International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Maximizing Cyber Security Through Threat Hunting for Advanced Threat Detection and Mitigation

Mohammed Mustafa Khan

Abstract

Threat hunting is the future of proactive cyber defense. It has emerged as the fundamental solution to counter sophisticated attacks. Threat hunting is not a relatively new technology. It existed in the past when security analysts utilized manual processes to examine various data to create hypotheses pertaining to possible threats using vulnerability know-how and experience to hunt threats. The advancement of threats has forced the security operational center teams to automate their hunting tools and models and to adopt the best practices to detect and mitigate advanced threats. Machine learning and artificial intelligence technologies are infused to make threat hunting more efficient and effective. To have a common ground for understanding threat hunting, a basic definition is needed. Threat hunting is the prescient effort of identifying signals of malicious activity in the IT infrastructure that have evaded underlying security controls. Threat hunting relies on the formulation of an objective-driven hypothesis and is an iterative process. Organizations strive to protect their assets and reduce possible damages. This research paper discusses threat hunting as one of the promising technologies that can help organizations proactively secure their IT infrastructure.

Keywords: Threat hunting, threat detection, IT infrastructure

1.0 Introduction

In today's hyperconnected world that drives the digital economy, organizations are bombarded with a multitude of cybersecurity incidents emanating from internal and external threats, mounting a lot of pressure on the IT and security teams. Cyber threats are becoming pervasive, and the adversaries hidden behind the scenes are sophisticated. Organizations need to keep up with the pace and stay ahead of threats by employing proactive techniques that help to protect their IT infrastructure. Traditional security tools and approaches can no longer have the capabilities to secure data in the era of advanced threats [7]. Threat hunting holds a promising future as the next industrial revolution. It is an active approach to cyber defense compared to traditional protection approaches like intrusion detection and prevention systems, isolation of malicious programs in sandboxes, and firewalls. Cyber threat hunting entails proactively investigating organizational IT infrastructure for advanced threats that have dodged traditional security controls. Threat hunting aims to keep track of and dismantle cyber adversaries as soon as possible in the sequence of attack and to enhance the agility and precision of organizational responses.

1.1 Research Problem

Conventional detection methods, like signature-based and predefined rules, are becoming untenable in discovering advanced threats, and they use reactive approaches. The threat landscape has evolved to avoid the legacy methods of detection. Attackers identify the weak spots in a system and exploit these

vulnerabilities without being noticed until they execute malicious code that harms and damages the organizational IT infrastructure, which results in reputational damage and financial and compliance incidents. This paper aims to address the challenge of how organizations can enhance their cybersecurity posture to detect and mitigate these advanced threats with efficacy.

1.2 Research Objectives

This paper aims to:

- Explore the concept of threat hunting and its importance in modern cybersecurity.
- Explore the tools, technologies, and frameworks used in threat hunting.
- Expound on effective implementation of threat hunting program.

This paper is structured to include a proper understanding of threat hunting, threat hunting tools, technologies, and frameworks, implementation of an effective threat hunting program, mitigation strategies for advanced threats, and future trends in the field of cybersecurity.

2.0 Understanding Threat Hunting

Threat hunting is an active process that is conducted by a cybersecurity professional that involves the formulation of hypotheses to drive their investigations into possible threats. There are various types of hunting processes, including indicator-driven hunting and intelligence-driven hunting. However, the common type that is used by cybersecurity professionals is hypothesis-driven hunting since it has proven to be the best in discovering advanced threats that evade traditional security measures. Threat hunting does not single-handedly conduct the hunting process. It involves the use of tools, technologies, frameworks, and processes to successfully detect advanced threats before they cause harm to the IT infrastructure [3].

Threat hunting process involves data collection, formulation of a hypothesis, active hunting, and response. Security tools such as SIEM collect data from heterogeneous sources and store it in a single log file. Cybersecurity professionals, like security analysts, utilize the data collected to formulate hypotheses pertaining to potential threats and search for any indicators of compromise (IoC) [3]. The IoC simply means there is something amiss in the system, such as unregistered entries being added to the system. The indicators of attack reveal some information, such as attempts by an entity to login to the system, which becomes a concern to the security analyst. The intelligence feeds will help the security analyst to discover certain types of vulnerabilities that are being exploited. The vulnerability scans on the environment will show the analyst what the attacker is targeting. The intelligent hunter who has experience utilizes all the aforementioned details, experience, and intuitions to connect the dots and evaluate the threats. Once the threats have been detected, appropriate remedies are employed to mitigate the threats [3].

3.0 Threat Hunting Tools and Technologies

Threat hunting leverages the use of threat detection solutions to accomplish its task. Threat detection is a method that is designed to discover cyber security threats that are actively trying to break into the company's IT infrastructure [4]. It utilizes specialized systems that generate a response when anomalous activity is detected. Threat hunters utilize the data collected by threat detection systems to formulate their hypotheses. Effective hunting requires specialized tools and technologies, including:

- SIEM and SOAR: SIEM (Security Information and Event Management) collects data and alerts the security operation center team, while SOAR (Security Orchestration, Automation Response) automates and orchestrates the response to those alerts [4].

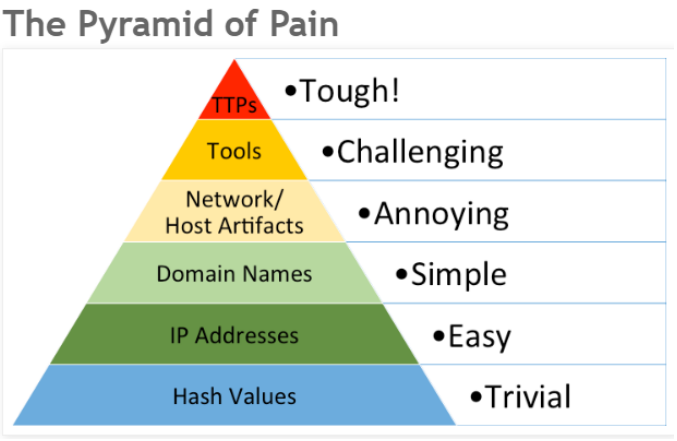
- EDR, EPP, and XDR: EDR (Endpoint Detection and Response) detects and responds to endpoint threats, while EPP (Endpoint Protection Platform) prevents them. XDR (Extended Detection and Response) extends these capabilities across the entire infrastructure, providing a holistic view [4].
- UEBA and UEM: UEBA (User and Entity Behavior Analytics) detects behavioral anomalies, and UEM (Unified Endpoint Management) ensures that all devices are securely managed and compliant with security policies [4].
- Network Traffic Analysis (NTA): Analyzes network traffic in real-time to identify anomalous behavior that indicates potential threats [4].

4.0 Threat Hunting Framework

There are different types of threat-hunting frameworks, including the pyramid of pain, cyber kill chain, and MITRE ATT&CK [8]. The framework is the roadmap that guides the threat hunters during the hunting process. Understanding and proper application of these frameworks enables threat hunters to effectively detect and interrupt any action initiated by attackers. The attackers end up giving up on their mission or decide to create other tactics, techniques, and procedures, which will be discovered by the threat hunters again to counteract them. This shows threat hunting is indeed a continuous and iterative process. If the threat hunter sleeps on the job and fails to hunt for the threats, there is a possibility of attackers gaining access to the IT infrastructure.

4.1 Pyramid of Pain

The concept of the pyramid of pain can be borrowed to guide threat hunters. It was developed by David Bianco. Pyramid of pain is a cybersecurity concept that demonstrates the increasing level of difficulty attackers experience as defenders (Threat hunters) disrupt their activities with ease. The pyramid categorizes indicators of compromise (IoC) that threat hunters can discover and disrupt [8]. Each layer of the pyramid represents various types of IOC.



Brief Description of Each Level of Pyramid of Pain

Pyramid of Pain	Explanation
Hash Values (Bottom Level)	These are unique identifiers for specific files. Changing hash values is easy for attackers, making this the least impactful disruption [9].

IP Addresses	Identifying and blocking IP addresses associated with malicious activity can be a nuisance for attackers, but they can quickly switch to new ones [9].
Domain Names	Attackers need to register and configure new domains, which requires more effort, making this a bit more painful to counter [9].
Network/Host Artifacts	These are specific patterns or behaviors on a network or host that indicate an attack. Changing these requires altering the attack's operational methods, which increases the difficulty for the attacker [9].
Tools	When defenders identify and disrupt specific tools used by attackers, the attackers must find or develop new tools, causing significant pain [9].
Tactics, Techniques, and Procedures (TTPs) (Top Level)	These are the overall strategies and methods attackers use. Changing TTPs requires rethinking the entire attack strategy, making this the most disruptive and painful level for attackers [9].

4.2 Cyber Kill Chain

Developed by Lockheed Martin to comprehend and distort the stages of cyber-attack [10]. It outlines the number of steps that attackers take to accomplish their mission. This concept has been borrowed by threat hunters to learn, discover, and interrupt these phases, thus stopping the attack from being executed.

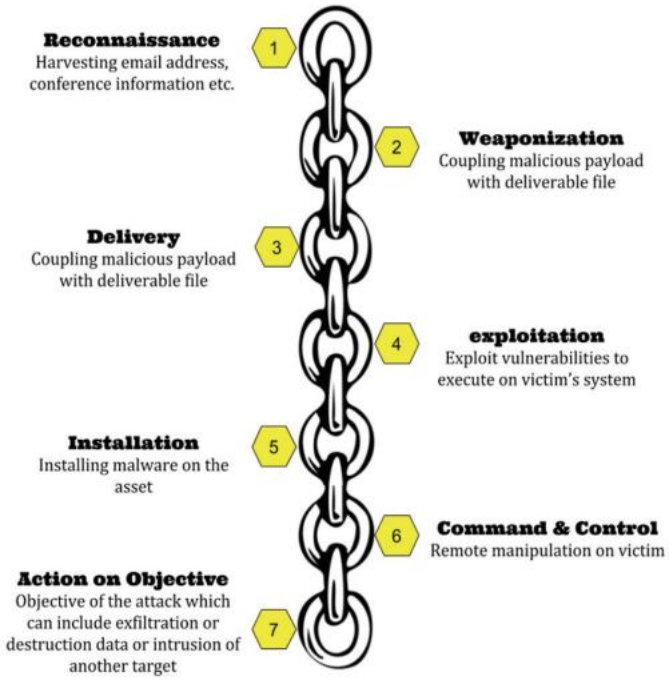


Table Showing a Description of Cyber Kill Chain

Cyber Kill Chain	Explanation
Reconnaissance	Attackers gather information about their target. Threat hunters look for signs of scanning, probing, or other intelligence-gathering activities [10].
Weaponization	Attackers develop a payload (e.g., malware) tailored to exploit the target. Threat hunters search for signs of payload preparation or delivery mechanisms [10].

Delivery	The payload is sent to the target, typically via email, websites, or direct network attacks. Threat hunters monitor for unusual traffic or suspicious files entering the network [10].
Exploitation	The payload is executed, exploiting a vulnerability [10]. Threat hunters focus on detecting and analyzing attempts to exploit known or unknown vulnerabilities.
Installation	The attacker installs malware or backdoors on the target system [10]. Threat hunters watch for indicators of unauthorized software installation or persistence mechanisms.
Command and Control (C2)	The attacker establishes a communication channel with the compromised system [10]. Threat hunters track outbound traffic and detect connections to known malicious C2 servers.
Actions on Objectives	The attacker achieves their goal, such as data exfiltration, encryption (ransomware), or destruction [10]. Threat hunters analyze behavior patterns to detect and prevent the attack before this stage is reached.

4.3 MITRE ATT&CK Framework

It is a worldwide accessible knowledge base of adversary tactics and techniques dependent on real-world observations [8]. The ATT&CK knowledgebase serves as a blueprint to develop particular threat models and methodologies in various domains like cybersecurity. The major purpose of this framework is to make the Internet a safe haven for each entity. It is an open-source framework that can be accessed by any individual. Threat hunters maximize the use of these frameworks since they show how attackers behave at various stages of an attack.

MITRE ATT&CK	Explanation
Tactics and Techniques Identification	Threat hunters use the ATT&CK framework to map out the specific tactics and techniques that attackers might use in different phases of an attack [8]. This helps identify what to look for during a hunt.
Gap Analysis	The framework allows threat hunters to assess their current detection capabilities by comparing them against the known TTPs listed in ATT&CK [8]. This helps identify gaps in security controls and detection mechanisms.
Threat Intelligence Integration	Threat hunters can integrate threat intelligence with the ATT&CK framework to understand how adversaries are operating. This helps in developing more effective hunting hypotheses and strategies [8].
Incident Response	By using the ATT&CK framework, threat hunters can quickly identify the techniques used in an attack and determine the next steps to contain and mitigate the threat [8].
Adversary Emulation	ATT&CK also supports creating adversary emulation plans for red teaming exercises, helping organizations understand how well they can detect and respond to specific threats [8].

5.0 Implementing an Effective Threat Hunting Program

Effective implementation of threat-hunting programs requires organizations to develop a proactive mindset when dealing with advanced threats. It is critical to augment the tricks used by attackers to launch

attacks [1]. Arguably, the roots of effective threat hunting literally are not contained in the knowledge of attack techniques. However, they can be found in situational awareness and visibility. The aim of an effective hunting program should be centered on the following factors;

- The initial focus is to discover previously unknown or ongoing threats across the IT environment.
- Gain a proper understanding of the IT environment.

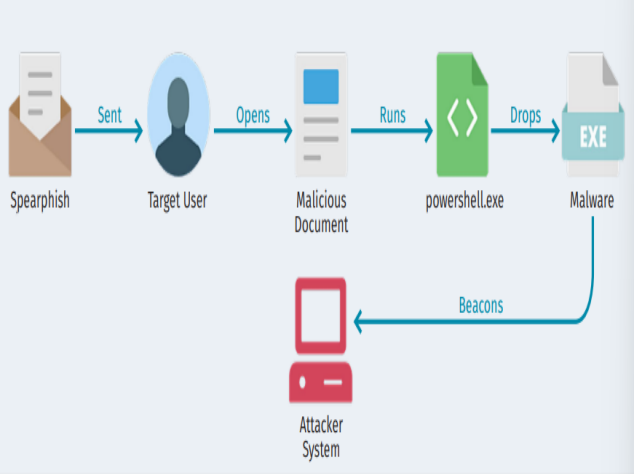
It is a tremendous aspect to bridge the gap between the two aforementioned factors during the hunting process.

5.1 The Importance of Threat Hunting

It is crucial to determine the goals and objectives of the hunting process. Any hunting program should focus on these two factors: presciently identifying threats to limit exploitation by an attacker and mastering the organizational and technical environment. Sometimes attackers have gained access to the system, but the security alarm tools have not triggered an alert to notify the security team. The attacker proceeds to position itself in a place where security solutions can no longer detect it. Hunting with intention will enable the threat hunters to discover hidden breaches and establish appropriate incident response and remediation strategies [1].

Hunting with clarity provides a clear visibility of the organizational IT infrastructure environment [1]. It is crucial for the hunting team to properly understand the environment to enable them to conduct a successful hunt exercise. Exploring the environment will enable the hunting team to utilize the available tools, frameworks, and processes to implement an effective hunting program.

Diagram showing spearphishing and malware dropping



From the diagram, a user receives an email with malicious intent. The user opens the email without noticing it has a suspicious program. The opened email executes a PowerShell code that embeds a malicious program on the system. This malware runs and notifies the attacker it has successfully infected the system [1]. From this use case, threat hunters can create intuitions and generate the following points as potential red flags to start the threat-hunting process.

- Additional unregistered file entries
- Unusual modification of files
- Attempt to open connections to suspicious servers
- Hidden processes identification that conducts network callouts to unknown network locations

- PowerShell executes to download suspicious processes.

These spots are based on visibility and situational awareness that threat hunters may use. There are various ways to gain intuitions and insights into the data. It is important for threat hunting teams to utilize all the tools, technologies, and frameworks to implement an effective threat hunting program.

6.0 Mitigation of Advanced Threats

6.1 Implementation of Cybersecurity Standards and Frameworks

It is crucial to adopt cybersecurity standards and frameworks to remediate advanced threats. Some of these strategies include the Center for Internet Security (CIS) Control and the NIST Cybersecurity Frameworks [6]. CIS Controls is known as a foundational framework for improving security hygiene and minimizing the attack surface. CIS Controls has 18 controls and 153 safeguards. It is essential to prioritize controls and safeguards relevant to advanced threats to interrupt cyber threats before they are initiated by cybercriminals. For instance, CIS Control number three speaks on data protection, and Safeguard 3.8 discusses how encryption of sensitive data can help protect sensitive company data, such as intellectual property. Additionally, the NIST Cybersecurity Frameworks provide a high-level view of the organizational security landscape. The aspects such as identifying, protecting, detecting, and responding used by these frameworks provide windows of opportunities for threat hunters to counter advanced threats unleashed by cybercriminals.

6.2 Zero-Trust Architecture

Zero-Trust architecture is a technology that helps to prevent the lateral spread of advanced threats. The Zeto-trust works only one principle: any traffic that an end device receives has to be verified before allowing it to proceed. It can not trust any traffic or request presented until it verifies and validates if an activity is legitimate [5]. If the activity is suspected to be malicious, the appropriate alerts are triggered to notify the security team that anomalous activity is percolating the system. The security team responds by screening and scrutinizing the activity to countermeasure the activity. Additionally, the suspicious activity is automatically blocked and redirected to sandboxes for further evaluation by the threat hunting team.

7.0 Future Trends

7.1 Quantum Computing in Cybersecurity

Quantum computing promises to transform cybersecurity. In the era of big data, quantum computers provide advanced computational power that can analyze the sheer amount of data and improve the accuracy of threat detection [2]. However, it remains a threat to the field of cryptography since quantum computing is a threat to encryption, which is the digital shell that protects many top secrets. Extensive scientific research must be performed that goes beyond post-quantum cryptography to protect sensitive data from emerging quantum threats.

8.0 Conclusion

Threat hunting represents a continuous battle between cybersecurity professionals and attackers. Basically, it can be referred to as "a leap and frog game." To stay ahead of the game, organizations need to utilize expert threat hunters, superior tools, and procedures to design new, efficient, and effective operational cybersecurity practices. Threat hunting is a crucial component of modern cybersecurity, providing advanced threat detection and mitigation capabilities that are essential in today's threat landscape. By proactively searching for and neutralizing threats that evade traditional security measures,

threat hunting helps organizations stay ahead of sophisticated adversaries. As cybersecurity threats continue to evolve, the role of threat hunting will only become more critical. Organizations must invest in threat hunting practices and tools to maximize their cybersecurity efforts and protect against emerging threats.

9.0 Reference:

1. M. Bromiley, "Thinking like a Hunter: Implementing a Threat Hunting Program," *Sans.org*, Apr. 2019. https://www.sans.org/media/analyst-program/thinking-hunter-implementing-threat-hunting-program-38923.pdf
2. A. Kudrati, C. Peiris, and B. Pillai, "Modern Approach to Multi-Cloud Threat Hunting," *IEEE Xplore*, Jun. 2022. https://ieeexplore.ieee.org/abstract/document/9946821
3. A. Bhardwaj and S. Goundar, "A framework for effective threat hunting," *Network Security*, vol. 2019, no. 6, pp. 15–19, Jun. 2019, doi: https://doi.org/10.1016/s1353-4858(19)30074-1.
4. A. Bolla and F. Talentino, "Threat Hunting driven by Cyber Threat Intelligence," *webthesis.biblio.polito.it*, Apr. 13, 2022. https://webthesis.biblio.polito.it/22631/
5. F. Kramer, M. Teplinsky, R. Butler, and C. Statecraft, "Cybersecurity for Innovative Small and Medium Enterprises and Academia," Jan. 2022. Available: https://www.atlanticcouncil.org/wp-content/uploads/2022/01/Cybersecurity-for-Innovative-Small-and-Medium-Enterprises-and-Academia.pdf
6. S. Sumitra, "An Analysis of Cybersecurity for Business Enterprises," *ERA*, Mar. 26, 2022. https://era.library.ualberta.ca/items/45502949-ac87-4e55-89e2-2bebf9c5d05e
7. P. Gao *et al.*, "Enabling Efficient Cyber Threat Hunting With Cyber Threat Intelligence," *arXiv.org*, Oct. 25, 2020. https://arxiv.org/abs/2010.13637
8. "Cyber Threat Hunting Workshop," Nov. 2020. Available: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/CyberDrill-2020/Cyber%20Threat%20Hunting%20Workshop%20-%20ITU%2019112020.pdf
9. R. Daszczyszak, D. Ellis, S. Luke, and S. Whitley, "Sponsor: USCYBERCOM TTP-Based Hunting," Mar. 2019. Available: https://www.mitre.org/sites/default/files/2021-11/prs-19-3892-ttp-based-hunting.pdf
10. P. Nikkhah Bahrami, A. Dehghantanha, T. Dargahi, R. Parizi, R. Choo, and H. Javadi, "Cyber Kill Chain-Based Taxonomy of Advanced Persistent Threat Actors: Analogy of Tactics, Techniques, and Procedures," *Journal of Information Processing Systems*, vol. 15, no. 4, Aug. 2019, doi: https://doi.org/10.3745/JIPS.03.0126.