How do we detect threats?

Jaden Martin

***Abstract*—This study observes the multiple methods of threat detection systems in today's society in cybersecurity. More importantly, this study focuses on their functionalities as well as their techniques for implementation. By analyzing different facets of cybersecurity systems today through scholarly papers and evaluations conducted of the systems, this research aims to educate and compare the differences of each system as well as their relevance in the cybersecurity infrastructure.**

Keywords—network security, threat detection systems, cybersecurity, cyber threats

I. Introduction

Throughout the recent times of the cybersecurity world, the display of events and occurrences revolved around system vulnerabilities and exploitations have presented new challenges that demand state of the art threat detection systems to combat these issues before they happen. Threat detection systems implement unique algorithms and techniques to observe and mitigate potential risks by malicious individuals. In order to understand how relevant these techniques are to the cybersecurity infrastructure, a proper explanation of the different areas of detections as well as the types and how they contribute to mitigating risks is needed.

II. Background of threat detection systems

A. *The Early Days of Threat Detection*

Initially, threat detection methods included signature-based techniques to combat risks. This type of method utilized past situations patterns to match with present threats to detect them. This became irrelevant with the implementation of zero-day attacks and advanced persistent threats, which thrive on the unknown factors of vulnerabilities within software or hardware systems.

B. *Recent Growth in Threat Detection*

As technology and innovations grew, the techniques that proved inefficient in the past towards known and unknown threats became clearer with the implementation of AI-based detection as well as machine learning detection and anomaly detection, which all stem on the use of deviations/inconsistencies within the system to predict future threats.

III. Threat Detection Techniques and methods

Within the confines of threat detection come the varied techniques that separate one from another. There are methods that can be used to provide adequate protection and potential exploitation from hackers and malicious individuals.

A. *Foundational Tools*

These techniques are the basis behind our cybersecurity infrastructure, as they create the backbone for detecting and mitigating cyber threats [1].

- Intrusion Detection Systems (IDS): This type of system monitors network traffic to determine in inconsistencies or uncommon behavior in the system itself. Since IDS is a combination of networked based IDS and host-based IDS, it is able to monitor the system as well as alert the administrator or organization of any events efficiently and effectively[1].
- Intrusion Prevention Systems (IPS): this type of system stems off the capabilities of the prior detection system IDS. They are the brawn out of the two systems and its main priority is to try to halt or distract the malicious actor from making any actions through the use of blocking and ethical hacking attacks[1].

B. *Network Security*

Network Security is the bodyguard of the digital world. They use the wide range of tools and assets within the digital space to prevent and protect network infrastructure.

- Firewalls: Firewalls monitor the traffic of incoming and outgoing data and communications. They ensure that the integrity of the data within the network is being transferred safely and discretely so that third parties can not interfere or modify data. The three most common types of firewalls are packet filters, connection tracking, and application firewalls.

- Security Information and Event Management (SIEM): This type of network management involves an effective analysis of host and communications within an organization's infrastructure [2]. SIEM has operations that utilize multiple sources of events through advanced analytics to identify and use patterns to respond to incidents.

C. *Endpoint Detection*

Endpoint Detection and Response was created to protect specific endpoints from hackers. Host such as computers and mobile devices are protected through these types of systems, and they strive on nonstop monitoring of endpoint activities to respond to incidents in real time [1].

D. *Advanced Detection*

- Anomaly Detection: This type of detection system focuses on user activity and deviation patterns to determine potential development of risks before it even starts. It uses algorithms to establish different behaviors within the system, and it focuses on factors like resource allocation changes and abnormal user actions and patterns to trigger further investigation into potential risk. It also utilizes signature based mechanisms to aid it in these challenges[2].

- Honeypots: This detection system serves as a decoy for malicious actors to distract and deviate attackers from the right path. It simulates assets that look appealing to the attacker, and if contacted with by the attacker, the honeypot sends an alert signal to the administrator or organization to dig deeper into the interaction and potential risk [1].

E. *Threat Intelligence*

Threat Intelligence provides organizations with a surefire way of identifying emerging threats.

Conclusion

This paper explored the varied techniques of modern day detection systems and methods of protected against hackers. By exploring the comparisons between each method and technique, we displayed out each method contributed to the overall growth of the cybersecurity infrastructure.

References

[1] EC-Council University."How Can Companies Detect a Potential Cyber Attack."eccu.edu. Accessed Dec. 5, 2024. [Online.] Available: https://www.eccu.edu/blog/methods-technologies-detect-cyber-attacks/

[2] DeVry University. "9 Essential Cyber Security Tools and Techniques."devry.edu. AccessedDec. 5. 2024. [Online.] Available: https://www.devry.edu/blog/cyber-security-tools-and-techniques.html#firewalls

[3]

Identify applicable funding agency here. If none, delete this text box.