Exploring Advanced Threat Hunting Techniques to Enhance Cyber Security Defences

Tija P Thomas[1], Ravindra M[2], Alok Ranjan[3], Prasanna Kumara[4]
[1] Assistant Professor, Govt. First Grade College for Women, Balmatta, Mangaluru
[2] Lecturer, Govt. First Grade College for Women, Balmatta, Mangaluru
[3] Assistant Professor, Canara College of Engineering, Benjanapadavu, Mangaluru
[4] Assistant Professor, Moodlakatte Institute of Technology, Kundapura

Abstract: In the rapidly evolving landscape of cyber security, organizations are increasingly turning to advanced threat hunting techniques to stay ahead of sophisticated cyber threats. By proactively seeking out and neutralizing potential threats before they can cause harm, businesses can significantly enhance their cyber security defences. This paper explores the key advanced threat hunting techniques that organizations can leverage to reinforce their security posture, the methods through which these techniques can enhance cyber security defences, and the challenges that come with their implementation.

Index Terms: **cyber security, threat hunting, threat intelligence, cyber-attack.**

I. INTRODUCTION

One of the primary advanced threat hunting techniques involves leveraging threat intelligence to proactively identify potential threats. Threat intelligence provides organizations with valuable insights into emerging threats, malicious actors, and attack vectors, allowing them to pre-emptively defend against potential cyber-attacks. By continuously monitoring and analyzing threat intelligence feeds, organizations can stay informed about the latest cyber security trends and proactively adjust their security strategies to mitigate risks. Another crucial technique is conducting behavioral analytics to detect anomalous activities within the network.[1]

Behavioral analytics involve monitoring user and entity behavior to identify deviations from normal patterns. By establishing baselines of typical behavior and using advanced analytics tools to detect deviations, organizations can uncover potential insider threats, compromised accounts, or unauthorized access attempts that traditional security measures might miss. Additionally, organizations can implement machine-learning algorithms for pattern recognition to enhance their threat hunting capabilities.[2] Machine learning algorithms can analyze vast amounts of data to identify patterns, trends, and anomalies that human analysts may overlook. By training machine learning models on historical data and continuously refining them with new information, organizations can improve their ability to detect and respond to emerging threats in real-time.

To enhance cyber security defences, organizations can develop custom scripts for automated threat detection and response. These scripts could be automated routine security tasks, such as log analysis, threat detection, and incident response, allowing security teams to focus on more strategic activities. By customizing scripts to their specific security needs and environment, organizations can improve their incident response times and mitigate the impact of cyber-attacks. Furthermore, utilizing SandBoxing techniques can help organizations analyze suspicious files and applications in a controlled environment.[3]

SandBoxing involve isolating potentially malicious files or executables in a virtual environment to observe their behavior without risking the security of the production network. By analyzing the actions of suspicious files in a SandBoxed environment, organizations can better understand their intent and potential impact, enabling more effective threat mitigation strategies. Moreover, implementing network segmentation is another effective way to enhance cyber security defences.[4] Network segmentation involves dividing the network into smaller, isolated segments to contain and isolate potential threats. By restricting lateral movement within the network and implementing access controls between segments, organizations can limit the spread of malware and unauthorized access, reducing the overall attack surface and minimizing the impact of security incidents.[5]

Despite the benefits of advanced threat hunting techniques, organizations face several challenges when implementing them. One significant challenge is overcoming limitations in data visibility and analysis. With the proliferation of data sources and the complexity of modern IT environments, the organizations often struggle to aggregate, correlate, and analyze the vast amount of data generated by their systems and applications. This can hinder their ability to detect and respond to advanced threats effectively.[6]

Another challenge is addressing the shortage of skilled cyber security professionals proficient in advanced threat hunting techniques. As the demand for cyber security expertise continues to outstrip supply, organizations find it challenging to recruit and retain qualified professionals with the necessary skills and experience to implement and manage advanced threat hunting tools and technologies. This skills gap can impede organizations' ability to effectively leverage advanced threat hunting techniques to enhance their cyber security defences.[7]

Furthermore, ensuring compatibility and integration with existing security infrastructure poses a significant challenge for organizations adopting advanced threat hunting techniques. Integrating new tools and technologies with legacy security systems and architectures can be complex and time -consuming, requiring careful planning and coordination to avoid disruptions to existing security operations. Incompatibility issues can hinder the seamless deployment and operation of advanced threat hunting solutions, limiting their effectiveness in strengthening cyber security defences.[8]

II. PRELIMINARY WORK

Traditional Threat Hunting involves reacting to alerts and security incidents. Advanced threat hunting goes beyond that, assuming a proactive stance to unearth hidden threats creep around within the network. Here are some key techniques employed by advanced threat hunters:[11]

A. Hunting based on Indicators of Compromise (IoCs): This technique involves searching for specific signatures or artifacts linked to known malware or attacker tools. Threat hunters can leverage Security Information and Event Management (SIEM) systems and threat intelligence feeds to hunt for IoCs.

B. Hunting based on Indicators of Attack (IoAs): IoAs focus on behaviors that might signal malicious activity. This includes things like unusual login attempts, unauthorized data access, or suspicious file transfers. IoA hunting requires a deeper understanding of attacker Tactics, Techniques, and Procedures (TTPs) as mentioned in the frameworks such as MITRE ATT&CK. By analyzing behaviors, IoA hunting can identify novel threats that haven't yet been flagged by traditional security solutions.

C. Hypothesis-Driven Hunting: This technique involves formulating a hypothesis about a potential threat based on intelligence or current events. The hunter then gathers data and logs to test the hypothesis and determine if there's evidence of malicious activity.

D. Custom Hunting Queries: Advanced threat hunters can craft custom queries to search through network traffic, system logs, and other data sources for suspicious patterns or anomalies. Security Orchestration, Automation, and Response (SOAR) platforms can be helpful in automating these queries.

E. Advanced Analytics and Machine Learning: Security analysts can leverage Machine Learning (ML) and advanced analytics to detect subtle anomalies in network traffic or user behavior that might be missed by manual investigation.

In addition to these techniques, threat hunters also need a strong understanding of attacker mindsets and the latest hacking trends to stay ahead of the curve.

III. METHODOLOGY

Advanced threat hunting techniques are vital for enhancing cyber security defences. These proactive measures involve actively searching for signs of malicious activity within a network, rather than relying solely on automated tools and alerts. Below are some key techniques and strategies:

A. Behavioral Analysis:

Behavioral analysis involves monitoring the typical behavior of users and systems within a network. By establishing a baseline of normal activity, deviations can be quickly identified as potential threats.

a. User and Entity Behavior Analytics (UEBA): This technique uses Machine Learning to understand normal behavior and identify anomalies that may indicate malicious activity.
b. Endpoint Detection and Response (EDR): EDR tools collect data from endpoints (like computers and mobile devices) to detect, investigate, and respond to threats.

B. Threat Intelligence Integration:

Integrating threat intelligence involves using external data on known threats to enhance detection capabilities.

a. Indicators of Compromise (IOCs): Information such as malicious IP addresses, file hashes, and domain names can be used to identify and block threats.
b. Tactics, Techniques, and Procedures (TTPs): Understanding the methods used by attackers helps in anticipating and identifying new threats.

C. Advanced Analytics and Machine Learning:

Advanced Analytics and Machine Learning are used to analyse large volumes of data to identify patterns and predict future threats.

a. Anomaly Detection: Machine Learning algorithms can detect unusual patterns that may indicate a breach.
b. Predictive Analytics: By analyzing historical data, predictive models can forecast potential future attacks.

D. Deception Technologies:

Deception technologies involve creating traps and decoys to detect and analyze attackers.

a. Honeypots: Fake systems set up to attract attackers and study their methods.
b. Honey Tokens: Decoy data planted in real systems to detect unauthorized access.

E. Threat Hunting Frameworks

Using structured frameworks helps in systematically approaching threat hunting.

a. MITRE ATT&CK: A comprehensive knowledge base of adversary tactics and techniques based on real-world observations.
b. Cyber Kill Chain: A model that outlines the stages of a cyber-attack, helping to understand and disrupt the attacker's progress.

F. Endpoint and Network Forensics

Endpoint and Network Forensics involve deep dive into system and network activity logs to uncover hidden threats.

a. Log Analysis: Reviewing system and network logs to identify suspicious activities.
b. Memory Forensics: Analyzing the volatile memory (RAM) of endpoints to detect malware that operates in-memory.

G. Proactive Incident Response:

Proactive incident response involves preparing for incidents before they occur, ensuring rapid and effective action when they do.

a. Playbooks: Predefined response strategies for various types of incidents.
b. Red Teaming: Simulated attacks by security experts to test and improve defenses.

H. Collaboration and Sharing

Collaboration within the cyber security community enhances threat detection and response.

a. Information Sharing and Analysis Centers (ISACs): Industry-specific groups that share threat intelligence.
b. Open Source Tools: Utilizing and contributing to open source cyber security tools and frameworks.

I. Continuous Improvement:

Threat hunting is an ongoing process that requires continuous learning and adaptation.

a. Regular Training: Keeping the security team updated with the latest threat hunting techniques and tools.
b. Post-Incident Reviews: Learning from past incidents to improve future defences.

IV. CONCLUSION

Advanced Threat Hunting Techniques offer organizations a proactive approach to cyber security that can significantly enhance their defences against evolving cyber threats. By leveraging threat intelligence, behavioral analytics, machine learning algorithms, and other advanced techniques, organizations can detect and respond to threats more effectively, reducing the risk of security incidents and data breaches.

However, the challenges of data visibility, skills shortage, and integration complexities must be addressed to fully realize the benefits of advanced threat hunting techniques. Through strategic investments in technology, talent development, and process optimization, organizations can overcome these challenges and establish robust cyber security defences that protect their critical assets and operations.

V. REFERENCE

[1]. Nour B, Pourzandi M, Debbabi M. A survey on threat hunting in enterprise networks. IEEE Communications Surveys & Tutorials. 2023 Aug 14.

[2].Takey YS, Tatikayala SG, Samavedam SS, Eswari PL, Patil MU. Real time early multi stage attack detection. In 2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS) 2021 Mar 19 (Vol. 1, pp. 283-290). IEEE

[3].Akinsola JE, Olajubu EA, Aderounmu GA. Development of Threat Hunting Model Using Machine Learning Algorithms for Cyber Attacks Mitigation. In2022 International Conference on Computational Science and Computational Intelligence (CSCI) 2022 Dec 14 (pp. 1010-1015). IEEE.

[4].Oosthoek K, Doerr C. Cyber threat intelligence: A product without a process? International Journal of Intelligence and Counter Intelligence. 2021 Apr 3;34(2):300-15.

[5].Faruk MJ, Shahriar H, Valero M, Barsha FL, Sobhan S, Khan MA, Whitman M, Cuzzocrea A, Lo D, Rahman A, Wu F. Malware detection and prevention using artificial intelligence techniques. In2021 IEEE International Conference on Big Data (Big Data) 2021 Dec 15 (pp. 5369-5377). IEEE.

[6] Sun N, Ding M, Jiang J, Xu W, Mo X, Tai Y, Zhang J. Cyber threat intelligence mining for proactive cybersecurity defense: a survey and new perspectives. IEEE Communications Surveys & Tutorials. 2023 May 5

[7].Zoppi T, Ceccarelli A, Bondavalli A. Unsupervised algorithms to detect zero-day attacks: Strategy and application. Ieee Access. 2021 Jun 21; 9:90603-15.

[8] .Razaulla S, Fachkha C, Markarian C, Gawanmeh A, Mansoor W, Fung BC, Assi C. The age of ransomware: A survey on the evolution, taxonomy, and research directions. IEEE Access. 2023 Apr 19

[9].Aldauiji F, Batarfi O, Bayousef M. Utilizing cyber threat hunting techniques to find ransomware attacks: A survey of the state of the art. IEEE Access. 2022 Jun 8;10:61695-706.

[10].Pourahmadi V, Alameddine HA, Salahuddin MA, Boutaba R. Spotting anomalies at the edge: Outlier exposure-based cross-silo federated learning for ddos detection. IEEE Transactions on Dependable and Secure Computing. 2022 Nov 25.

[11].Khakurel U, Rawat DB. Real-Time Physical Threat Detection on Edge Data Using Online Learning. IEEE Consumer Electronics Magazine. 2023 Mar 14.

[12].Ali W, Malebary S. Particle swarm optimization-based feature weighting for improving intelligent phishing website detection. IEEE Access. 2020 Jun 19;8:116766-80.

[13].Khan MN, Ara J, Yesmin S, Abedin MZ. Machine learning approaches in cybersecurity. InData Intelligence and Cognitive Informatics: Proceedings of ICDICI 2021 2022 Feb 1 (pp. 345-357). Singapore: Springer Nature Singapore.

[14]. Islam S, Hayat MA, Hossain MF. ARTIFICIAL INTELLIGENCE FOR CYBERSECURITY: IMPACT, LIMITATIONS AND FUTURE RESEARCH DIRECTIONS.

[15]. Ahsan M, Nygard KE, Gomes R, Chowdhury MM, Rifat N, Connolly JF. Cybersecurity threats and their mitigation approaches using Machine Learning—A Review. Journal of Cybersecurity and Privacy. 2022 Jul 10;2(3):527-55

[16]. Akhtar MS, Tao F, Zhang J. The future of artificial intelligence in cybersecurity: a comprehensive survey. EAI Endorsed Transactions on Energy Web. 2021;9(1):12-20.

[17]. von der Assen J, Celdrán AH, Luechinger J, Sánchez PM, Bovet G, Pérez GM, Stiller B. Ransomai: Ai-powered ransomware for stealthy encryption. InGLOBECOM 2023-2023 IEEE Global Communications Conference 2023 Dec 4 (pp. 2578-2583). IEEE.