Designing Effective Threat Hunting to Enhance Security Programs

ASSOUJAA ISMAIL
Faculté des Sciences Dhar El Mahraz,
Université Sidi Mohamed Ben AbdellahThis link is disabled.,
Fez,
MOROCCO
https://orcid.org/0000-0001-8572-5593

Abstract: Cyber threat hunting is a proactive cybersecurity approach focused on identifying threats that evade traditional security measures. It involves the integration of human expertise, data analytics, and advanced tools to detect anomalies within organizational networks and systems. Despite its potential, many organizations remain dissatisfied with their threat hunting programs due to gaps in required analytical skills and the lack of integration of advanced techniques such as machine learning. This paper explores the design of an effective threat hunting exercise, examining its role in complementing traditional security measures. It emphasizes the importance of advanced data analytics, threat intelligence integration, and automation to enhance the effectiveness of threat hunting. The proposed framework underscores the significance of the data collection and analysis process, improving detection rates and reducing the impact of advanced threats. This study also addresses the challenges faced in threat hunting, including skills gaps and the need for better tools, and outlines strategies for overcoming these obstacles to create more robust security programs.

Keywords: Threat hunting, Frameworks, Security

Received: May 13, 2024. Revised: November 5, 2024. Accepted: December 7, 2024. Published: December 30, 2024.

1. Introduction

Organizations today are confronted with increasingly complex and sophisticated cyber threats. Traditional cybersecurity measures, such as firewalls and intrusion detection systems (IDS), often struggle to keep pace with the rapidly evolving tactics, techniques, and procedures (TTPs) employed by adversaries. This has led to the rise of cyber threat hunting, a proactive approach to identifying threats that may bypass conventional defenses. Unlike reactive incident response measures, which rely on predefined rules or alerts, threat hunting actively seeks out potential indicators of compromise (IoCs) by leveraging both human expertise and machine intelligence.

At its core, threat hunting involves continuous monitoring, analysis, and defense against cyber threats through the collection of data from various sources, including network traffic, endpoint logs, and threat intelligence feeds. As adversaries increasingly adopt automated and adaptive malware, organizations must evolve their defensive strategies to address these emerging risks. Effective threat hunting provides critical visibility and situational awareness, enabling security teams to detect threats that might otherwise go unnoticed. However, several challenges such as insufficient machine intelligence, the need for real-time data analysis, and the knowledge gap regarding new and emerging threats pose significant barriers to the success of threat hunting programs.

This paper explores the essential components of an effective threat hunting strategy, with a focus on the integration of advanced analytics techniques. It also highlights the need for organizations to enhance their threat hunting capabilities by addressing skill gaps in both data analysis and cybersecurity expertise. By adopting a proactive, threat-hunting-centric approach, organizations can reduce their attack surface, improve incident response times, and strengthen their overall security posture against both known and unknown threats.

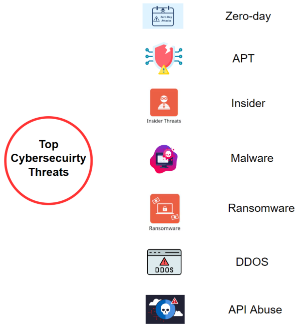
The paper is organized as follows: Section 2 discusses threat types and identification. Section 3 outlines the requirements for effective threat hunting. Section 4 examines the threat hunting framework and strategies for mitigation. Finally, Section 5 concludes the paper.

2. Threat Types and Identification

Organizations face a wide range of threats that vary in complexity, stealth, and impact. Identifying and understanding these threats is essential for effective threat hunting, a proactive process that seeks out malicious activities before they can inflict significant damage. This section explores the types of threats faced by organizations and the methodologies employed in threat identification.

2.1 Types of Threats

Threats can be classified into various categories, depending on the TTPs employed by attackers. These threats can range from well-known methods like phishing to more advanced threats, such as zero-day exploits and advanced persistent threats (APTs). Key types of threats that often challenge threat hunters include:



- Zero-Day Vulnerabilities: These are security flaws in software that are unknown to the vendor or have not yet been patched. Zero-day exploits take advantage of these vulnerabilities, allowing attackers to breach systems before defenses are in place. Since they are novel and lack predefined signatures, they often bypass traditional defenses, making proactive threat hunting critical for detection.
- Advanced Persistent Threats: APTs involve stealthy, prolonged cyberattacks, often orchestrated by well-funded and sophisticated adversaries. They target high-value assets, remaining undetected for extended periods by avoiding overt disruption and focusing on data exfiltration. Threat hunters need advanced techniques, such as behavior analysis, to uncover these threats.
- Insider Threats: These threats arise from individuals within an organization, such as employees, contractors, or partners, who have access to sensitive systems. Whether malicious or accidental, insider threats are difficult to detect using conventional security tools, as they originate from trusted users. Behavioral monitoring and anomaly detection are essential in identifying these threats.
- Malware and Ransomware: While malware encompasses various malicious software designed to damage or disrupt systems, ransomware specifically encrypts files and demands payment for their decryption. Threat hunting focuses on detecting unusual file system activity, such as unauthorized encryption or deletion of large volumes of data, to mitigate ransomware attacks.
- Distributed Denial of Service (DDoS) Attacks: DDoS attacks overwhelm network resources by flooding them with traffic, rendering services unavailable. While traditional defenses focus on mitigating these attacks as they happen, proactive threat hunting can help identify unusual traffic patterns early, enabling preemptive action.
- API Abuse: APIs are integral to modern applications but can be vulnerable to exploitation. Threat hunters can focus on detecting anomalies in API traffic, such as abnormal call frequencies or unauthorized access attempts, to preempt attacks that exploit API weaknesses.

2.2 Threat Identification

Identifying threats requires a comprehensive approach that integrates multiple data sources and analysis techniques. The effectiveness of threat identification is significantly enhanced when threat hunters combine human expertise with automated tools. Below are some key methodologies employed in identifying threats:

Pattern Recognition framework:

1) Identify Relevant Sources
2) Data Collection: Gather data from different sources
3) Baseline Establishment: Define Normal Behavior, Pattern Learning
4) Analyze Data
5) Spot Unusual Behavior Using Threat Intelligence
6) Anomaly Detection: Detect Deviations, Correlate Events
7) Contextualization: Contextual Analysis, Cross-Check with Baseline
8) Incident Confirmation: Validate Findings, Generate Hypotheses, Give the Impact
9) Response and Mitigation: Trigger Incident Response, Mitigate Threats

Threat hunters begin by identifying relevant data sources and gathering logs, network traffic, and other system data. They establish a baseline by defining normal behavior and using pattern learning techniques. Once the baseline is set, they analyze the collected data to spot unusual behavior, often leveraging threat intelligence for enhanced detection. Anomalies are detected by identifying deviations and correlating events. These deviations are then contextualized by cross-checking with the baseline and analyzing their potential impact. If malicious activity is suspected, the findings are validated, hypotheses are generated, and the potential impact is assessed. In confirmed cases, the threat hunting team triggers incident response and mitigates the threat.

User Behavior Analytics (UBA) framework:

1) Data Collection
2) Baseline Establishment
3) Behavior Analysis
4) Anomaly Detection
5) Incident Confirmation
6) Response and Mitigation

User Behavior Analytics (UBA) begins with data collection, where user activities are monitored and logged from various sources, including login records and application usage. Next, a baseline is established by analyzing typical user behavior, allowing the system to understand what constitutes normal activity. Once the baseline is set, the behavior analysis phase involves continuously examining user actions to identify any deviations from the norm. Anomaly detection is a critical component, flagging unusual behaviors, such as logins from unfamiliar locations or access attempts at odd hours, as potential security threats. If any anomalies are identified, incident confirmation follows, where findings are validated to determine if they indicate insider threats or compromised accounts. In cases where malicious activity is confirmed, the UBA system triggers a response and mitigation process to address the threat effectively.

Threat Intelligence Integration framework:

1) Data Collection
2) Threat Intelligence Acquisition
3) Correlation Analysis
4) Anomaly Detection
5) Contextualization
6) Incident Confirmation
7) Response and Mitigation

The Threat Intelligence Integration framework begins with data collection, where network behavior data is gathered from various sources, including logs and alerts. This is followed by threat intelligence acquisition, which involves obtaining relevant threat intelligence feeds that provide IoCs and insights into known threats. Next, correlation analysis is performed to match observed network behaviors with the IoCs and TTPs identified in the threat intelligence feeds. This step enhances anomaly detection, allowing threat hunters to identify malicious activities more effectively by recognizing behaviors that align with previously identified threats. Once anomalies are detected, contextualization occurs, where the context of the correlated behaviors is analyzed to determine their severity and potential impact. If malicious activity is suspected, incident confirmation is conducted to validate the findings and assess the risk they pose to the organization. In confirmed cases, the framework triggers a response and mitigation process, implementing appropriate actions to address the threat effectively. This comprehensive integration of threat intelligence enables faster and more accurate detection of potential security threats.

Real-Time Monitoring framework:

1) Setup Monitoring Tools
2) Data Collection
3) Event Correlation
4) Suspicious Activity Detection
5) Alert Generation
6) Incident Response Activation
7) Reporting and Documentation

The Real-Time Monitoring framework begins with setting up monitoring tools, where Security Information and Event Management (SIEM) platforms and other relevant tools are implemented across the network and endpoints. Following this, data collection is initiated, involving the continuous gathering of information from various sources, including logs, network traffic, and endpoint activities. Once data is collected, event correlation takes place, where the incoming data is analyzed to identify patterns and relationships among different activities in real time. This analysis is crucial for suspicious activity detection, enabling threat hunters to identify potentially harmful behaviors as they occur. When suspicious activities are detected, alert generation is activated to notify security teams of the anomalies, prompting immediate attention. This leads to incident response activation, where predefined procedures are initiated to investigate and mitigate any confirmed security threats. Finally, reporting and documentation are essential components of the framework, as they ensure that all detected incidents and responses are recorded, providing valuable insights for future monitoring efforts and improving overall threat detection capabilities. This continuous real-time analysis significantly reducing and minimizing the potential impact of an attack.

Anomaly Detection framework:

1) Data Collection
2) Baseline Establishment
3) Feature Selection:
4) Anomaly Detection Algorithm Application
5) Anomaly Scoring
6) Alert Generation
7) Incident Investigation
8) Response and Mitigation

The Anomaly Detection framework begins with data collection, where large datasets are gathered from various sources, including network traffic, system logs, and user activities. Following this, baseline establishment occurs, defining what constitutes normal system behavior by analyzing historical data to identify typical patterns. Next, feature selection is performed to identify relevant features and metrics that will be crucial for evaluating system behavior and detecting anomalies. Once the relevant features are established, anomaly detection algorithms are applied to analyze the data for deviations from the baseline. Detected anomalies are then assigned scores through anomaly scoring, which assesses the severity of each anomaly based on the degree of deviation from normal behavior. Significant anomalies trigger alert generation, notifying security teams of potential threats that require further investigation. The framework continues with incident investigation, where flagged anomalies are examined to determine their nature and whether they represent genuine threats. In cases where real threats are confirmed, a response and mitigation process is initiated to address the security issues effectively. By analyzing large datasets for deviations from normal behavior, the anomaly detection technique aids in identifying previously unknown threats, making it particularly useful for detecting zero-day exploits and advanced persistent threats (APTs) that traditional signature-based detection methods may overlook.

2.3 Common Indicators of Compromise (IoCs)

Threat identification relies heavily on recognizing IoCs, which are artifacts or signals that suggest a security breach has occurred. These can include:

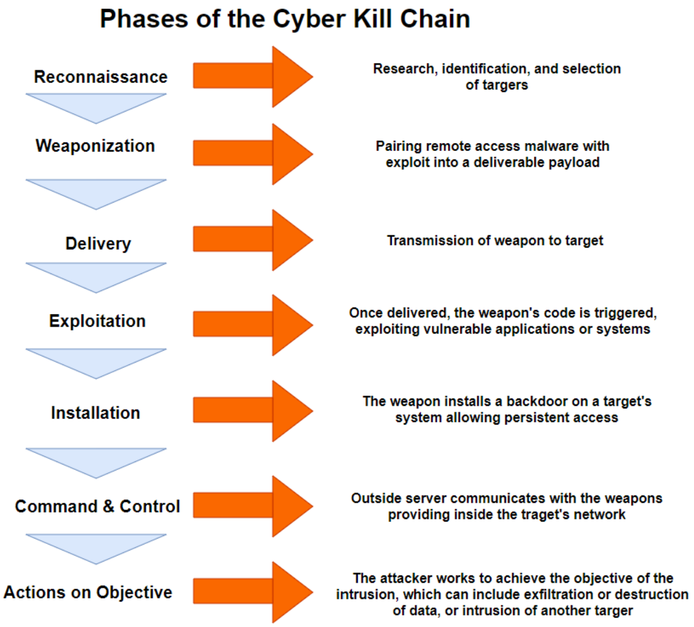
- Unusual login activities: For example, multiple failed login attempts from different geolocations or login attempts from previously unused devices.
- Suspicious file transfers: Large volumes of data being sent to unfamiliar external IP addresses can indicate data exfiltration.
- Process anomalies: Unusual processes running on a system, such as unauthorized system-level commands or unrecognized software, are often signs of malware or exploitation attempts.

Based on these IoCs, we can establish proactive measures and actions to enhance our defense against threats. These measures include blocking insecure URLs, scanning laptops for malware, investigating suspected users for potential insider threats or compromised accounts, and implementing spam filters to reduce phishing risks.

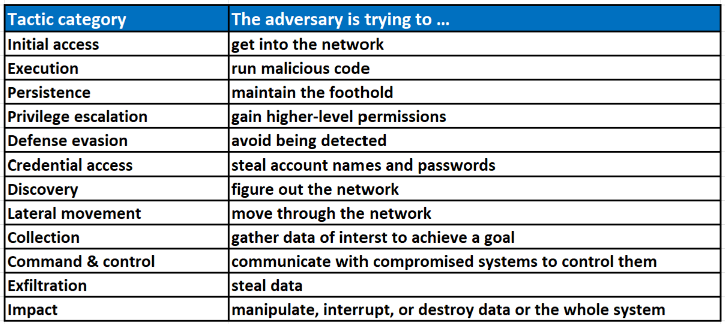
2.4 Frameworks for Threat Identification

Frameworks such as the Lockheed Martin Cyber Kill Chain and MITRE ATT&CK provide structured approaches to identifying and analyzing threats. These models break down attacks into stages, allowing threat hunters to identify malicious activity at various points in the attack lifecycle:

• Cyber Kill Chain: The model below outlines the stages of a cyberattack, from reconnaissance to actions on ojbective, allowing threat hunters to focus on disrupting attacks early in their lifecycle.


Phases of the Cyber Kill Chain
Reconnaissance
Research, identification, and selection of targers
Weaponization
Pairing remote access malware with exploit into a deliverable payload
Delivery
Transmission of weapon to target
Exploitation
Once delivered, the weapon's code is triggered, exploiting vulnerable applications or systems
Installation
The weapon installs a backdoor on a target's system allowing persistent access
Command & Control
Outside server communicates with the weapons providing inside the traget's network
Actions on Objective
The attacker works to achieve the objective of the intrusion, which can include exfiltration or destruction of data, or intrusion of another targer

- MITRE ATT&CK: This framework catalogs adversarial behaviors, tactics, and techniques, providing threat hunters with insights into the common strategies employed by attackers.



Tactic category	The adversary is trying to ...
Initial access	get into the network
Execution	run malicious code
Persistence	maintain the foothold
Privilege escalation	gain higher-level permissions
Defense evasion	avoid being detected
Credential access	steal account names and passwords
Discovery	figure out the network
Lateral movement	move through the network
Collection	gather data of interst to achieve a goal
Command & control	communicate with compromised systems to control them
Exfiltration	steal data
Impact	manipulate, interrupt, or destroy data or the whole system

By mapping threats to these techniques, threat hunters can develop more targeted and effective detection strategies.

The proactive identification of threats is a cornerstone of effective threat hunting. By understanding the different types of threats and utilizing advanced identification techniques, we can reduce the risk of undetected breaches, improving the overall security posture.

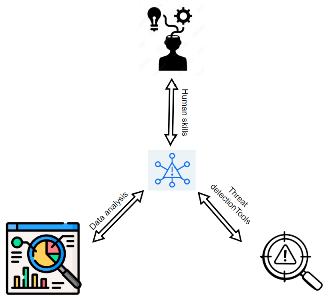
3. Threat Hunting Requirements

Effective threat hunting necessitates a diverse set of skills and resources, blending technical expertise, data analytics, and advanced detection capabilities to address these cyber threats. This proactive approach involves identifying potential threats and IoCs before they materialize into full-blown incidents, emphasizing the need for continuous monitoring and analysis across an organization's digital infrastructure. Below are the key requirements for successful threat hunting:

Technical Expertise and Security Knowledge:
Threat hunting requires deep cybersecurity knowledge, including understanding network architectures, traffic analysis, network segmentation, access control, and malware analysis through both static and dynamic techniques. It also involves a thorough understanding of attack methodologies such as ransomware and APTs. Familiarity with frameworks like MITRE ATT&CK and the Cyber Kill Chain is crucial for analyzing Tactics, Techniques, and Procedures (TTPs).

Data Analytics Skills:
Analyzing large datasets to detect threats is essential. Skills in data correlation, such as combining different data sources and contextual analysis; anomaly detection, including recognizing deviations from the norm, behavioral analytics, and real-time vs. retrospective analysis; and applying machine learning for pattern recognition, supervised vs. unsupervised learning, and automating threat detection are vital for identifying patterns and behaviors that bypass traditional security tools.

Tools and Technologies:
Threat hunters rely on a diverse set of tools and technologies to effectively detect, analyze, and respond to potential threats within an organization. These tools provide visibility across networks, endpoints, and user behavior, enabling the proactive identification of malicious activity. Tools such as SIEM platforms for centralized log management and real-time monitoring and alerting; EDR solutions for monitoring endpoint activity, threat detection, response, and forensic capabilities; Threat Intelligence Platforms (TIPs) for integrating external intelligence, enriching internal data, and proactive hunting; UEBA (User and Entity Behavior Analytics) for monitoring user and entity behavior, performing behavioral analytics, and reducing false positives; Deception Technologies for deploying traps and decoys, detecting lateral movement, and providing high-fidelity alerts; Network Traffic Analysis (NTA) for monitoring network traffic in real time and performing deep packet inspection; Security Orchestration, Automation, and Response (SOAR) for automating repetitive tasks and streamlining incident response; Packet Capture and Forensic Tools for full packet capture and forensic investigations; and Vulnerability Scanning and Management Tools for identifying weaknesses and prioritizing threats all enhance detection and response capabilities.



Automation and Machine Intelligence:
Automation can handle routine tasks, enhancing the efficiency

of threat hunting. While human expertise is indispensable, integrating cognitive machine intelligence could improve threat detection and response, though there are gaps in adoption due to skills shortages.

Effective threat hunting requires a combination of technical skills, data analytics, and advanced tools to proactively detect threats. Security teams need deep knowledge of cybersecurity, the ability to analyze large datasets, and the flexibility to adapt to new threats. By integrating automation and continuously learning, organizations can build robust threat-hunting programs capable of defending against emerging cyber threats.

4. Threat Hunting Framework and Strategies For Mitigation

To develop a robust threat-hunting capability, organizations must employ a structured framework that not only identifies and responds to threats but also supports continuous improvement in threat mitigation strategies. Effective threat hunting is a proactive activity that integrates various tools, technologies, and methodologies, aiming to uncover stealthy threats that may bypass traditional security defenses. This section outlines key elements of a threat-hunting framework and discusses the strategies for mitigation that organizations can implement to improve their overall security posture.

4.1 Defining the Threat Hunting Framework

The below framework outlines a structured approach to threat hunting in cybersecurity, focusing on data collection, analysis, and continuous feedback to improve detection and response to evolving threats.

1) Data Collection:
   The threat-hunting process begins by gathering relevant security data from various sources. This is critical for identifying potential threats. The data sources include:
   - Network Data: Logs from proxies, DNS, firewalls, and network sessions that provide visibility into network activities and potential threats.
   - Endpoint Data: Logs from applications and systems on endpoints, which can reveal signs of device compromise.
   - Threat Intelligence Data: External reports on known attacks, vulnerabilities, and indicators of compromise (IoCs) that help contextualize internal findings.
2) Data analysis using tools:
   Automation and tools play a crucial role in the efficiency of threat hunting. Solutions like Security Information and Event Management (SIEM), Endpoint Detection and Response (EDR) tools, and User and Entity Behavior Analytics (UEBA) help aggregate and analyze large volumes of security data in real-time, enabling more effective detection of potential threats.
3) Finding based on hypothesis:
   Threat hunters form hypotheses based on observed behaviors and data patterns. This step may follow one of two approaches:
   - Hypothesis-Driven Hunting: The investigation is guided by hypothesized behaviors or deviations from normal patterns.
   - Indicator-Driven Hunting: The investigation is based on known indicators of compromise (IoCs), such as malware hashes or IP addresses associated with known attacks.
4) Assess the impact:
   Threat hunters assess the potential impact of identified anomalies or suspicious behavior by analyzing the tactics, techniques, and procedures (TTPs) of adversaries. Frameworks like the Cyber Kill Chain and MITRE ATT&CK are often used to map the detected activities to known stages of attacks, helping assess how far an attacker may have progressed.
5) Report:
   After assessing the findings, threat hunters create detailed reports outlining the discovered threats, their potential impact, and recommendations for mitigation. This helps security teams understand the scope of the threat and take informed actions.
6) Follow up and feedbacks:
   The threat-hunting process is iterative and adaptive. Retrospective analysis and continuous feedback loops allow organizations to refine their methodologies. As threats evolve, organizations adjust their hunting techniques and improve their detection capabilities, ensuring that they remain proactive against new attack methods.

This threat-hunting framework emphasizes the importance of data collection from diverse sources, tool-assisted analysis, and a hypothesis-driven investigative approach. Also feedbacks, lessons learned and continuous adaptation to evolving threats, ensuring that organizations can keep up with new attack vectors and improve their defenses over time.

4.2 Strategies for Mitigation

Mitigating threats discovered during the threat-hunting process requires a blend of real-time response, automated defense mechanisms, and long-term strategic improvements. Effective mitigation strategies include:

- Endpoint Protection: Utilizing Endpoint Protection Platforms (EPP) and next-generation anti-virus solutions to block malicious activity before it spreads. Enforcing policies are important defensive measures.
- Layered Defense Strategies: Implementing defense-in-depth strategies, which combine multiple layers of defense, such as firewalls, intrusion detection/prevention systems (IDS/IPS), and network segmentation, helps limit the impact of any one security breach. These layered defenses must be regularly updated based on the latest threat intelligence.
- Leveraging Threat Intelligence: Incorporating external threat intelligence feeds into security operations enhances detection capabilities by correlating internal activities with known threats. Threat intelligence platforms (TIPs)

facilitate this integration, enriching the data available for analysis.
- Automation and orchestration of detection and response: enable early threat identification and rapid incident response by detecting anomalous behaviors, such as unusual login attempts, through continuous monitoring and automation, which streamline data analysis, integrate security technologies, and automate threat responses to minimize damage and reduce manual intervention.

4.3 Continuous Improvement and Adaptation

Threat hunting is an ongoing process that requires continual refinement and adaptation to new threat landscapes. Organizations should regularly review their hunting efforts and adjust strategies based on lessons learned:

- Lessons learned assessment: Reviewing the effectiveness of previous threat-hunting campaigns helps identify gaps in detection capabilities and fine-tune tools, techniques, and workflows.
- Training and Skill Development: As threat hunting evolves, so must the skills of the personnel involved. Continuous education and training in advanced analytical techniques, including machine learning and artificial intelligence (AI), are essential for staying ahead of emerging threats.
- Feedback Loop: The insights gained through threat hunting should inform broader security strategies, including policy changes, infrastructure upgrades, and the adoption of new security tools.

An effective threat-hunting framework integrates human expertise, automated tools, and proactive detection strategies to uncover threats before they cause harm. By employing mitigation strategies such as automation, continuous monitoring, and defense-in-depth, organizations can significantly reduce risk and improve their overall security posture. Continuous adaptation to evolving threats and fostering collaboration across the cybersecurity ecosystem are essential components of a successful and resilient threat-hunting program.

5. Conclusion

Threat hunting has become a critical component of modern cybersecurity strategies, providing a proactive defense against sophisticated threats such as zero-day vulnerabilities and APTs. Unlike traditional reactive approaches, threat hunting teams must establish frameworks that can anticipate, detect, and mitigate threats before significant damage occurs. The combination of human expertise, data analytics, and advanced tools has proven effective in enhancing an organizations threat detection and incident response capabilities. However, challenges remain, including the need for more advanced tools for autonomous analysis and addressing the skills gap in data analytics among security professionals. While threat hunting programs are effective in reducing attack surfaces and improving response times, many organizations still struggle to fully realize the benefits of these initiatives. To address these challenges, security programs must prioritize continuous improvement by embracing automation, enhancing detection capabilities, and adapting methodologies over time. By doing so, organizations can reduce the impact time, improve their overall security posture, and strengthen their defenses against evolving cyber threats.

References

[1] Eduardo B. Fernndez, A Threat Model Approach to Threats and Vulnerabilities in On-line Social Networks. January 2010 DOI: 10.1007/978-3-642-16626-6_15 Source: DBLP
[2] Borja Sanz, Gonzalo Alvarez, Carlos Laorden, Pablo Garca Bringas. A Threat Model Approach to Attacks and Countermeasures in On-line Social Networks. October 2011.
[3] Mohammad Aijaz, Mohammed Nazir, Malik Nadeem Anwar Mohammad. Threat Modeling and Assessment Methods in the HealthcareIT System: A Critical Review and Systematic Evaluation. SN Computer Science (2023) 4:714. https://doi.org/10.1007/s42979-023-02221-1
[4] Suvda Myagmar Adam J. Lee William Yurcik. Threat Modeling as a Basis for Security Requirements.
[5] Mohammed Kharma, Adel Taweel. Threat Modeling in Cloud Computing - A Literature Review. February 2023. DOI: 10.1007/978-981-99-0272-9_19.
[6] Matteo Groe-Kampmann, Norbert Pohlmann, Markus Hertlein, Thorsten Holz. Threat Modeling for Mobile Health Systems. April 2018. DOI: 10.1109/WCNCW.2018.8369033.
[7] Habeeb Omotunde, Rosziati Ibrahim. A Review of Threat Modelling and Its Hybrid Approaches to Software Security Testing. December 2015.
[8] Eduardo B. Fernndez. Threat Modeling in Cyber-Physical Systems. August 2016. DOI: 10.1109/DASC-PICom-DataCom-CyberSciTec.2016.89
[9] ISMAIL ASSOUJAA, SIHAM EZZOUAK, HAKIMA MOUANIS. Compression Point in Field of Characteristic 3. Springer, I4CS 2022, CCIS 1747, pp. 104111, 2022 https://doi.org/10.1007/978-3-031-23201-5_7.
[10] ISMAIL ASSOUJAA, SIHAM EZZOUAK, HAKIMA MOUANIS. Tower Building Technique on Elliptic Curve with Embedding Degree 36. WSEAS TRANSACTIONS ON COMPUTERS. DOI: 10.37394/23205.2022.21.39.
[11] ISMAIL ASSOUJAA, SIHAM EZZOUAK, HAKIMA MOUANIS. Tower Building Technique on Elliptic Curve with Embedding Degree 72. WSEAS Transactions on Computer Research 10:126-138 DOI: 10.37394/232018.2022.10.17
[12] ISMAIL ASSOUJAA, SIHAM EZZOUAK, HAKIMA MOUANIS. TOWER BUILDING TECHNIQUEON ELLIPTIC CURVEWITH EMBEDDING DEGREE 18. Tatra mountains mathematical publications, DOI: 10.2478/tmmp-2023-0008Tatra Mt. Math. Publ. 83 (2023), 103118.
[13] ISMAIL ASSOUJAA, SIHAM EZZOUAK, HAKIMA MOUANIS. Pairing based cryptography New random point exchange key protocol. Conference: 2022 7th International Conference on Mathematics and Computers in Sciences and Industry (MCSI), DOI: 10.1109/MCSI55933.2022.00017.
[14] ISMAIL ASSOUJAA, SIHAM EZZOUAK. New Compression Point Reducing Memory Size in Field of Characteristic Different From 2 And 3.International Journal of Scientific Research and Innovative Studies. https://doi.org/10.5281/zenodo.11244720.
[15] ISMAIL ASSOUJAA, SIHAM EZZOUAK. Improving arithmetic calculations on elliptic curves with embedding degree 2i.3. Journal of Xidian University. https://doi.org/10.5281/Zenodo.11505701. ISSN No:1001-2400.
[16] ISMAIL ASSOUJAA, SIHAM EZZOUAK, Improving Arithmetic Calculations on Elliptic Curves with Embedding Degree 2i and 3j, International Journal of Recent Engineering Research and Development (IJRERD), ISSN: 2455-8761-Volume 09 Issue 03, PP. 131-142.
[17] ISMAIL ASSOUJAA, SIHAM EZZOUAK, Compression points in elliptic montgomery and edwards curves. ACM ISBN 979-8-4007-0929, https://doi.org/10.1145/3659677.3659834.
[18] Nombeko Ntingi, Petrus Duvenage. Effective Cyber Threat Hunting: Where and how does it fit? European Conference on Cyber Warfare and Security June 2022 DOI: 10.34190/eccws.21.1.240
[19] Muhammad Salman Khan, Rene Richard. Cyber Threat Hunting: A Cognitive Endpoint Behavior Analytic System. International Journal of Cognitive Informatics and Natural Intelligence Volume 15 - Issue 4.

[20] Naseemuddin Mohammad. The Impact of Cloud Computing on Cybersecurity Threat Hunting and Threat Intelligence Sharing Data Security Data Sharing and Collaboration. September 2022. International Journal of Computer Applications (IJCA) Volume 3, Issue 1, Jan-Dec 2022, pp. 21-32, Article ID: IJCA_03_01_004. 2341-7801, 2969-1566.

[21] Sankha Chakraborty, Nisha T N. Next generation proactive cyber threat hunting - A complete framework. October 2022. DOI: 10.1063/5.0109674

[22] Md Nazmus Sakib Miazi, Mir Mehedi A. Pritom, Mohamed Shehab, Bill Chu, and Jinpeng Wei. The Design of Cyber Threat Hunting Games: A Case Study. July 2017. DOI: 10.1109/ICCCN.2017.8038527

[23] Ismail Assoujaa, Siham Ezzouak, Extended Diffie-hellman Key Exchange With Pairing Cryptography To Multiple Users. International Journal of Advances in Electronics and Computer Science. Volume-11, Issue-7, July 2024.

[24] Ismail Assoujaa, Siham Ezzouak, Enhancing Security Through Implementation Of Double Encryption Algorithm. International Journal of Advances in Electronics and Computer Science. Volume-11, Issue-7, July 2024.

[25] Ismail Assoujaa, Siham Ezzouak, Tower Building Technique on Elliptic Curve with Embedding Degree 54. PROOF. DOI: 10.37394/232020.2024.4.8. Volume 4, Issue 2024.

Contribution of Individual Authors to the Creation of a Scientific Article (Ghostwriting Policy)

The author contributed in the present research, at all stages from the formulation of the problem to the final findings and solution.

Sources of Funding for Research Presented in a Scientific Article or Scientific Article Itself

No funding was received for conducting this study.

Conflict of Interest

The author has no conflict of interest to declare that is relevant to the content of this article.

Creative Commons Attribution License 4.0 (Attribution 4.0 International, CC BY 4.0)