World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Check for updates

Threat hunting in large-scale SOCs: A cyber threat intelligence-driven model using MITRE ATTandCK and machine learning

Tim Abdiukov *

NTS Netzwerk Telekom Service AG.

World Journal of Advanced Research and Reviews, 2024, 21(03), 2679-2689

Publication history: Received on 01 February 2024; revised on 21 March 2024; accepted on 28 March 2024

Article DOI: https://doi.org/10.30574/wjarr.2024.21.3.0830

Abstract

The scale of large-scale Security Operations Centers (SOCs) has led to a serious need for implementing proactive security solutions, as cyber threats have become more complex and elusive. The proposed paper introduces a unified threat hunting model that integrates Cyber Threat Intelligence (CTI), the MITRE ATTandCK framework, and Machine Learning (ML) to enhance threat detection, investigation, and response. The paper sets out with an explanation of the changing role of threat hunting in contemporary SOCs and addresses the way CTI provides contextual information to adversaries. It also discusses the structural strengths of the MITRE ATTandCK framework and demonstrates how machine learning methods can be utilized to identify patterns that cannot be observed with conventional tools. A CTI-based model is subsequently proposed, along with an explanation of its structure, development process, and enabling technologies. The practical use of the model and its benefits are illustrated in real-life case studies. At the same time, a discussion of the main challenges, including data integration and trade-offs between automation, provides the background for exploring future trends. This paper concludes that an intelligence-driven, behavior-based, and machine learning-enhanced approach to threat hunting is a critical measure to ensure that SOCs remain several steps ahead of the adversary in a rapidly evolving strategic environment.

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

Threat hunting is an active process of cybersecurity in which analysts proactively search through networks, datasets, and systems to identify and counter threats that evade commonly used security measures, such as firewalls, SIEMs, or antivirus software. In contrast to reactive strategies, threat hunting relies on human intuition and paying specific attention to context, proactive comprehension, and investigation rather than being alert-dependent. Nour et al. (2023) describe a threat-hunting process as a hypothesis-based search that fills the gap in detection by revealing indicators of compromise (IOCs) and tactics, techniques, and procedures (TTPs) used by adversaries. Such a process is especially significant in the modern threat environment, where threats in the form of advanced persistent threats (APTs) and stealthy attackers frequently go undetected by conventional methods (Chakraborty and Nisha, 2022). Kulkarni et al. (2023) state that a proactive threat hunting approach not only reduces dwell time but also improves incident response and threat containment, ultimately enhancing the overall cyber resilience of an organization.

* Corresponding author: Tim Abdiukov.

1.2. Overview of Security Operations Centers (SOCs)

Security Operations Centers (SOCs) represent the centralized entities within organizations that are involved in continuous monitoring, identification, analysis, and response to cybersecurity incidents. SOCs provide a platform for threat interception and response because they integrate technology, human efforts, and procedures into a single defense system. According to Vielberth et al. (2020), contemporary SOCs address issues of excessive alerts, a lack of talent, and the need to synchronize various security tools. With cyber threats becoming more advanced, the change to intelligence-driven and automated SOCs, commonly known as the next-generation SOCs, is needed (Muniz, 2021). With the use of cloud, advanced analytics, machine learning, and cyber threat intelligence (CTI), these next-generation SOCs can enhance their situational awareness and decision-making capabilities.

Figure 1 Conceptual model for the success of SOC establishment

1.2.1. Purpose of Integrating Cyber Threat Intelligence with MITRE ATTandCK and Machine Learning

The combination of Cyber Threat Intelligence (CTI), MITRE ATTandCK, and Machine Learning (ML) is the game changer in the future of threat hunting. CTI offers situational awareness of threats, whereas the MITRE ATTandCK framework offers an organized list of adversarial TTPs arranged across the attack lifecycle. Machine learning is used to improve detection by identifying abnormal behavior and automatically analyzing the data. A combination of these three terms creates the paradigm of active and adaptive threat hunting: CTI-MITRE ATTandCK-ML. Bolla and Talentino (2022) note that aligning threat hunting with CTI and ATTandCK enables more precise hunts, thereby avoiding false positive results and enhancing the accuracy of the process. In the meantime, Sree et al. (2021) emphasize that integrating AI and ML into this unified model is associated with improved threat prediction and the possibility for SOCs to identify previously unknown or zero-day threats. Finally, this holistic approach also makes threat hunting in large SOCs scalable, intelligence-based, and enables them to adapt to the changing behavior of adversaries (Roy et al., 2023).

2. Understanding the MITRE ATTandCK Framework

2.1. Overview of MITRE ATTandCK

The MITRE ATTandCK (Adversarial Tactics, Techniques, and Common Knowledge) knowledge base is a globally recognized cyber intelligence resource that details and categorizes the actions of an adversary throughout the entire cyber-attack life cycle. Designed by the MITRE Corporation, it aims to establish a common language for describing and examining threats, providing defenders with a guide on how threat actors operate after gaining access to a system (Roy et al., 2023). The framework enables security teams to develop a more effective understanding of how attackers operate and implement their strategies, allowing for the identification and response to them through a systematic categorization of known tactics, techniques, and procedures (TTPs). Georgiadou et al. (2021) mention that ATTandCK serves as a mediator between threat intelligence and defensive counteractions, thus being a fundamental tool in threat modeling and adversary emulation.

Figure 2 The ATTandCK Matrix for Enterprise (categories of enterprise tactics across the attack lifecycle)

2.2. Key Components and Tactics

MITRE ATTandCK is divided into tactics, techniques, and sub-techniques. Tactics refer to the technical objectives of the adversary, such as privilege escalation, lateral movement, or data exfiltration. Techniques refer to the methods used to accomplish the objective. Sub-techniques offer finer granularity in each technique. The framework also includes mappings to the groups of threats and software used in real-world attacks, making it much more applicable in the field of operation, as explained by Roy et al. (2023). Kinnunen (2022) also points out that the structure of ATTandCK enables organizations to analyze gaps and prioritize detection activities, allowing them to identify what is already being monitored and what should be covered. We also have ATTandCK matrices customized for different platforms, including enterprise systems, mobile devices, and industrial control systems (ICS), which offer flexibility in diverse security situations.

2.3. Relevance of ATTandCK in Threat Hunting

The MITRE ATTandCK framework can be used as a reference for instruction when conducting threat hunting. It allows analysts to create hypotheses using known TTPs and enables them to map adversary detection use cases to behaviors they are known to demonstrate within the wild (Chukwu, 2023). The framework also allows the enhancement of threat intelligence through the use of structured mappings between the behavior of threat actors and defensive capabilities. Al-Sada et al. (2023) also note that the application of ATTandCK enhances detection fidelity through a behavior-based approach, further improving detection by mitigating the issue of static indicators being easily outdated by common evasion methods. In addition, integrating ATTandCK into the machine learning models and intelligence platforms related to threats permits growing automation, thereby allowing large-scale SOCs to discover connected data and identify unrecognized risks (Shin et al., 2023). This form of behavior ultimately changes the aspect of threat hunting into a proactive and intelligence-based concept.

3. The Role of Cyber Threat Intelligence

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

The process of gathering, analyzing, and correlating data about potential or current cyber threats to inform security decisions is known as Cyber Threat Intelligence (CTI). It provides background information on how and why threat actors acted, as well as their tools and methodologies, thereby forming part of proactive cybersecurity. According to Ainslie et al. (2023), CTI refers to the evidence-based knowledge that helps a defender make informed decisions when balancing,

detecting, responding to, and recovering from cyber incidents. CTI has assumed critical importance in large-scale Security Operations Centers (SOCs) in handling the quantity and complexity of threats to the enterprise environment. According to Tounsi and Rais (2018), integrating CTI makes passive security more vulnerable, as one can foresee the moves of adversaries. Möller (2023) notes that CTI supports both technical and strategic operations, including incident response, risk assessment, policy enforcement, and security investment decisions. CTI brings a much-needed boost to the arena of modern threat environments, characterized by constant and dynamic attacks, creating a level of uncertainty and a lack of security acumen.

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

CTI can be broadly categorized into strategic, tactical, and operational intelligence, each of which plays a distinct role in the security lifecycle. Long-term, high-level assessments of new threats and geopolitical trends, as well as trends in cybercrime, are provided through strategic intelligence. Designed to facilitate executive decision-making, the form of intelligence provides a macro-level perspective into a threat landscape (Abu et al., 2018**).** Tactical intelligence specializes in the methods, scripts, and systems of adversaries, including indicators of compromise (IOCs), malware scripts, phishing websites, and vulnerability exploits. It is most useful to SOC analysts and threat hunters who need technical granularity to build detection measures and incident response playbooks (Mavroeidis and Bromander, 2017). Operational intelligence provides time-bound information on ongoing or impending attacks. This consists of telemetry data, behavioral analytics, and adversary infrastructure information that helps in real-time decision-making when responding to an incident. As Yang and Lam (2019) note, active CTI is essential in forecasting and eliminating threats early and on schedule. Implemented comprehensively, these three levels of intelligence would equip SOCs with a multi-layered defense plan, comprising strategic foresight, tactical preparedness, and operational responsiveness.

3.3. How CTI Informs Threat Hunting Efforts

With the inclusion of CTI into threat hunting, the accuracy and scope of investigations are increased. Threat hunting is, by nature, typically hypothesis-driven and requires an active search for signs of malicious activity that may not be detected through automated detection tools. CTI accelerates this task by providing threat hunters with actionable intelligence (including those of adversary TTPs, known attack vectors, campaign indicators), which can be remixed into specific, focused hypotheses to guide hunting. Based on the research conducted by Bolla and Talentino (2022), threat hunting based on CTI significantly reduces investigative overhead, allowing analysts to focus on high-risk behaviors and potential attack patterns. Entered into specific frameworks, such as MITRE ATTandCK, threat intelligence provides an empirical platform that enables the development of anomaly-based identification of adversary behavior specific to adversary profiles (Roy et al., 2023).

Additionally, CTI, as noted by Rastogi and Alam (2023), provides a more contextual flavor of raw data gathered at the endpoint, on a network, or in the cloud, which simplifies the task of analysts in determining whether a given anomaly is benign or a legitimate threat. In addition to this, CTI assists in automation by supplying enriched intelligence into SIEMs, SOAR platforms, and machine learning models, thereby increasing the detection accuracy of these tools and reducing the hunt cycle. Essentially, CTI helps threat hunting evolve from an ad-hoc task performed manually to a structured one, following the lines of intelligence-led threat hunting that corresponds to the types of threats out there and the adversarial methodologies employed.

4. Integrating Machine Learning in Threat Hunting

4.1. Overview of Machine Learning Concepts

Machine Learning (ML) is a branch of artificial intelligence (AI) that enables systems to learn and make decisions, drawing conclusions and making predictions based on data. It utilizes algorithms that improve as they process more data and perform more effectively over time. ML finds an essential application in the cybersecurity sector, complementing existing security strategies to ensure that threat mitigation and classification are automatically performed. According to Shon and Moon (2007), ML can be particularly useful in settings where the amount of data and its complexity exceed the abilities of people to analyze it.

The most notable paradigms of ML, including supervised, unsupervised, and reinforcement learning, enable cybersecurity systems to identify targeted known threats, detect new anomalies that have never been seen before, and dynamically respond to new attack methodologies. Martinez Torres et al. (2019) identify the following adaptability as the reason why ML is a highly suitable tool for complementing reactive and proactive security measures, including threat hunting.

4.2. Applications of Machine Learning in Cybersecurity

Security technologies feature intrusion detection, malware classification, phishing detection, and behavioral analysis, which rely increasingly on machine learning techniques. In the specific case of threat hunting, ML enables SOCs to identify thinly veiled patterns and changes that deviate from typical behavior, which can indicate a threat. As Omar et al. (2013) point out, zero-day malware attacks and insider threats would not be detected by rule-based systems, as ML-driven anomaly detection devices could discover them. Likewise, Bharadiya (2023) highlights that clustering, classification, and dimensionality reduction methods are applied to identify malicious actions that are buried in a vast amount of security data. In addition to this, the combination of ML and cyber threat intelligence enables predictive analytics, through which systems can predict likely attacks using past data and patterns of cyber threat actors (Sree et al., 2021). New tools, such as RedAI (Noel, 2021) and systems suggested by Chen et al. (2022), prove that ML-based platforms are becoming more mature and ready to facilitate real-time and near-real-time detection processes within the SOC.

4.3. Benefits of Using ML for Threat Detection and Analysis

The application of machine learning in threat hunting and investigation processes provides several key advantages in large-scale and data-intensive settings. ML can first identify threats that are accurately detected by recognizing both known and unknown threats, depending on its learned patterns of behavior. By eliminating benign anomalies and leaving high-confidence alerts, it can diminish false positives, which are also prominent in traditional security tools (Katragadda et al., 2020). Second, ML enables scaling for threat detection, allowing continuous scouting and analysis of vast datasets across networks, endpoints, and cloud environments without compromising performance (Handa et al., 2019). Third, ML contributes to responsive agility since it allows systems to respond to changing TTPs that adversaries use. Chakraborty and Nisha (2022) report that machine learning algorithms can be continuously retrained with new threat intelligence, enabling them to address changing threat conditions. Moreover, the joint application of ML and frameworks like MITRE ATTandCK enables the development of a systematic and automated way to match observed behaviors with known tactics and techniques (Shin et al., 2023). This integration will enable SOCs to enhance their threat visibility, minimizing dwell time and enabling more effective use of threat intelligence throughout operations. Finally, machine learning transforms threat hunting into a scalable, dynamic, and intelligence-driven field that is less manual.

5. Developing a Cyber Threat Intelligence-Driven Model

5.1. Framework for Integrating CTI with MITRE ATTandCK

Contextual threat intelligence can be combined with structured adversary behavior frameworks in a model to translate threat hunting into a cyber threat intelligence-driven approach, providing a higher degree of detection and investigation of threats within the SOCs. It aligns with the MITRE ATTandCK framework, a standardized taxonomy of tactics and techniques that can be referred to as mappings of threat intelligence feeds. According to Bolla and Talentino (2022), such correspondence enables analysts to transform high-level threat intelligence into definite, technical operations and indications in operational settings. When the model commences, it usually engages in the process of identifying relevant threat actor profiles and TTPs that would be mapped into the ATTandCK matrix. Roy et al. (2023) note that these mappings can be utilized to generate proactive hunting hypotheses and develop detection logic based on adversary behavior, rather than relying on reactive indications. Correlating intelligence with the ATTandCK structured framework can help SOCs ensure alignment of strategy around threats and tactical threat detections, facilitating more appropriate prioritization and response.

Figure 3 The Threat Intelligence Life Cycle

5.2. Steps for Model Development

The evolution process (building an intelligence-based threat hunting model) is divided into several logical stages that combine CTI, behavioral structures, and machine learning. First, the organizations are required to collect and standardize threat intelligence data from various sources, including threat feeds, incident reports, and malware analysis platforms (Tounsi and Rais, 2018). These volumes are then analyzed and overlaid against ATTandCK techniques to identify areas that require improvement in visibility and threat coverage gaps. The next stage, according to Jadidi and Lu (2021), involves developing hypotheses about hunting, i.e., targeting the adverse behavior of specific adversaries based on the frequency and potential consequences of those behaviors. Machine learning systems are then added to analyze vast amounts of collected telemetry data in search of evidence that supports these suppositions. Chen et al. (2022) advocate for training and validating ML models on continually labeled data and observations from actual field investigations of incidents. Lastly, the model is operationalized using SIEM and SOAR solutions, directed by playbooks, alerting functionality, and visualization of the SOC network, which helps guide analysts through the steps of investigating a threat (Al-Sada et al., 2023).

5.3. Tools and Technologies for Implementation

Managing this model would need a mix of threat intelligence platforms, ML frameworks, and security analytics. An example of threat intelligence platforms (TIPs) is MISP (Ammi and Jama, 2023), through which CTI is ingested, normalized, and shared among teams. These platforms tend to utilize direct integration with the MITRE ATTandCK framework, allowing for the unmistakable overlap of TTPs. In behavior-based telemetry, data is collected in real-time by endpoint detection and response (EDR) systems and network traffic analysis (NTA). To create and train a model capable of detecting anomalies or classifying events based on patterns of adversarial behavior, one often uses ML toolkits, such as Scikit-learn, TensorFlow, or PyTorch (Bharadiya, 2023; Martinez Torres et al., 2019). Moreover, detection coverage and threat activity are visualized using tools such as Kibana or ATTandCK Navigator, which help validate hypotheses and inform decisions (Kinnunen, 2022). Platforms such as RedAI (Noel, 2021) also demonstrate how AI can be integrated into threat hunting processes to automate the extraction of intelligence and identify patterns and relationships between them. As a combination, they comprise the technical core of a CTI-driven threat hunting architecture, enabling SOCs to respond to multidimensional threats with greater velocity and accuracy in detection and response.

6. Case Studies and Practical Applications

6.1. Examples of SOCs Utilizing the Model

Several enterprise-grade SOCs have begun to apply cyber threat intelligence-based models, incorporating MITRE ATTandCK and machine learning, to enhance threat Detection and response. The SOC at Telefonica has, for example, implemented a threat hunting paradigm that translates the behaviors observed of enemy adversaries into ATTandCK techniques, utilizing intelligence developed from both in-house adversary actions and external threat feeds (Roy et al., 2023). The practice enabled prioritization of better and helped uncover new threats that had not been identified before. In the same way, ATTandCK and CTI were introduced to the IBM X-Force threat hunting team to enable proactive identification of threat actors, such as FIN7 and APT29, due to their capability to harmonize patterns of behavior across various telemetry sources by combining machine learning classifiers (Tounsi and Rais, 2018). In their model, the detection speed was improved, along with cross-team cooperation, providing contextual intelligence based on known adversarial playbooks. These examples illustrate the practical feasibility of integrating structured intelligence with machine-learning-enhanced detection processes to enhance proactive defense strategies in SOC environments.

6.2. Lessons Learned from Real-World Applications

The application of these models has also generated important insights into issues and areas of success that contribute to their effectiveness. Among the major lessons is the meaning of context-rich threat intelligence in defining machine learning algorithms. ML models tend to have difficulty with false positives or lack generalization detection without quality targeted CTI (Jadidi and Lu, 2021). The second thing found is the mapping of CTI to MITRE ATTandCK, which leads to the standardization of threat analysis across teams, resulting in a consistent explanation of adversary behaviors and response plans. Nevertheless, organizations have also learned that not all threat hunting operations can currently be fully automated; human analysts still play a crucial role in developing hypotheses, interpreting context, and validating incidents (Noel, 2021). Additionally, examples suggest that implementing feedback loops between ML systems and analysts is crucial for the process of continuous improvement and adaptation. Iterative tuning, along with close links among people, processes, and technologies, is key to the model's success.

6.3. Metrics for Evaluating Effectiveness

The effectiveness of a CTI-driven threat hunting model is typically measured using a combination of quantitative and qualitative metrics by SOCs. The accuracy of detection and evaluation, measured by precision and recall, is also a major technical metric for assessing the efficiency of machine learning elements (Chen et al., 2022). The additional operational metrics are the mean time to detect (MTTD) and mean time to respond (MTTR), which denote the overall agility and responsiveness of the SOC. Within the threat intelligence context, the mapping of MITRE ATTandCK techniques is exploited to estimate the extent to which there is visibility of adversary behaviors. Moreover, the threat detection-to-response ratio and the percentage of resolved threats detected during proactive hunting, not based on reactive alerts, are used to measure the maturity of the threat hunting ability at the SOC (Kinnunen, 2022). The post-incident review, as well as analyst experience, is also crucial in refining the model. Ultimately, a successful implementation demonstrates a heightened awareness of advanced persistent threats (APTs), increased operational efficiency, and enhanced decision-making by analysts based on well-formed intelligence and behavioral paradigms.

7. Challenges and Considerations

7.1. Common Obstacles in Threat Hunting

The detection of threats in large-scale Security Operations Centers (SOCs) is already challenging, presenting several persistent challenges. The first key challenge can be explained by situations where an overwhelming amount of generated data on enterprise networks becomes too much for even the most well-resourced SOCs, causing an alert fatigue effect. Analysts would struggle to distinguish between benign anomalies and legitimate threats, especially when attackers employ highly advanced evasion methods or opt for stealthy tactics, such as living-off-land techniques, to blend in and behave as regular activity (Tounsi and Rais, 2018). Additionally, in a constantly evolving threat environment, tactics, techniques, and procedures (TTPs) rapidly change, rendering the use of static detection rules inadequate. The absence of standard threat hunting procedures among teams, combined with varying analyst skills, often results in inconsistent outcomes and reduced effectiveness.

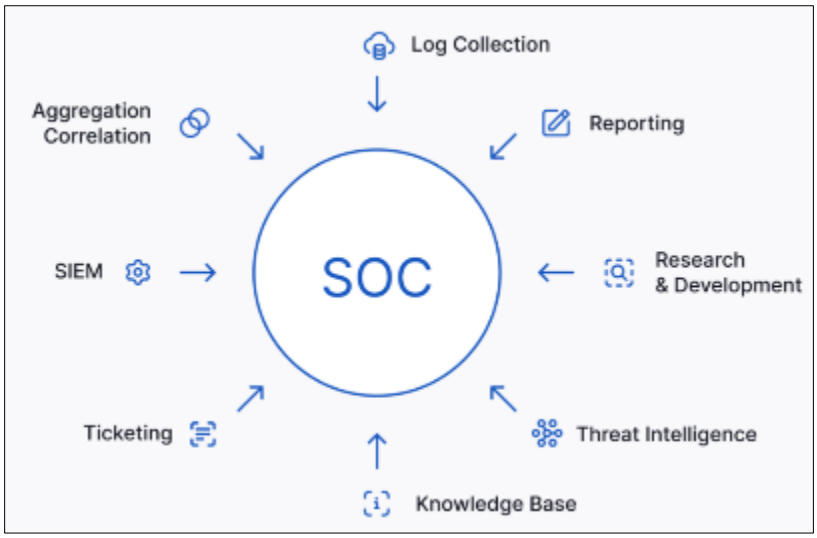

Figure 4 Security Operations Centers (SOCs)

7.2. Addressing Data Quality and Integration Issues

Threat hunting is significantly dependent on the quality and combination of various data sources, including endpoint logs, network traffic, external threat feeds, and security alerts. Nevertheless, it may create issues with machine learning algorithms and interfere with detection, as inconsistencies in data formats, timestamps, and labeling (Rcanet al., 2023) can hinder their performance. The disaggregated nature of CTI and the variation in the depth and confidence of sources make the process difficult when integrating CTI into the workflow further. Making data consistent with the MITRE ATTandCK framework to enable mapping of the data and detection of known adversary behaviors will require parsing instruments as well as validation. Additionally, there can be a legal and ethical issue between data privacy and security, and the benefits of filling out clear telemetry. Remedies typically involve implementing data normalization, utilizing high-powered threat intelligence platforms (TIPs), and employing advanced, real-time ingestion and correlation of various data streams.

7.3. Balancing Automated and Manual Threat Hunting Efforts

Although the very prospect of machine learning and automation promises scalability and efficiency, the ultimate goal of having a fully automated threat hunting system is unrealistic. The key elements in responding to and detecting threats are human intuition, specialized knowledge of a specific area, and situational awareness. The use of automated and manual analytics requires a delicate balance between the two by SOCs. With automated systems, it is possible to prioritize alerts, identify anomalies, and propose possible ATTandCK mappings; however, the primary role of human analysts in forming hypotheses, validating threats, and selecting an appropriate action remains unchanged (Jadidi and Lu, 2021). Blind spots can arise when automation is overdone, and over-intervention can lead to a lack of responsiveness as well as burnout for analysts. There is therefore a need for a hybrid approach where machine learning is not used to replace human decision or knowledge but to complement it. Additionally, promoting a culture of lifelong learning and teamwork in SOC teams is essential to harness the best of both human and artificial intelligence. The threat models can be refined over time based on regular red teaming exercises, post-incident reviews, and also through the feedback loop between analysts and the ML system.

8. Future Trends in Threat Hunting

8.1. Advances in Machine Learning and AI in Cybersecurity

Machine learning (ML) and artificial intelligence (AI) are closely tied to the future growth of threat hunting. New developments in these technologies are enabling more advanced and active detection. Machine learning techniques are being increasingly applied to cybersecurity data, with the potential to identify anomalies that are hidden from rule-based systems, including deep learning, reinforcement learning, and unsupervised anomaly detection. Explainable AI (XAI) is also emerging as a crucial enabler, enhancing analysts' comprehension and confidence in the decisions made by ML models, which is vital for operationalizing AI in SOC processes. Additionally, the application of natural language processing (NLP) techniques enables systems to automatically analyze threat reports, incident reports, and CTI feeds,

converting unstructured data into actionable intelligence. Such innovations will enable the further alleviation of the cognitive burden on analysts, allowing for quicker and more precise detection and prioritization of threats.

8.2. Evolving Threat Landscape and Implications for SOCs

Due to cyber threats being more targeted, persistent, and stealthy, SOCs will be under pressure to modify some of their threat hunting processes. Both nation-state and organized cybercriminal domains relentlessly work on improving their tradecraft by employing sophisticated TTPs that sit well with the legitimate system action. Increased attack surface through deployment of cloud-native infrastructures, and remote workers (and mobile endpoints) further complicates visibility and control. SOCs will need to transform through the use of threat intelligence sharing via federations, real-time behavioral analytics, and endpoint detection and response (EDR) tools that are tightly integrated with MITRE ATTandCK mapping. The increase in malware written by AI and polymorphic attacks, which change their appearance to avoid detection, will also need to be countered by threat hunters. The shift on the part of SOCs, therefore, requires a transformation of the existing reactive models of defense into proactive models, utilizing intelligence-driven operations that can learn and dynamically respond to the adversary's actions.

8.3. Predictions for the Future of Threat Hunting Practices

Looking forward, threat hunting will evolve into an organization-wide activity, leveraging input services, contextual intelligence, and an ongoing learning process that makes the practice independent of specialized analysts. The meeting between ML-enabled automation and frameworks such as MITRE ATTandCK will make hunting strategies consistent and enhance interoperability between SOC tools. It will also be more predictive, relying on historical attack data, behavioral baselines, and predictive analytics to identify future threats before they fully materialize. Additionally, cloud-native threat hunt platforms will facilitate investigations in a distributed and collaborative manner, thereby dissolving silos among security investigations. With an increasing integration between the SOCs and the threat intelligence platforms and security orchestration, automation, and response (SOAR) solutions, the turnaround period between the identification of the threat and the subsequent remediation will be reduced considerably. Next, the threat hunter of the future will be more of an orchestrator of intelligent systems, thinking with a strategic mindset rather than just a technical one, as we have today, in order to align cybersecurity goals with business risk management.

9. Conclusion

Intelligence-driven and automated threat hunting has become an important necessity for large-scale SOCs required to identify and resolve complicated cyber threats. The combination of various Cyber Threat Intelligence services, the MITRE ATTandCK framework, and Machine Learning technologies enables organizations to adopt a proactive defense model. The model allows SOC analysts to generate focused hypotheses, automate behavior-based detection, and prioritize threats with more precision. Anomalies need context using CTI, and ATTandCK is a systematic way to describe adversary activity. Machine learning goes further, allowing for the recognition of patterns, classification of anomalies, and prediction in large datasets.

Nevertheless, these models can only be effective due to the quality of information, constant control by a person, and the alignment of automation and manual skills. In an ever-changing environment of threats, SOCs must adapt to remain relevant through predictive and collaborative methods that reflect the latest technologies and real-time information. Ultimately, the intersection of CTI, ATTandCK, and ML represents a versatile, flexible, and future-proof model for defense against advanced cybercrime in enterprises.

References

[1] 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.

[2] 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.

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

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

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

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

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

[8] Chukwu, C. J. (2023). Leveraging the MITRE ATTandCK Framework to Enhance Organizations' Cyberthreat Detection Procedures (Doctoral dissertation, Carleton University).

[9] 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.

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

[11] Kinnunen, J. (2022). Threat Detection Gap Analysis Using MITRE ATTandCK Framework.

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

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

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

[19] 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.

[20] 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.

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

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

[23] 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.

[24] 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.

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

[26] 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.

[27] Omar, S., Ngadi, A., and Jebur, H. H. (2013). Machine Learning Techniques for Anomaly Detection: An Overview. International Journal of Computer Applications, 79(2).

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

[29] 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.

[30] 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.

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

[32] 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/

[33] 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

[34] Grant McDonald (March 12, 2021). The MITRE ATTandCK Framework Explained. https://www.bmc.com/blogs/mitre-attack-framework/

[35] 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/