses VirusTotal to run new analysis on hash.

For the first example, it is used the VirusTotal GetReport Analyzer. The hash provided as input is from Hive ransomware and is in the IOCs section available at [10]. The generated report by Cortex is in Fig. 4.

The job report above provides us some useful insights about the observable that we submitted as input such as the level(indicating that it is indeed malicious), the value, which says how many Security Vendors identified the observable as malicious(in this case, 60/76). The second example (5), the data type provided is an URL (WannaCry IOC [12]) In this example, VirusTotal Job reported the URL as malicious and the Scan made by VirusTotal stated that 7/91 Security Vendors detected the URL as malicious.

MalwareBazaar is a project operated by abuse.ch. The purpose of the project is to collect and share malware samples, helping IT-security researchers and threat analysts protecting their constituency and customers from the most recent cyber threats. Similar to the VirusTotal requirements, to successfully enable this Analyzer an API key is needed. The MalwareBazaar analyzer takes as input an hash and query it's database to try to retrieve useful information about a possible hash that is registered as malicious. An example of the output we get when the MalwareBazaar analyzer finishes running is represented in Fig. 6.

From the job report provided by MalwareBazaar analyzer (Fig. 6), it is possible to see in the summary section that the

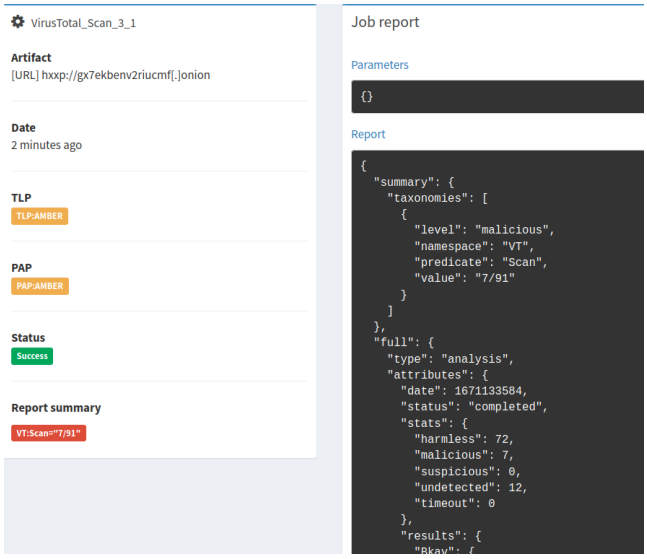

Fig. 5. VirusTotal analyzer report for an WannaCry URL IOC

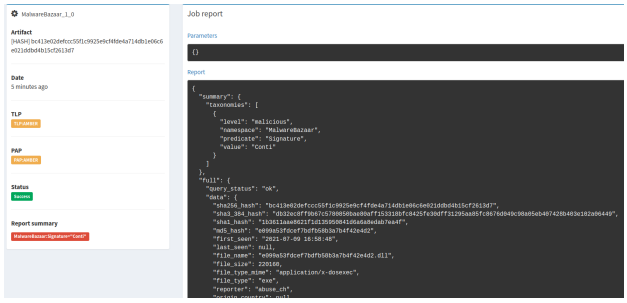

Fig. 6. MalwareBazaar analyzer report for Conti Ransomware IOC

hash provided is malicious and its signature is associated with Conti, a well-known ransomware. Other information such as the date that it was first seen, the file type and the file size are also available in the report. This information can be useful for analysts that will do a further analysis to study the ransomware behaviours.

As we saw in the previous examples, Cortex can be executed as an independent service and the Analyzers complete the jobs normally. However it is possible and advised to, when possible, to integrate it with TheHive. For this integration to be completed, an API key from one of the users within the organization that manages Analyzers is needed. This key can be specified as an environment variable in the docker-compose.yml file. After this is specified, TheHive should now detect Cortex and Analyzers can now be run within TheHive web interface. Fig. 7 is an example of a case that has 3 observables that can serve as inputs for the Analyzers that were configured before.

After running the Analyzers from VirusTotal and MalwareBazaar within TheHive get the summary output represented by Fig. 8. All the observables that were analyzed were flagged as being malicious.

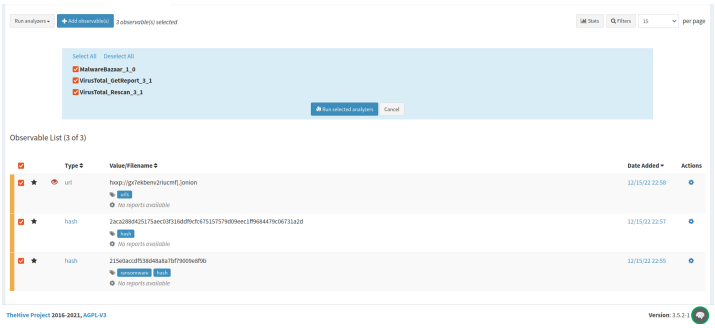

Fig. 7. Preparing Cortex Analyzers to run from TheHive

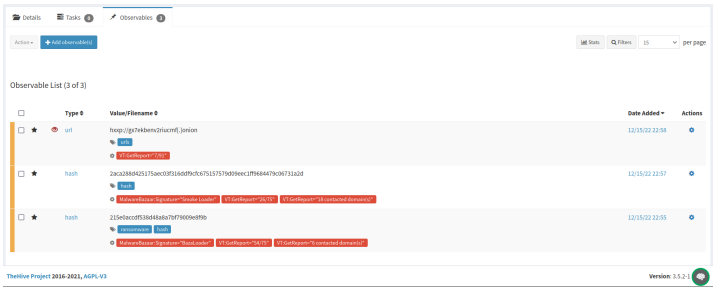

Fig. 8. Output of Analyzers from TheHive

IV. Conclusion

In conclusion, it is notorious that TheHive, is a useful and practical platform, which makes it easy to the SOC team, CERT and CSIRT to communicate and exchange knowledge about the various cases and alerts. This SIRP makes it possible to speed up all the process of analyzing and knowing what we should do to proceed with the eradication and recovery of the machine, from previous cases. Moreover, TheHive can also compile and correlate statistics on cases, tasks, observables, metrics and more to generate useful KPIs (key performance indicator - quantifiable measure of performance over time) and MBOs (Management by Objectives - to manage businesses based on their needs and goals).

References

[1] What Is a Security Operations Center (SOC)? (n.d.). Trellix. https://www.trellix.com/en-us/security-awareness/operations/what-is-soc.html

[2] Habte, F. (2022, May 11). What is SOC (Security Operation Center)? Check Point Software. https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-soc/

[3] What Is a Security Operations Center — Cybersecurity — CompTIA. (n.d.). Default. https://www.comptia.org/content/articles/what-is-a-security-operations-center

[4] SOC as a service. (2022, November 8). Claranet PT. https://www.claranet.pt/cybersecurity/soc-as-a-service

[5] Donegan, K., & Sullivan, P. (2021, March 24). computer security incident response team (CSIRT). WhatIs.com. https://www.techtarget.com/whatis/definition/Computer-Security-Incident-Response-Team-CSIRT

[6] TheHive Project. (n.d.). http://thehive-project.org/

[7] MalwareBazaar - Cortex Neurons documentation. (n.d.). https://thehive-project.github.io/Cortex-Analyzers/analyzers/MalwareBazaar/

[8] VirusTotal - Cortex Neurons documentation. (n.d.). https://thehive-project.github.io/Cortex-Analyzers/analyzers/VirusTotal/

[9] Run Cortex with Docker - TheHive Project Documentation. (n.d.). https://docs.thehive-project.org/cortex/installation-and-configuration/run-cortex-with-docker/
[10] Ozeren, S. (2022, December 12). CISA Alert AA22-321A: Hive Ransomware Analysis, Simulation, TTPs & IOCs. https://www.picussecurity.com/resource/blog/cisa-alert-aa22-321a-hive-ransomware-analysis-simulation-ttps-iocs
[11] CortexDox - Step 4: Create an Organization. (n.d.). https://github.com/TheHive-Project/CortexDocs/blob/master/admin/quick-start.md#step-4-create-an-organization
[12] wannacry-iocs-and-technical-details (n.d.). https://www.criticalstart.com/wannacry-iocs-and-technical-details/