IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 4, April 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204156 |

Threat Hunting as a Method of Protection against Cyber Threats

Dr. V. Rama Krishna, Konderu Abhinav Varma, Shaik Mahaboob Akram,

Vootkuri Sai Nithin Reddy

Assistant Professor, Department of CSE, Anurag University, Hyderabad, India

UG Student, Department of CSE, Anurag University, Hyderabad, India

UG Student, Department of CSE, Anurag University, Hyderabad, India

UG Student, Department of CSE, Anurag University, Hyderabad, India

ABSTRACT: This paper presents the structuring of a new approach to countering cyber threats – Threat Hunting. This concept is proactive threat search, mainly a manual process with elements of automation, in which the analyst uses his knowledge and skills to check large amounts of information for indicators of compromise, according to a predetermined hypothesis of the presence of a threat. All key elements of Threat Hunting approach were explained as well as functional diagram for a deep understanding and application of this approach in practice by specialists in the field of cybersecurity was proposed in the paper.

KEYWORDS: Threat Hunting, indicators of compromise, proactive cybersecurity, cyber threat.

I. INTRODUCTION

To date, most information security threats are known, and can be defended by traditional means of protection such as antivirus, firewalls, and so on. Such threats include spam, denial-of-service attacks, viruses, rootkits, and other classic malware. The remaining minority of threats are unknown and the most dangerous. They are difficult to detect and even more so to protect against them. Examples of such threats are encryption viruses, crypto miners, etc.

In a company with organized information security management processes, the majority of the risk of known threats can be resolved with a traditional risk management approach: avoid, accept (accept possible financial or image losses), reduce (implement the necessary protection) or transfer (for example, to a service provider). Instead, protecting against zero-day vulnerabilities, targeted attacks, phishing, supply chain attacks, and a large number of other attacks is much more difficult. The consequences of these threats will be much more serious than the consequences of spam or viruses, from which modern anti-virus software is quite able to protect.

This situation has led to the development of means of protection against cyber threats in the direction of developing new technology that would be able to counteract the most serious and complex threats.

Proactive threat search or Threat Hunting (hereinafter – TH) is the latest way to counter cyberattacks, which through proactive and iterative search, allows to detect complex threats that traditional means of protection are not even able to notice. It should be noted that TH is not a specific software or hardware product and is not a passive activity. Proactive threat search is, first of all, mainly a manual process with elements of automation, in which the analyst, based on his knowledge and skills, checks large amounts of information for indicators of compromise, according to a predetermined hypothesis of the presence of a threat. Due to the fact that this concept is relatively new in the field of cybersecurity, it is advisable to explain it from the opposite, that is, to describe what this process is not in order to avoid confusion of concepts and technologies.

II. RELATED WORK

In some related works that could provide valuable insights and context for a project on Threat Hunting as a Method of Protection Against Cyber Threats:

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204156 |

"The Pyramid of Pain: A Model for Prioritizing Cyber Threat Intelligence" by David J. Bianco: This paper introduces the concept of the Pyramid of Pain, which categorizes indicators of compromise (IOCs) based on their level of difficulty for adversaries to change or evade. Understanding this model can help in developing effective threat hunting strategies.

"Hunting and Gathering in the Cyber Swamp" by Richard Bejtlich: Bejtlich is a prominent figure in the field of threat hunting. This book provides practical guidance on establishing and improving threat hunting capabilities within an organization, including methodologies, tools, and case studies.

"Enterprise Security Architecture: A Business-Driven Approach" by John Sherwood, Andrew Clark, and David Lynas: While not specifically focused on threat hunting, this book provides a comprehensive overview of designing and implementing security architectures. Understanding the broader context of security architecture can help in integrating threat hunting into an organization's overall security strategy.

"Practical Threat Intelligence and Data-Driven Threat Hunting" by Junaid Islam and Omar Santos: This book covers the fundamentals of threat intelligence and its application in threat hunting. It provides practical techniques for leveraging threat intelligence feeds, analyzing data, and proactively hunting for threats within an organization's network.

"Blue Team Handbook: Incident Response Edition" by Don Murdoch: Although primarily focused on incident response, this handbook offers valuable insights into the tactics, techniques, and procedures (TTPs) commonly used by attackers. Understanding adversary behaviors is crucial for effective threat hunting.

"The Practice of Network Security Monitoring" by Richard Bejtlich: Another work by Bejtlich, this book focuses on network security monitoring (NSM) techniques, which are closely related to threat hunting. It covers topics such as network traffic analysis, log collection and analysis, and the use of NSM tools for detecting and responding to security incidents.

III. PROPOSED METHOD

Threat hunting is not a one-size-fits-all approach; rather, it requires a systematic and well-defined methodology tailored to the organization's specific needs and resources. The proposed method consists of several key steps:

Firstly, it is crucial to define clear objectives and scope. This involves identifying the assets and data critical to the organization, understanding the potential threats they face, and establishing specific goals for threat hunting activities. Objectives may include identifying advanced persistent threats (APTs), detecting insider threats, or uncovering unknown vulnerabilities. Next, extensive data collection and analysis are essential components of threat hunting. This process involves gathering data from various sources within the organization's network and systems, such as logs, network traffic, and endpoint telemetry. The collected data is then analyzed to identify anomalous behavior and indicators of compromise (IOCs) that may indicate the presence of a threat. Once potential threats have been identified, threat hunters employ a variety of techniques and tools to investigate further. This may include conducting in-depth analysis of suspicious activity, correlating disparate data sources to uncover hidden threats, and leveraging threat intelligence to gain insights into the tactics, techniques, and procedures (TTPs) of potential adversaries.

Throughout the investigation process, collaboration and communication are critical. Threat hunters work closely with various stakeholders, including security analysts, incident responders, and IT personnel, to share information, validate findings, and coordinate response efforts. This collaborative approach ensures that all relevant expertise and resources are leveraged effectively to address identified threats. Finally, threat hunting is an iterative process that requires continuous refinement and improvement. Organizations should regularly review and update their threat hunting methodologies in response to evolving threats, changes in the organization's infrastructure, and lessons learned from previous hunts. By adopting a proactive stance and continually refining their threat hunting capabilities, organizations can enhance their resilience to cyber threats and better protect their critical assets and data. In conclusion, threat hunting offers a proactive defense strategy that complements traditional security measures by enabling organizations to identify and neutralize threats before they escalate into full-blown incidents. By following a systematic methodology tailored to their specific needs, organizations can leverage threat hunting as a powerful tool for enhancing their cyber defense capabilities and staying one step ahead of adversaries in today's dynamic threat landscape.

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204156 |

IV. SIMULATION RESULTS

Let's delve deeper into the scenario by considering a medium-sized financial institution located in a metropolitan area. The institution serves a diverse clientele, ranging from individual account holders to small businesses and corporate entities. Due to the nature of its operations, the institution handles sensitive financial data, including personal and corporate account information, transaction records, and proprietary trading data. The institution's cybersecurity team, led by a dedicated threat hunting unit, implements a robust methodology for conducting threat hunts. They start by defining clear objectives aligned with the organization's risk profile and business priorities. Objectives may include detecting insider threats, identifying external attackers targeting financial data, or uncovering vulnerabilities in critical systems. To scope the threat hunts effectively, the team collaborates with stakeholders across the organization, including IT personnel, network administrators, and business unit leaders. Together, they identify the critical assets, systems, and data repositories that require protection.

Once the objectives and scope are defined, the threat hunting team collects and analyzes data from various sources within the institution's network and systems. This includes network traffic data captured by intrusion detection systems (IDS) and firewall logs, endpoint telemetry from antivirus and endpoint detection and response (EDR) solutions, and server logs from critical infrastructure components.

During a routine threat hunting exercise, the team detects unusual network traffic patterns originating from an employee's workstation in the finance department. Upon closer inspection, they identify indicators of compromise (IOCs) associated with a known malware variant used by cybercriminals to exfiltrate sensitive data. Further investigation reveals that the malware had infiltrated the workstation through a phishing email disguised as a routine internal communication. Once inside the network, the malware attempted to escalate privileges and establish communication with an external command-and-control server. Thanks to the proactive monitoring and detection capabilities enabled by threat hunting, the cybersecurity team swiftly responds to contain the threat. They isolate the infected workstation from the network, disable compromised user accounts, and deploy endpoint security updates to prevent further propagation of the malware. Additionally, the threat hunting team conducts a thorough post-incident analysis to identify gaps in existing security controls and enhance detection and response capabilities. They share their findings with relevant stakeholders and implement targeted security awareness training to educate employees about phishing threats and best practices for email hygiene.

In this elaborated scenario, the simulation results underscore the importance of threat hunting as a proactive defense strategy for safeguarding sensitive financial data against cyber threats. By leveraging a systematic methodology and collaborative approach, organizations can detect and mitigate threats in real-time, reducing the risk of data breaches, financial losses, and reputational damage. Threat hunting not only enhances the organization's cybersecurity posture but also fosters a culture of resilience and continuous improvement in the face of evolving cyber threats.

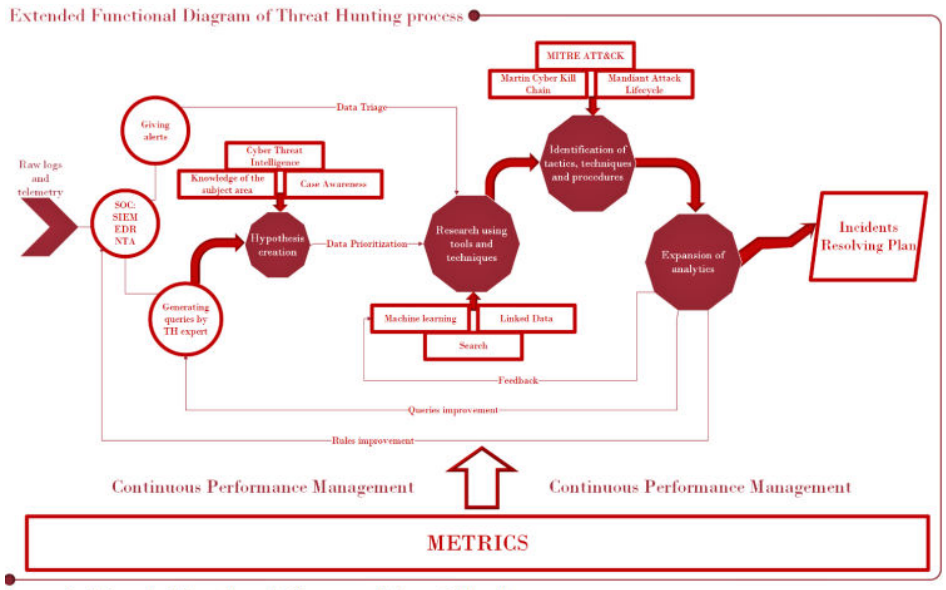

Figure 1: Extended Functional Diagram of Threat Hunting process

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204156 |

V. CONCLUSION AND FUTURE WORK

In this paper the structuring of a new approach to countering cyber threats – Threat Hunting, was presented. This study shows that TH is an effective method of modern cyber threat countering for organizations at a high level of maturity, that already have their own SOC or use such services through outsourcing and are ready to move to the level of proactive threat response. The main purpose of the paper is achieved – a functional diagram of Threat Hunting approach is proposed and the following objectives are solved: enrichment of the existing TH model with SOC analytics tools, queries improvement and continuous performance measurement is proposed; a triad of the most important SOC tools is proposed for the effective implementation of the analytics stage; the process of converting raw logs and telemetry from network and infrastructure assets of the organization into structured queries for conducting TH is proposed and clarified; the place of cyber threat intelligence at the stage of hypothesis creation is determined as a small part of the whole process of TH, which helps to disseminate effective information about threats by understanding the motives, capabilities and methods of attackers to inform about measures to reduce cybersecurity; the examples of effective metrics or KPIs to evaluate TH are proposed; the incidents resolving plan is proposed as an ultimate goal of the TH, which helps to fit it into the existing process of incident management process, which is an integral part of the organization's overall information security management process.performance.

REFERENCES

[1] R. van Os, M. Bakker, R. Bouman, "TaHiTI Threat Hunting Methodology", FI-ISAC NL Publication, version 17.12.2018, 2018.
[2] "Detecting the Unknown: A Guide to Threat Hunting, Home Office Digital, Data and Technology, version 2.0, 2019.
[3] A. Chuvakin, "How to Hunt for Security Threats", Gartner, Inc., 2017.
[4] D. Akacki, "5 types of Threat Hunting", Sqrrl Data
[5] D. Akacki, D. Bianco, R. Bejtlich, "Huntpedia: Your Threat Hunting Knowledge Compendium", Sqrrl Data, 2018.
[6] White paper: A Framework for Cyber Threat Hunting, Sqrrl Data, 2018.
[7] R. Lee, D. Bianco, "Generating Hypotheses for Successful Threat Hunting", SANS Institute, 2016.
[8] MITRE ATT&CK Framework, 2020.
[9] S. Schmitt, F. I. Kandah and D. Brownell, "Intelligent Threat Hunting in Software-Defined Networking", 2019 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 2019, pp. 1-5, doi: 10.1109/ICCE.2019.8661952.
[10] M. Iavich, S. Gnatyuk, E. Jintcharadze, Y. Polishchuk, A. Fesenko and A. Abisheva, "Comparison and Hybrid Implementation of Blowfish, Twofish and RSA Cryptosystems", Proceedings of 2019 IEEE 2nd Ukraine Conference on Electrical and Computer Engineering (UKRCON), Lviv, Ukraine, 2019, pp. 970-974.
[11] M. N. S. Miazi, M. M. A. Pritom, M. Shehab, B. Chu and J. Wei, "The Design of Cyber Threat Hunting Games: A Case Study", 2017 26th International Conference on Computer Communication and Networks (ICCCN), Vancouver, BC, 2017, pp. 1-6, doi: 10.1109/ICCCN.2017.8038527.
[12] K. Wafula and Y. Wang, "CARVE: A Scientific Method-Based Threat Hunting Hypothesis Development Model", 2019 IEEE International Conference on Electro Information Technology (EIT), Brookings, SD, USA, 2019, pp. 1-6, doi: 10.1109/EIT.2019.8833792.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details