Journal of Advanced Research in Agriculture Science & Technology
Volume 8, Issue 1 - 2025, Pg. No. 7-10
Peer Reviewed Journal

Review Article

A Comprehensive Review of Modern Cyber Defence: The Role of Threat Intelligence and Hunting

Abhishek Sharma[1], Jayant Singh[2]

Research Scholar, Thakur Institute of Management Studies, Career Development & Research TIMSCDR, Mumbai, India

I N F O

E-mail Id:
abhishekanandsharma99@gmail.com
Orcid Id:
https://orcid.org/0009-0003-0869-7260

How to cite this article:
Sharma A, Singh J. A Comprehensive Review of Modern Cyber Defence: The Role of Threat Intelligence and Hunting. *J Adv Res Agri Sci Tech* 2025; 8(1): 00-00.

Date of Submission: 2025-03-20
Date of Acceptance: 2025-06-15

A B S T R A C T

In today's era of relentless cyberattacks, organisations must priortise strengthening their digital security measures. This study explores the critical roles of threat intelligence and cyber threat hunting in modern cybersecurity frameworks. By defining the concepts, categorising types and sources of threat intelligence, and detailing the iterative processes involved in cyber threat hunting, the research underscores their proactive contributions to identifying and mitigating potential risks. Additionally, it examines the challenges organisations encounter during implementation and proposes actionable solutions to address these issues. In an evolving threat landscape, the findings highlight the necessity of adopting a proactive, collaborative, and adaptable approach to cybersecurity.

Keywords: Threat Intelligence, Cybersecurity, Malware Analysis

Introduction

Information assets, systems, and networks within a business may be at danger, and threat intelligence is the understanding and analysis of both present and future cyberthreats. Information regarding opponents' goals, skills, and tactics must be gathered, analysed, and interpreted.[1] The goal is to identify and understand potential threats ahead of time in order to make informed decisions and improve the organization's security posture.

A proactive approach to cybersecurity called "cyber threat hunting" is actively and repeatedly looking for indications of harmful behaviour within the networks and systems of a company. Threat hunting is a dynamic process in which cybersecurity specialists actively investigate the environment to uncover dangers that may have evaded automated defences, as opposed to typical security solutions that rely on predetermined rules. To identify and reduce possible security issues, advanced analytics, threat intelligence, and human knowledge are frequently used.[2-7]

Threat Intelligence

Threat intelligence is a data set including information about attempted or successful intrusions that is typically collected and evaluated by automated security systems that use machine learning and AI.

Threat intelligence is a compilation of data about successful or attempted attacks. It is typically gathered and examined by automated security systems that use artificial intelligence and machine learning.[2]

Definition and Types

Strategic Threat Intelligence: A high-level focus on long-term trends and prospective hazards that assists organisations in making educated strategic decisions.

Operational Threat Intelligence: Provides precise information about specific threats, such as indicators of compromise (IoCs) and adversaries' tactics, methods, and procedures (TTPs).

Tactical Threat Intelligence: Provides real-time and actionable insights to aid in urgent response activities, such as identifying specific threats aimed at the enterprise.

Collection and Sources

Collecting threat intelligence entails gathering information about potential and current cyber threats in order to understand adversaries' tactics, techniques, and procedures (TTPs). Here are a few methods for gathering threat intelligence that are commonly used.

OSINT, Open-Source Intelligence entails gathering data from publicly available sources such as news articles, social media, public forums, and government reports.

CSINT (Closed-Source Intelligence) is the gathering of information from proprietary or subscription-based sources such as commercial threat intelligence feeds, dark web forums (where legal), and specialised intelligence services.

HUMINT is the collection of intelligence through direct interactions with individuals. This could include insider information, industry contacts, or threat informants.

Analysis and Processing

Several key steps and methodologies are involved in the analysis and processing of collected data to generate actionable threat intelligence. This procedure is critical for converting raw data into meaningful insights that businesses can use to strengthen their cybersecurity defences.

Data collection, normalisation and standardisation, enrichment, correlation, and aggregation are all steps in the data collection process. Analysis of Threat Intelligence, Prioritisation of Threat Intelligence, Actionable Intelligence, Feedback Loop, and Integration with Security Tools

Cyber Threat Hunting

Threat hunting, often referred to as cyber threat hunting, is a proactive method used to detect unknown or unresolved threats that may already exist within an organisation's network.

Methodologies

Signature-Based Detection: This method involves looking for recognised patterns or signs of malicious activity, which is frequently based on predefined rules.

Anomaly Detection: Identifies deviations from typical behaviour, assisting in the detection of odd or suspicious actions that may signal a security problem.

Behaviour Analysis

Examines system and user behaviour to detect subtle symptoms of compromise or malicious behaviour.

Tools and Technologies

Security Information and Event Management (SIEM): Collects and analyses log data from several sources in order to identify potential security problems.

Threat Intelligence Platforms

These platforms make it easier to acquire, analyse, and disseminate threat intelligence in order to enable proactive security actions.

Endpoint Detection and Response (EDR)

Endpoint Detection and Response (EDR) monitors and responds to endpoint activity, offering visibility into possible threats at the device level.

Human Element

Human Element: Cyber Threat Hunting mainly relies on qualified cybersecurity experts who use their expertise and experience to discover and respond to sophisticated threats that may be difficult to detect using automated means.

Integration Of Threat Intelligence And Cyber Threat Hunting

Threat intelligence and cyber threat hunting work in tandem to provide the foundation and guidance for proactive defence, while threat hunting ensures a continuous, hands-on investigation to uncover and address threats that may evade automated detection. This collaborative approach improves a company's ability to detect, respond to, and mitigate cyber threats.

Enhanced Incident Response, Contextual Understanding of Threats, Proactive Threat Identification, Real-Time Detection and Response, Constant Improvement and Adaptation, and Integration of Findings

Challenges And Ethical Considerations

Data Privacy Concerns

The difficulty comes from the fact that gathering and sharing threat intelligence frequently involves the collection and dissemination of sensitive information. Balancing the need for comprehensive threat data with privacy concerns is difficult, especially because regulations such as GDPR impose stringent requirements on the handling of personal data.

Implications: In order to comply with privacy regulations while also contributing to and benefiting from threat intelligence sharing initiatives, organisations must implement robust data anonymisation and protection measures.

Information Accuracy

Depending on the reliability of sources introduces challenges, as information from untrustworthy or compromised sources can lead to inaccuracies.

Implications: Relying on unreliable sources may result in the integration of false or misleading data into cybersecurity assessments.

Rapid Evolution of Cyber Threats

Incomplete or inaccurate data hampers the ability to form a comprehensive understanding of the threat landscape.

Implications: Inaccurate threat intelligence may result in misinformed decisions and inadequate protection measures.

Wasted Resources

False positives may lead to unnecessary allocation of resources to investigate non-existent threats.

Implications: organisations may expend resources on mitigating perceived threats, diverting attention and funds from actual risks.

Attribution Challenges:

Accurately attributing cyber threats to specific entities is a complex task, often prone to errors.

Implications: Misattribution can lead to unwarranted actions against innocent parties, damaging reputations and escalating tensions.

Case Studies

APT1 Report from Mandiant

Mandiant (now FireEye) published a report in 2013 detailing the activities of APT1, a Chinese cyber espionage group .[3] Based on extensive threat intelligence and incident response investigations, the report revealed details about the group's tactics and infrastructure. This example demonstrates how threat intelligence can be used to attribute cyber threats and inform the larger community.

CrowdStrike's DNC Hack Investigation

CrowdStrike investigated a cyber intrusion into the Democratic National Committee (DNC) in 2016. The firm used threat intelligence to attribute the attack to Russian state-sponsored actors, thereby increasing public awareness of nation-state cyber threats.[4] This case illustrates the application of threat intelligence in political and strategic contexts.

WannaCry Ransomware Explosion

The WannaCry ransomware attack in 2017 impacted organisations all over the world. Security researchers from Kaspersky and Symantec studied the ransomware's behaviour and used threat intelligence to connect it to the North Korean Lazarus Group. The incident demonstrated the significance of threat intelligence as well as rapid cyber threat hunting in responding to large-scale attacks.[5]

Future Trends

Ransomware has recently received a lot of attention due to an increase in ransomware attacks on individuals, businesses, and governments all over the world. Ransomware attacks are evolving and becoming more sophisticated than ever. This study investigates the literature review of CTI and CTH for both malware and ransomware works with their limitations and gaps from this perspective. This study will also look into current CTH techniques and the use of CTI techniques. To highlight the main trends, related studies and available datasets were reviewed. Potential research directions for ransomware studies are also described.

AI and Machine Learning in Threat Intelligence:

- **Behavioural Analysis:** AI and machine learning are increasingly being used to analyze patterns of behaviour in order to detect anomalies and potential threats. This method goes beyond traditional signature-based detection by detecting novel and previously unknown threats.

Machine learning algorithms can analyze historical data to forecast future threats and trends. This enables organisations to strengthen their defences proactively based on predictive insights.

- **Natural Language Processing (NLP):** NLP is used to extract valuable insights from unstructured data, such as threat intelligence reports and social media. This improves understanding of the threat landscape and aids decision-making.

AI and machine learning for threat detection:

- **Anomaly Detection:** AI and machine learning algorithms assist threat hunters in detecting subtle anomalies in network traffic, user behaviour, and system activity that indicate potential security incidents.

Threat hunters can use AI-powered tools to automate repetitive tasks, freeing them up to focus on higher-level analysis and decision-making.

- **Adaptive Learning:** Machine learning algorithms can learn from the outcomes of threat hunting operations, adapting over time to improve the accuracy and efficiency of future investigations.

Sharing of Threat Intelligence in Collaboration:

- **Federated Learning:** Machine learning collaborative models, such as federated learning, allow organisations to share threat intelligence without sharing sensitive raw data. This enables a collective defence strategy without jeopardising privacy.

Malware Analysis Using Deep Learning:

- **Deep Neural Networks (DNNs):** Deep learning techniques, including DNNs, are used in malware analysis to detect malicious code and behaviour more accurately and efficiently.

Analytics of User and Entity Behaviour (UEBA):

- **AI-Driven UEBA:** AI and machine learning (ML) play an important role in UEBA by learning normal patterns of user and entity behaviour and detecting deviations that may indicate insider threats or compromised accounts.

Conclusion

The evolving threat landscape necessitates a comprehensive and adaptive cybersecurity strategy. To stay ahead of emerging cyber threats, organisations must leverage advanced technologies, collaborate within the cybersecurity community, and constantly refine their strategies. This proactive defence strategy relies heavily on threat intelligence and cyber threat hunting.

It's important to note that the threat landscape is dynamic, and new trends may have emerged since my last update. Organisations are increasingly relying on these advanced technologies to stay ahead of sophisticated cyber threats and to improve the efficiency and effectiveness of their threat intelligence and cyber threat hunting efforts.

References

1. P. W. Singer and A. Friedman, Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press, 2014. [Online]. Available: https://scholar.google.com/scholar?q=Cybersecurity+and+Cyberwar:+What+Everyone+Needs+to+Know
2. A. Azmoodeh, M. Tabandeh, and A. R. Seifi, "Cyber Threat Intelligence: Challenges and Opportunities," Journal of Network and Computer Applications, vol. 103, pp. 57–71, Feb. 2018. [Online]. Available: https://scholar.google.com/scholar?q=Cyber+Threat+Intelligence:+Challenges+and+Opportunities
3. Mandiant, "APT1: Exposing One of China's Cyber Espionage Units," 2013. [Online]. Available: https://scholar.google.com/scholar?q=Mandiant+APT1+report
4. CrowdStrike, "CrowdStrike Global Threat Report," 2024. [Online]. Available: https://go.crowdstrike.com/rs/281-OBQ-266/images/CrowdStrikeGlobalThreatReport2025.pdf?version=0
5. Symantec, "Internet Security Threat Report," Vol. 23, 2018. [Online]. Available: https://scholar.google.com/scholar?q=Symantec+Internet+Security+Threat+Report+2018
6. Sun N, Ding M, Jiang J, Xu W, Mo X, Tai Y, Zhang J. Cyber threat intelligence mining for proactive cybersecurity defence: A survey and new perspectives. IEEE Communications Surveys & Tutorials. 2023 May 5;25(3):1748-74.
7. Mahboubi A, Luong K, Aboutorab H, Bui HT, Jarrad G, Bahutair M, Camtepe S, Pogrebna G, Ahmed E, Barry B, Gately H. Evolving techniques in cyber threat hunting: A systematic review. Journal of Network and Computer Applications. 2024 Aug 23:104004.