Threat intelligence platform tracking through taking advantage of TheHive platform integrated with Cortex and MISP

***Abstract— Threat intelligence is critical for organizations to identify and prevent potential cyber threats. By using threat intelligence tools, organizations can gain insights into the latest tactics, techniques, and procedures used by cybercriminals. This knowledge allows security teams to stay ahead of the curve and proactively protect their systems and networks from attacks.***

***This project is going to identify the security threats that report on cybersecurity websites or cybersecurity Twitter accounts and collect and filter them based on our needs. Then shows on the dashboard by taking advantage of TheHive project and using cortex and MISP. By implementing this project, we will provide a list of special threats that can be helpful for small businesses that are looking to secure their platforms*.**

INTRODUCTION:

The Internet has become an essential part of our daily lives. However, with the widespread use of the internet, there has been a significant increase in security threats. Malware and virus attacks, phishing attacks, denial of service attacks, and network attacks are some of the most common security threats that internet users face. To mitigate these risks, security analysts and organizations must quickly identify and respond to these threats.

TheHive, Cortex, and MISP are open-source projects that provide a collaborative and powerful security incident response platform. In this proposal, we will outline how we can configure these tools together by using IOCs from cybersecurity websites or cybersecurity Twitter accounts and collect and filter theaters based on our needs then have a report on the dashboard.

OVERVIEW OF PREVIOUS WORKS:

There are several tools and techniques available to identify security threats. Many of these tools use various technologies, such as machine learning, to detect threats. However, the most commonly used tools are the ones that use open-source platforms, such as thehive project, cortex, and MISP.Each tool provides a range of additional services and capabilities that are designed to meet the needs of different organizations and use cases.They have been used both separately and together and evolved gradually regarding features and tasks which could be done more and more.

|  |
| --- |
| XXX-X-XXXX-XXXX-X/XX/$XX.00 ©20XX IEEE |

Thehive project is a collaborative incident response tool that allows analysts to track and respond to security threats in real-time. The tool can integrate with various security solutions and provides a single point of view to analyze and track incidents. However, individually it lacks Cortex's analytical power. The capacities of cortex to carry out automatic analysis and response to security situations have received increased attention.

Cortex is a companion analysis engine for TheHive, providing a range of powerful tools for threat intelligence analysis. It can be used to automate the enrichment and analysis of observables, such as IP addresses, domains, and files. Cortex integrates with various third-party tools and services, allowing analysts to quickly gather additional information on potential threats.

MISP is intended to make it easier for security experts to share indicators of compromise (IOCs). Enhancing user rolebased access control and two-factor authentication, among other security and privacy features of MISP has been done more frequently.

All of these tools have been used extensively in the industry to identify and mitigate security threats. However, there is a need for a more comprehensive approach that integrates these tools to provide a holistic view of security threats.

OBJECTIVES:

The objective of this proposal is to demonstrate how we can use TheHive Project, Cortex, and MISP to:

* gathering IoCs (Indicators of Compromise) such as malicious IP addresses, domain names, file hashes, and patterns of suspicious behavior
* Collect and store threat intelligence data
* Identify security threats
* Filter and sort threats and data that needed
* Exhibit the identified threats on a dashboard

METHODOLOGY:

To achieve our objectives, we will integrate TheHive, Cortex, and MISP to collect and store threat intelligence data and identify security threats on the internet. TheHive will act as the central incident response platform, Cortex will automate threat intelligence gathering, and MISP will act as the central repository for threat intelligence data. The following steps will be taken to achieve our objectives:

1. Configuring TheHive involves several steps, including setting up the server, installing TheHive, and configuring the necessary components such as Docker.
2. Configure MISP: MISP will be configured to store threat intelligence data. First should setup docker and configuring MISP.
3. Configuring Cortex involves several steps, including setting up the server, installing Cortex, and configuring the necessary components for Cortex to function properly.
4. Integrate TheHive with MISP: TheHive will be integrated with MISP to allow security analysts to access and utilize threat intelligence data and share data with other entities.
5. Analyze threats: When potential threats are identified, Cortex will automatically gather threat intelligence data to identify the nature of the threat.
6. Filter threat intelligence data: The identified threat intelligence data will be stored in MISP.
7. Display threat intelligence data on a dashboard: The identified threats and associated threat intelligence data will be displayed on a dashboard for security analysts to review.

Conclusion

The proposed approach of using thehive project, cortex, and MISP to identify and list security threats on a dashboard is a comprehensive and effective approach to threat detection. By automating threat intelligence gathering and storing threat intelligence data, security analysts will have access to a

wealth of information that will enable them to respond to incidents quickly and efficiently. The dashboard will provide an at-a-glance view of the identified threats, allowing security analysts to prioritize their response efforts. Many small businesses struggle to protect themselves from cyber threats due to limited resources and a lack of cybersecurity expertise, resulting in a growing number of successful attacks and data breaches, organizations can stay informed about the latest threats and take timely action to mitigate the risks. This approach can be used by organizations of all sizes to improve their security posture and protect against the everincreasing number of security threats in the digital age.

VII. Project weekly schedule

REFERENCES:

1. Danjoux, B., Poth, A., Frere, R., Milanese, M. R., Baere, K. D., Bossiroy, G., Tischer, S., & Nixon, R. (2023, February 10). NVISO Labs. Retrieved February 21, 2023, from https://blog.nviso.eu/
2. YouTube. (2020, March 20). Leveraging TheHive &amp; Cortex for automated IR. YouTube. Retrieved February 21, 2023, from https://www.youtube.com/watch?v=K6K1fNpbf9w
3. *TheHive project#*. TheHive Project Documentation. (2022, March 15). Retrieved February 21, 2023, from https://docs.thehiveproject.org/
4. *Joshua Wright*. SANS Institute. (2023, January 4). Retrieved February 21, 2023, from https://www.sans.org/webcasts/leveragingthehive-cortex-automated-ir-113265/

# Appendix A: Manual/ Implementation

About the threat intelligence tools, we tried to install thehive first, however as it needs considerable resources like RAM , We encountered some problems. Then we figured out to use cloud server as the alternative. After checking them out based on our needs, We finally could find an Azure server and setup Azure subscription and virtual network.

Then Created ubuntu VM, set firewall inbound ports. After that we found out we need to install a hypervisor like docker, to setup thehive on it and finally could be able to install thehive.

Why thehive ver5