Journal of New Technology and Materials

ISSN:2170161X | E-ISSN: 2588-2082 | Vol.15 Issue2 (Dec 2025)

Threat Hunting in Large-Scale Socs: A Cyber Threat Intelligence-Driven Model Using MITRE ATT&CK And Machine Learning

Dr. Oliver Smith
Department of Cybersecurity, University of Manchester, UK
Dr. Rachel Hughes
Department of Computer Science, University of Manchester, UK

Abstract

Cyber threats have grown increasingly sophisticated and difficult to track, necessitating the implementation of proactive security solutions at large-scale Security Operations Centers (SOCs). In order to improve threat detection, investigation, and response, the proposed research presents a unified threat hunting paradigm that incorporates MITRE ATT&CK, ML, and Cyber Threat Intelligence (CTI). The paper begins by discussing how CTI gives attackers contextual knowledge and how threat hunting has evolved in modern SOCs. Also covered are the MITRE ATT&CK framework's structural strengths and how to use machine learning to spot patterns that are not visible with the naked eye. After that, we lay out the framework, development methodology, and supporting technologies for a model that is based on CTI. A number of real-world case studies demonstrate the model's utility and advantages. While doing so, we lay the groundwork for investigating potential trends in the future by talking about the primary obstacles, such as data integration and the trade-offs between automation. To stay ahead of the competition in a constantly changing strategic landscape, this study suggests that SOCs should employ a threat hunting strategy that is intelligence-driven, behavior-based, and improved with machine learning.

Keywords: Cyber Threat Intelligence; Threat Hunting; MITRE ATT and CK Framework; Security Operations Center (SOC); Machine Learning

1. Introduction

1.1. Definition of Threat Hunting and Its Importance

When it comes to cybersecurity, threat hunting is a proactive process where analysts scour databases, networks, and systems for dangers that manage to elude routinely used security protections like antivirus software, firewalls, or security information and event management systems. Instead than depending on alerts, danger hunting focuses on human intuition, proactive understanding, and research, with a focus on context. The threat-hunting method, according to Nour et al. (2023), is a hypothesis-based search that helps with detection by uncovering adversaries' tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs). Due to the prevalence of advanced persistent threats (APTs) and other forms of stealthy attackers in today's threat landscape, this approach takes on added importance (Chakraborty and Nisha, 2022). Proactive threat hunting, according to Kulkarni et al. (2023), enhances incident response, threat containment, and dwell time, which in turn increases an organization's cyber resilience.

ISSN:2170161X | E-ISSN: 2588-2082 | Vol.15 Issue2 (Dec 2025)

1.2. Overview of Security Operations Centers (SOCs)

Organizational centralized units engaged in continuous monitoring, detection, analysis, and reaction to cybersecurity incidents are known as security operations centers (SOCs). The ability to integrate human efforts, procedures, and technology into a unified defense system is what makes SOCs so useful for threat interception and response. Vielberth et al. (2020) states that modern SOCs deal with problems such too many warnings, insufficient personnel, and the necessity to coordinate different security solutions. The progression of cyber threats necessitates the adoption of next-generation SOCs, which are characterized by intelligence-driven automation (Muniz, 2021). Cyber threat intelligence (CTI), cloud computing, advanced analytics, and machine learning allow these next-gen SOCs to improve their situational awareness and decision-making skills.

Figure 1. Conceptual model for the success of SOC establishment

1.2.1. *Purpose of Integrating Cyber Threat Intelligence with MITRE ATT&CK and Machine Learning*

Machine learning (ML), Cyber Threat Intelligence (CTI), and MITRE ATT&CK are going to revolutionize threat hunting in the future. While MITRE's ATT&CK framework provides an orderly catalog of hostile TTPs structured across the attack lifecycle, CTI provides situational awareness of threats. Through the automated analysis of data and the identification of anomalous behavior, machine learning enhances detection. The CTI-MITRE ATT&CK-ML paradigm of active and adaptive threat hunting is formed by combining these three terminologies. According to Bolla and Talentino (2022), integrating threat hunting with CTI and ATTa&CK allows for more targeted hunts, which in turn reduces the likelihood of false positives and improves the

ISSN:2170161X | E-ISSN: 2588-2082 | Vol.15 Issue2 (Dec 2025)

process's accuracy. Meanwhile, Sree et al. (2021) stress that SOCs can improve their threat prediction and perhaps detect zero-day threats by integrating AI and ML into this unified model. Lastly, this comprehensive method also allows large SOCs to scale threat hunting, make it intelligence-based, and respond to evolving adversarial behavior (Roy et al., 2023).

2. Understanding the MITRE ATT&CK Framework

2.1. Overview of MITRE ATT&CK

An internationally acclaimed cyber intelligence resource, MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) organizes and describes an adversary's activities across the whole cyber-attack life cycle. Its creators, MITRE, set out to create a shared vocabulary for defining and analyzing threats so that defenders could follow a blueprint for what malicious actors do once they get into a system (Roy et al., 2023). By systematically classifying known tactics, methods, and procedures (TTPs), the framework helps security teams gain a better grasp of how attackers function and execute their schemes. This, in turn, allows for their discovery and response. One of the most important tools for threat modeling and adversary simulation is ATT&CK, which mediates between threat intelligence and defensive counteractions (Georgiadou et al., 2021).

Figure 2. The ATT&CK Matrix for Enterprise (categories of enterprise tactics across the attack lifecycle)

2.2. Key Components and Tactics

The three main components of MITRE ATT&CK are tactics, techniques, and subtechniques. The technical goals of the enemy, or tactics, could include things like data exfiltration, privilege escalation, or lateral movement. Methods used to achieve a goal are called techniques. Each

ISSN:2170161X | E-ISSN: 2588-2082 | Vol.15 Issue2 (Dec 2025)

method can be fine-tuned with the help of sub-techniques. The framework is enhanced for usage in the field of operation by including mappings to groupings of threats and software used in real-world attacks, as outlined by Roy et al. (2023). Additionally, as Kinnunen (2022) notes, businesses can use the ATT&CK structure to examine gaps and prioritize detection actions. This helps them determine what needs to be covered and what is already being watched. We also provide ATT&CK matrices tailored to various platforms, allowing for versatility in a wide range of security scenarios. These platforms include enterprise systems, mobile devices, and industrial control systems (ICS).

2.3. Relevance of ATT&CK in Threat Hunting

For guidance on how to carry out threat hunting, the MITRE ATT&CK framework is a good resource. As a result, analysts can use known TTPs to generate hypotheses and correlate adversary detection use cases with real-world behaviors (Chukwu, 2023). Structured mappings between threat actor behavior and defensive capabilities can also be used to improve threat intelligence inside the framework. According to Al-Sada et al. (2023), ATT&CK improves detection accuracy by reducing the likelihood that static indicators would become irrelevant due to popular evasion techniques, and this is achieved through a behavior-based approach. Moreover, large-scale SOCs can uncover connected data and identify unknown dangers by incorporating ATT&CK into threat-related machine learning models and intelligence platforms, which allows for greater automation (Shin et al., 2023). By acting in this way, danger hunting is transformed into an intelligence-based, proactive idea.

3. The Role of Cyber Threat Intelligence

3.1. Definition and Importance of Cyber Threat Intelligence (CTI)

Cyber Threat Intelligence refers to the act of collecting, evaluating, and relating data regarding existing or future cyber dangers in order to guide security decisions. As a component of preventative cybersecurity, it gives context regarding the motivations, means, and outcomes of threat actors' actions. The information that a defender needs to balance, detect, respond to, and recover from cyber incidents is called CTI (knowledge based on evidence), according to Ainslie et al. (2023). In order to manage the amount and complexity of threats to the enterprise environment, CTI has become crucial in large-scale Security Operations Centers (SOCs). Tounsi and Rais (2018) state that the incorporation of CTI renders passive security more susceptible to adversaries' actions becoming predictable. The technical and strategic operations, such as incident response, risk assessment, policy enforcement, and security investment decisions, are both aided by CTI, as pointed out by Möller (2023). Modern threat environments are defined by frequent and dynamic attacks, which create a level of unpredictability and a lack of security acumen. CTI gives a much-needed boost to this field.

3.2. Types of Threat Intelligence (Strategic, Tactical, Operational)

Different stages of the security lifecycle call for different types of CTI, which can be generically classified as strategic, tactical, or operational intelligence. Strategic intelligence provides

ISSN:2170161X | E-ISSN: 2588-2082 | Vol.15 Issue2 (Dec 2025)

extensive, high-level analyses of emerging dangers, geopolitical shifts, and cybercrime patterns. This intelligence provides a bird's-eye view of a danger landscape and is designed to help executives make decisions (Abu et al., 2018). Threat actors' methodologies, scripts, and infrastructure, including as vulnerability exploits, phishing websites, and indicators of compromise (IOCs), are the domain of tactical intelligence. Its primary audience consists of security operations center (SOC) analysts and threat hunters, who require a high level of technical detail in order to construct detection strategies and incident response plans (Mavroeidis and Bromander, 2017). When an attack is underway or about to happen, operational intelligence can tell you about it with a time limit. In order to respond to incidents in real-time, this includes telemetry data, behavioral analytics, and knowledge on enemy infrastructure. For accurate danger forecasting and timely elimination, active CTI is crucial (Yang and Lam, 2019). When taken as a whole, these three tiers of intelligence would provide SOCs with a multi-pronged defense strategy that includes strategic planning, tactical readiness, and operational resilience.

3.3. How CTI Informs Threat Hunting Efforts

The use of CTI in threat hunting improves the precision and breadth of investigations. In order to actively seek out indicators of harmful activity that automated detection technologies might miss, threat hunters often rely on hypothesis testing. Threat hunters can speed up this process with the help of CTI, which provides them with actionable intelligence (such as adversary TTPs, known attack pathways, and campaign indicators) that can be combined into targeted hypotheses. Bolla and Talentino (2022) found that threat hunting using CTI drastically cuts down on investigative overhead, freeing analysts to concentrate on patterns of possible attacks and high-risk behaviors. By incorporating threat intelligence into specialized frameworks like MITRE ATT&CK, an empirical platform may be created to build anomaly-based methods of identifying adversary activity that is profile-specific (Roy et al., 2023).

According to Rastogi and Alam (2023), CTI also gives raw data collected at the endpoint, on a network, or in the cloud a more contextual flavor, making it easier for analysts to tell if an anomaly is harmless or a real threat. Further, CTI aids automation by enhancing the detection accuracy and search cycle reduction of SIEMs, SOAR platforms, and machine learning models with richer intelligence. In essence, CTI facilitates the transition from ad hoc, manually-performed threat hunting to a structured process that follows the models of intelligence-led threat hunting, taking into account the various threats and adversarial tactics in use.

4. Integrating Machine Learning in Threat Hunting

4.1. Overview of Machine Learning Concepts

The ability for systems to learn and make judgments, drawing conclusions and predictions from data, is the essence of Machine Learning (ML), a subfield of AI. It makes use of algorithms that get better and better with time as they handle more data. As a vital component of current cybersecurity tactics, ML automates threat mitigation and classification, making it an indispensable tool in the cybersecurity industry. Shon and Moon (2007) state that ML excels in

ISSN:2170161X | E-ISSN: 2588-2082 | Vol.15 Issue2 (Dec 2025)

situations when human analysts are unable to handle the sheer volume or complexity of the data. Notable ML paradigms like supervised, unsupervised, and reinforcement learning allow cybersecurity systems to dynamically react to new attack tactics, discover previously unseen abnormalities, and identify targeted recognized threats. According to Martinez Torres et al. (2019), ML's adaptability is one of the main reasons why it is a great tool to supplement both proactive and reactive security methods, such as threat hunting.

4.2. Applications of Machine Learning in Cybersecurity

Machine learning is becoming more and more important in security technology for tasks such as intrusion detection, malware categorization, phishing detection, and behavioral analysis. Regarding threat hunting in particular, ML allows SOCs to spot subtle trends and deviations from normal activity that might be signs of a threat. Omar et al. (2013) note that rule-based systems are not up to the task of detecting insider threats and zero-day malware, but ML-driven anomaly detection devices are. Also, as Bharadiya (2023) points out, dimensionality reduction, clustering, and classification are used to find dangerous acts in massive amounts of security data. On top of that, systems can use historical data and trends of cyber threat actors to anticipate assaults thanks to predictive analytics made possible by ML combined with cyber threat intelligence (Sree et al., 2021). More and more, ML-based platforms are maturing and prepared to enable real-time and near-real-time detection procedures within the SOC. This is demonstrated by new tools like RedAI (Noel, 2021) and systems proposed by Chen et al. (2022).

4.3. Benefits of Using ML for Threat Detection and Analysis

There are a number of significant benefits to using machine learning for threat hunting and investigation in large-scale, data-intensive environments. In order for ML to effectively detect dangers, it must first learn to recognize patterns of behavior that allow it to identify both known and unknown risks. Traditional security solutions also suffer from false positives; this method can reduce them by leaving high-confidence alarms and removing harmless abnormalities (Katragadda et al., 2020). Secondly, ML makes it possible to scale threat detection, which means that huge datasets may be continuously scanned and analyzed across many networks, endpoints, and cloud environments without slowing down (Handa et al., 2019). Third, ML helps systems be more agile in responding to threats by enabling them to adapt to new techniques, tactics, and procedures (TTPs). Machine learning algorithms may be regularly updated with fresh threat knowledge, according to Chakraborty and Nisha (2022). This allows them to adapt to changing threat conditions. Shin et al. (2023) notes that ML and frameworks like MITRE ATT&CK can work together to provide an automated system for matching observed actions with established strategies and techniques. By improving threat visibility, SOCs will be able to reduce dwell time and make better use of threat intelligence across operations thanks to this integration. Last but not least, machine learning makes threat hunting less of a manual process and more of a dynamic, scalable, and intelligence-driven one.

ISSN:2170161X | E-ISSN: 2588-2082 | Vol.15 Issue2 (Dec 2025)

5. Developing a Cyber Threat Intelligence-Driven Model

5.1. Framework for Integrating CTI with MITRE ATT&CK

An improved level of threat identification and investigation within SOCs can be achieved by combining contextual threat information with structured adversary behavior frameworks in a model. This transforms threat hunting into a methodology driven by cyber threat intelligence. This is in line with what is known as the MITRE ATT&CK framework, which is a defined taxonomy of strategies and methods for mapping threat intelligence feeds. Analysts are able to convert broad threat knowledge into specific, technical actions and signals in operational contexts when there is such connection (Bolla and Talentino, 2022). Upon startup, the model often begins to find threat actor profiles and techniques, tactics, and vulnerabilities (ATT&CK) that should be mapped into the matrix. Instead of depending on reactive indicators, these mappings can be used to create detection logic based on adversary behavior and generate proactive hunting hypotheses (Roy et al., 2023). Security operations centers (SOCs) can better prioritize and respond to attacks when intelligence is correlated with the ATT&CK structured framework, which aligns strategy with tactical threat detections.

Figure 3. The Threat Intelligence Life Cycle

5.2. Steps for Model Development

An intelligence-based threat hunting model is built through an evolutionary process that incorporates CTI, behavioral frameworks, and machine learning. The method is divided into various logical steps. To begin, businesses must gather and standardize threat intelligence data from a variety of sources, such as malware analysis platforms, incident reports, and threat feeds

ISSN:2170161X | E-ISSN: 2588-2082 | Vol.15 Issue2 (Dec 2025)

(Tounsi and Rais, 2018). To find out where visibility is lacking and where threat coverage is lacking, these volumes are examined and superimposed with ATT&CK procedures. The last step, as stated by Jadidi and Lu (2021), is to formulate hunting hypotheses, which entails focusing on the harmful actions of particular enemies according to how often they occur and the possible outcomes of those actions. The next step is to incorporate machine learning techniques to sift through mountains of telemetry data for proof that these hypotheses are correct. According to Chen et al. (2022), real-world incident investigations with continuously labeled data and observations should be used to train and validate ML models. The model is finally put into action with the use of SIEM and SOAR systems. Analysts are guided through the processes of threat investigation via playbooks, alerting functionality, and visualization of the SOC network (Al-Sada et al., 2023).

5.3. Tools and Technologies for Implementation

A combination of security analytics, machine learning frameworks, and threat intelligence platforms would be required to manage this model. The MISP platform is one example of a threat intelligence platform (TIP) that allows teams to consume, standardize, and exchange CTI (Ammi and Jama, 2023). The MITRE ATT&CK framework is often directly integrated with these platforms, enabling the clear overlap of TTPs. Network traffic analysis (NTA) and endpoint detection and response (EDR) systems gather data in real-time in behavior-based telemetry. Machine learning (ML) toolkits like Scikit-learn, TensorFlow, or PyTorch are commonly used to build and train models that may identify abnormalities or categorize events according to patterns of hostile behavior (Bharadiya, 2023; Martinez Torres et al., 2019). In addition, decision-makers and hypothesis-validators can use threat activity and detection coverage visualization tools like ATT&CK Navigator or Kibana (Kinnunen, 2022). Platforms like RedAI (Noel, 2021) show how AI can automate intelligence extraction and find patterns and linkages in threat hunting operations. Working in tandem, they form the backbone of a CTI-driven threat hunting architecture, which allows SOCs to swiftly and accurately detect and respond to multidimensional threats.

6. Case Studies and Practical Applications

6.1. Examples of SOCs Utilizing the Model

In order to improve threat detection and response, a number of enterprise-grade SOCs have started using models based on cyber threat intelligence, which incorporate MITRE ATT&CK and machine learning. One example is the threat hunting paradigm that Telefonica's SOC has put into place. This paradigm uses intelligence derived from both internal adversary activities and external threat feeds to convert observed adversary behaviors into ATT&CK tactics (Roy et al., 2023). Better prioritization and the discovery of previously unseen dangers were both made possible by the procedure. Similar to how ATT&CK and CTI were brought to the attention of the IBM X-Force threat hunting team, they were able to proactively identify threat actors like FIN7 and APT29 by combining machine learning classifiers to harmonize patterns of behavior across

ISSN:2170161X | E-ISSN: 2588-2082 | Vol.15 Issue2 (Dec 2025)

different telemetry sources (Tounsi and Rais, 2018). With the help of cross-team communication and contextual intelligence derived from known adversary playbooks, their model enhanced detection speed. These cases show that it is possible to improve proactive protection methods in SOC environments by combining structured intelligence with detection processes that are augmented with machine learning.

6.2. Lessons Learned from Real-World Applications

Use of these models has also revealed useful information about problems and successes that make them work. One of the most important takeaways is how to define machine learning algorithms using context-rich threat knowledge. Without high-quality, focused CTI, ML models often fail to detect generalization or produce false positives (Jadidi and Lu, 2021). As for the second finding, it is the mapping of CTI to MITRE ATT&CK. This makes threat analysis standardized across teams, which in turn makes it easier to explain adversary actions and reaction plans consistently. However, businesses have also realized that not all threat hunting processes can be automated just yet; human analysts are still needed for things like validating occurrences, understanding context, and coming up with hypotheses (Noel, 2021). In addition, the examples show that feedback loops between ML systems and analysts are essential for adaptability and continual improvement. The effectiveness of the approach relies on iterative adjustment and strong connections among people, processes, and technologies.

6.3. Metrics for Evaluating Effectiveness

Typically, SOCs use a mix of quantitative and qualitative measures to measure the efficacy of a threat hunting model driven by CTI. Precision and recall, two important technical metrics for evaluating the efficiency of machine learning elements, are also used to estimate the accuracy of detection and evaluation (Chen et al., 2022). The other operational metrics that indicate the SOC's overall responsiveness and agility are the mean time to detect (MTTD) and the mean time to respond (MTTR). When it comes to threat intelligence, one way to gauge how visible adversary activities are is by using the mapping of MITRE ATT&CK methodologies. Additionally, the SOC's threat hunting capability is evaluated by looking at the ratio of threats recognized to responses and the percentage of threats resolved during proactive hunting, rather than relying on reactive alerts (Kinnunen, 2022). Important factors in improving the model include analyst experience and the post-incident review. In the end, a successful implementation shows that analysts are more aware of APTs, operational efficiency is up, and their decision-making is better based on behavioral and intelligence models.

7. Challenges and Considerations

7.1. Common Obstacles in Threat Hunting

A number of ongoing difficulties make threat detection in large-scale Security Operations Centers (SOCs) an already formidable task. Situations where even the most well-resourced SOCs experience alert fatigue due to an excessive amount of data collected on enterprise networks illustrate the first major challenge. When attackers use sophisticated evasion strategies or sneaky

ISSN:2170161X | E-ISSN: 2588-2082 | Vol.15 Issue2 (Dec 2025)

tactics like living-off-land techniques to blend in and behave like usual activities, analysts would have a hard time telling the difference between harmless anomalies and real threats (Tounsi and Rais, 2018). Furthermore, static detection rules are insufficient in a threat environment where tactics, methods, and procedures (TTPs) are continually changing. As a result of different analyst abilities and the lack of standardized threat hunting processes, teams frequently produce variable results and are less effective overall.

Figure 4. Security Operations Centers (SOCs)

7.2. Addressing Data Quality and Integration Issues

Endpoint logs, network traffic, security warnings, external threat feeds, and the quality of these data sources are crucial to threat hunting. However, discrepancies in data formats, timestamps, and labeling might impair the effectiveness of machine learning algorithms, which can lead to problems with detection (Rcanet al., 2023) and other related concerns. Further integration of CTI into the workflow is challenging due to its disaggregated nature and the fact that sources' depth and confidence vary. Data validation and parsing tools are necessary to make data compatible with the MITRE ATT&CK architecture, which is necessary for data mapping and the detection of known adversary actions. Furthermore, the advantages of explicit telemetry can be at odds with data privacy and security, which can lead to ethical and legal dilemmas. Solutions usually include data standardization, powerful threat intelligence platforms (TIPs), and enhanced real-time data intake and correlation.

7.3. Balancing Automated and Manual Threat Hunting Efforts

A completely automated threat hunting system is an impractical long-term objective, despite the fact that machine learning and automation in and of themselves offer efficiency and scalability. Intuition, domain expertise, and situational awareness are the three pillars upon which threat

ISSN:2170161X | E-ISSN: 2588-2082 | Vol.15 Issue2 (Dec 2025)

detection and response rest. Security operations centers must strike a careful balance when using automated and manual analytics. Automatic systems can help with alert prioritization, anomaly identification, and ATT&CK mapping proposal, but human analysts are still needed for hypothesis testing, threat validation, and action selection (Jadidi and Lu, 2021). Excessive automation might cause blind spots, while analysts can experience burnout and a lack of response due to over-intervention. Machine learning should not be utilized in place of human judgment or expertise, but rather as an adjunct to it. A hybrid approach is thus required. In order to maximize the potential of both humans and AI, it is crucial to foster an environment that encourages teamwork and continuous learning within SOC teams. Consistent red teaming exercises, post-incident evaluations, and the analyst-ML system feedback loop can all contribute to the gradual improvement of the threat models.

8. Future Trends in Threat Hunting

8.1. Advances in Machine Learning and AI in Cybersecurity

The development of threat hunting in the future is highly dependent on ML and AI. More sophisticated and proactive detection is becoming possible as a result of advancements in these technologies. Cybersecurity data is seeing a surge in the use of machine learning techniques like deep learning, reinforcement learning, and unsupervised anomaly detection, which can uncover irregularities that rule-based systems miss. To operationalize AI in SOC operations, explainable AI (XAI) is also becoming an important enabler by improving analysts' understanding and trust in ML model judgments. Furthermore, computers may automatically scan threat reports, incident reports, and CTI feeds using natural language processing (NLP) techniques. This transforms unstructured data into actionable intelligence. These advancements will make it easier for analysts to recognize and prioritize threats more quickly and accurately while also reducing the cognitive load on them.

8.2. Evolving Threat Landscape and Implications for SOCs

Security operations centers will face pressure to adjust some of its threat hunting procedures as a result of cyber threats that are increasingly sophisticated, persistent, and covert. When it comes to using complex TTPs that mesh nicely with the lawful system action, both nation-state and organized cybercriminal domains are always working to improve their tradecraft. Deploying cloud-native infrastructures increases the attack surface, and visibility and control are further complicated by distant workers and mobile endpoints. Security operations centers (SOCs) must undergo a transformation by integrating MITRE ATT&CK mapping with endpoint detection and response (EDR) capabilities, real-time behavioral analytics, and threat information sharing through federations. Threat hunters will also have to deal with an uptick in AI-written malware and polymorphic assaults, which alter their look to evade detection. With the help of intelligence-driven operations that can adapt to the enemy's moves in real time, SOCs will need to make the transition from reactive to proactive defense models.

ISSN:2170161X | E-ISSN: 2588-2082 | Vol.15 Issue2 (Dec 2025)

8.3. Predictions for the Future of Threat Hunting Practices

The future of threat hunting is an enterprise-wide endeavor that will become self-sufficient through the use of input services, contextual intelligence, and a never-ending cycle of learning. Hunting techniques will be more uniform and SOC tools will be more interoperable when ML-enabled automation meets frameworks like MITRE ATT&CK. Additionally, it will be more predictive, using attack history, behavioral baselines, and analytics to spot impending dangers before they happen. Furthermore, security investigations will be able to work together more effectively thanks to cloud-native threat hunt platforms that enable dispersed and collaborative investigations. Security operations centers (SOCs) are becoming more integrated with threat intelligence platforms and SOAR solutions, which means that the time it takes to identify a problem and then fix it will be much shorter. Secondly, in order to integrate cybersecurity objectives with company risk management, the future threat hunter will act more like a conductor of smart systems, bringing a strategic perspective to the table instead of relying just on technical knowledge.

9. Conclusion

In order for large-scale SOCs to detect and eliminate complex cyber threats, intelligence-driven and automated threat hunting has become crucial. Organizations can take a proactive approach to defense by combining Machine Learning technologies, the MITRE ATT&CK methodology, and Cyber Threat Intelligence services. The methodology enables SOC analysts to automate behavior-based detection, produce focused hypotheses, and prioritize risks with more precision. Anomalies necessitate CTI context, and ATT&CK provides a methodical approach to describing opponent actions. Even further, machine learning enables pattern detection, anomaly categorization, and large-scale dataset prediction.

Still, good data, human oversight at all times, and harmony between automated and human-operated processes are the three pillars upon which these models rest. Threats are always evolving, thus SOCs need to be nimble to stay relevant. This means using collaborative and predictive methods that are in line with current technology and real-time data. In the end, a model for corporate security against advanced cybercrime that is diverse, flexible, and future-proof may be found at the confluence of CTI, ATT&CK, and ML.

References

Sree, V. S., Koganti, C. S., Kalyana, S. K., and Anudeep, P. (2021, October). Artificial intelligence-based predictive threat hunting in the field of cybersecurity. In 2021 2nd Global Conference for Advancement in Technology (GCAT) (pp. 1–6). IEEE.

Chakraborty, S., and Nisha, T. N. (2022, October). Next generation proactive cyber threat hunting-A: A complete framework. In AIP Conference Proceedings (Vol. 2519, No. 1, p. 030093). AIP Publishing LLC.

ISSN:2170161X | E-ISSN: 2588-2082 | Vol.15 Issue2 (Dec 2025)

Bolla, A., and Talentino, F. (2022). Threat Hunting Driven by Cyber Threat Intelligence (Doctoral dissertation, Politecnico di Torino).

Vielberth, M., Böhm, F., Fichtinger, I., and Pernul, G. (2020). Security operations center: A systematic study and open challenges. IEEE Access, 8, 227756-227779.

Muniz, J. (2021). The modern security operations center. Addison-Wesley Professional.

Noel, L. (2021). RedAI: A machine learning approach to cyber threat intelligence.

Al-Sada, B., Sadighian, A., and Oligeri, G. (2023). Analysis and characterization of cyber threats leveraging the MITRE ATT&CK database. IEEE Access, 12, 1217–1234.

Chukwu, C. J. (2023). Leveraging the MITRE ATT&CK Framework to Enhance Organizations' Cyberthreat Detection Procedures (Doctoral dissertation, Carleton University).

Roy, S., Panaousis, E., Noakes, C., Laszka, A., Panda, S., and Loukas, G. (2023). Sok: The MITRE attack framework in research and practice. arXiv preprint arXiv:2304.07411.

Georgiadou, A., Mouzakitis, S., and Askounis, D. (2021). Assessing Mitre Attack Risk Using a Cybersecurity Culture Framework. Sensors, 21(9), 3267.

Kinnunen, J. (2022). Threat Detection Gap Analysis Using MITRE ATT&CK Framework.

Shin, C., Lee, I., and Choi, C. (2023). Exploiting ttp co-occurrence via GloVe-based embedding with ATT&CK, the MITRE ATT&CK framework. IEEE Access, 11, 100823–100831.

Jadidi, Z., and Lu, Y. (2021). A Threat Hunting Framework for Industrial Control Systems. IEEE Access, 9, 164118- 164130.

Kulkarni, M. S., Ashit, D. H., and Chetan, C. N. (2023, November). A Proactive Approach to Advanced Cyber Threat Hunting. In 2023 7th International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS) (pp. 1–6). IEEE.

Yang, W., and Lam, K. Y. (2019, December). Automated cyber threat intelligence report classification for early warning of cyber attacks in the next-generation SOC. In International Conference on Information and Communications Security (pp. 145-164). Cham: Springer International Publishing.

Ainslie, S., Thompson, D., Maynard, S., and Ahmad, A. (2023). Cyber-threat intelligence for security decision- making: A review and research agenda for practice. Computers and Security, 132, 103352.

Abu, M. S., Selamat, S. R., Ariffin, A., and Yusof, R. (2018). Cyber Threat Intelligence: Issues and Challenges. Indonesian Journal of Electrical Engineering and Computer Science, 10(1), 371–379.

Mavroeidis, V., and Bromander, S. (2017, September). Cyber threat intelligence model: an evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence. In 2017 European Intelligence and Security Informatics Conference (EISIC) (pp. 91-98). IEEE.

Möller, D. P. (2023). Threats and threat intelligence. In Guide to cybersecurity in digital transformation: Trends, methods, technologies, applications and best practices (pp. 71–129). Cham: Springer Nature Switzerland.

ISSN:2170161X | E-ISSN: 2588-2082 | Vol.15 Issue2 (Dec 2025)

Tounsi, W., and Rais, H. (2018). A survey on technical threat intelligence in the age of sophisticated cyber attacks. Computers and security, 72, 212–233.

Ammi, M., and Jama, Y. M. (2023). Cyber Threat Hunting Case Study using MISP. J. Internet Serv. Inf. Secur., 13(2), 1-29.

Bharadiya, J. (2023). Machine learning in cybersecurity: Techniques and challenges. European Journal of Technology, 7(2), 1-14.

Martínez Torres, J., Iglesias Comesana, C., and García-Nieto, P. J. (2019). Machine learning techniques applied to cybersecurity. International Journal of Machine Learning and Cybernetics, 10(10), 2823-2836.

Handa, A., Sharma, A., and Shukla, S. K. (2019). Machine learning in cybersecurity: A review. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 9(4), e1306.

Shon, T., and Moon, J. (2007). A hybrid machine learning approach to network anomaly detection. Information Sciences, 177(18), 3799–3821.

Katragadda, S., Kehinde, O., and Kezron, I. E. (2020). Anomaly detection: Detecting unusual behavior using machine learning algorithms to identify potential security threats or system failures. International Research Journal of Modernization in Engineering Technology and Science, 2(5), 1342-1350.

Omar, S., Ngadi, A., and Jebur, H. H. (2013). Machine Learning Techniques for Anomaly Detection: An Overview. Int\\ernational Journal of Computer Applications, 79(2).

Rastogi, N., and Alam, M. T. (2023). Cyber Threat Intelligence for SOC Analysts.

Chen, C. K., Lin, S. C., Huang, S. C., Chu, Y. T., Lei, C. L., and Huang, C. Y. (2022). Building a machine learning-based threat hunting system from scratch. Digital Threats: Research and Practice (DTRAP), 3(3), 1-21.

Nour, B., Pourzandi, M., and Debbabi, M. (2023). A survey on threat hunting in enterprise networks. IEEE Communications Surveys and Tutorials, 25(4), 2299–2324.

Wajid, F., and Shah, W. (2021). AI-Driven Threat Hunting: Revolutionizing SOC Capabilities for Advanced Cyber Defense.

Mahesh Channapatna Girish (May 13, 2023). Why SOC is Crucial for Protecting Your Business: Understanding the Importance of the Security Operations Centre. https://maheshcg.me/why-soc-is-crucial-for-protecting-your- business-understanding-the-importance-of-security-operations-centre/

Majid, M. A., and Ariffin, K. A. Z. (2021). Model for the successful development and implementation of Cyber Security Operations Centre (SOC). PLoS ONE, 16(11), e0260157. https://doi.org/10.1371/journal.pone.0260157

Grant McDonald (March 12, 2021). The MITRE ATT&CK Framework Explained.

https://www.bmc.com/blogs/mitre-attack-framework/Cyber Threat Intelligence explained in 5 steps, November 9, 2022. https://www.intellisync.it/2022/11/09/what-is-the-cyber-threat-intelligence-cti-explained-in-5-steps/