# Methodology for Threat Detection and Prevention Integrating Cyber Threat Intelligence and SIEM

Alexander André de Souza Vieira[1] and João José Costa Gondim[2]

[1] University of Brasilia (UnB), Brasilia, Distrito Federal. Zip Code 70910-900, Brazil, aaalexander95@gmail.com,
[2] University of Brasilia (UnB), Brasilia, Distrito Federal. Zip Code 70910-900, Brazil, gondim@unb.br

**Abstract.** Cyber threats, such as Advanced Persistent Threats (APTs), have evolved beyond the capabilities of traditional detection methods, necessitating more sophisticated solutions. This study presents an advanced methodology to enhance threat detection and prevention by integrating Cyber Threat Intelligence (CTI) with Security Information and Event Management (SIEM) systems. The proposed approach focuses on enriching threat intelligence with additional context and using SIEM platforms to identify malicious behavior by mapping Tactics, Techniques, and Procedures (TTPs). The integration between CTI and SIEM enhances detection capabilities by correlating security events with actionable intelligence, enabling faster identification of potential threats and improving the overall accuracy of incident response. Its effectiveness is demonstrated through case studies involving real malware samples, showing significant improvements in both detection speed and precision. Additionally, the study highlights the practical benefits of using enriched intelligence in real-time scenarios, emphasizing its value in proactive defense strategies. By advancing the integration between CTI and SIEM, this work provides a scalable framework for modern cybersecurity challenges, which could be further strengthened by incorporating NLP and LLMs, contributing to the global cybersecurity community's efforts to combat evolving threats.

**Keywords:** Threat Detection, Advanced Persistent Threats, SIEM, Cyber Threat Intelligence, TTPs

## 1 Introduction

With the continuous progress of technology and increasing complexity of computing systems, new challenges and vulnerabilities have emerged related to cybersecurity. The evolution of attack techniques and tools has kept pace with system advancements, leading attackers to adopt increasingly sophisticated and stealthy methods. As a result, many modern threats can go undetected by traditional security mechanisms [1].

Cyber attacks have significantly evolved over the years. In the past, attacks were generally carried out directly and used relatively simple techniques that could be identified by signature-based tools, which worked fast and efficiently against known malware [2]. However, with the emergence of more complex threats, such as Advanced Persistent Threats (APTs), attackers now employ more advanced and covert techniques. APTs are characterized by their ability to infiltrate and remain hidden in networks and systems for extended periods, often with the goal of stealing sensitive data, compromising system integrity, or causing service disruptions [3], [4].

The nature of these threats requires a security approach that goes beyond traditional reactive techniques. In response, Cyber Threat Intelligence Platforms (TIPs) have emerged, utilizing Cyber Threat Intelligence (CTI) to enhance the detection, prevention, and response to attacks. CTI consists of detailed information about cyber threats, collected and organized to provide valuable insights into emerging threats and attack trends. This intelligence can be used to identify patterns, anticipate attacks, and implement more effective defense measures [5].

For CTI to be effective, it must meet several fundamental characteristics. It must be timely, provided quickly to allow for an effective response; relevant, contextualized to the specific environment so that the information can be practically applied; comprehensive, offering a detailed view of incidents; and clear, with standardized and structured information to facilitate analysis and decision-making [6].

The intelligence production process in TIPs follows a well-defined cycle that includes data collection, processing, analysis, and dissemination or implementation of results [7]. However, one of the main challenges TIPs face is the lack of standardization in data formats and sources, which can lead to inconsistent and low-quality intelligence production. Additionally, many TIP tools predominantly focus on the data collection phase, neglecting subsequent analysis and dissemination [8]. This limited focus can result in platforms that offer little or no improvement in threat detection and response, often becoming mere data repositories.

Based on the context presented, this work seeks to address the following research questions: RQ1 - How can the integration of cyber intelligence sources improve the detection and prevention of advanced threats, such as APTs, in a monitoring environment? RQ2 - To what extent can proactive detection based on TTPs be optimized through data enrichment in cyber intelligence platforms? RQ3 - How can the use of IoCs in monitoring, detection, and alert tools be improved for more efficient detection of persistent threats?

This work addresses these gaps by developing and evaluating a methodology for detecting and preventing cyber threats. The proposed methodology focuses on mapping TTPs and improving the quality of CTI through a data enrichment process. By integrating data from various sources and improving detection accuracy, we aim to offer a more effective solution to address modern cyber threats and enhance system security.

The remainder of this article is organized as follows: Section 2 discusses related works that support and contextualize the research. Section 3 details the proposed methodology, explaining the tools and techniques used for detecting and preventing cyber threats. Section 4 focuses on the case study, where we implemented and tested the methodology in a controlled environment, presenting the results and test validations. Finally, Section 5 provides our conclusions and outlines directions for future work.

## 2 Related Works

on Advanced Persistent Threats (APTs) has explored their evasion techniques and the limitations of traditional security measures. Several studies have proposed improvements in threat detection and the use of Cyber Threat Intelligence (CTI) to enhance defense capabilities. Existing research highlights ways to improve CTI quality, share actionable intelligence, and integrate threat intelligence into Security Information and Event Management (SIEM) systems. These studies provide insights that support our work in integrating enriched threat intelligence into detection and response processes.

The research conducted by Ghafir et al. [9] explores the exploitation of vulnerabilities by Advanced Persistent Threats (APTs) and the limitations of traditional, signature-based detection mechanisms. It further introduces a novel approach that uses alert correlation and Hidden Markov Models (HMMs) to predict APT stages, emphasizing the importance of predictive analytics and behavior-based anomaly detection for addressing sophisticated multi-stage cyberattacks.

Mahboubi et al. [10] review the evolution of threat-hunting techniques, noting how emerging technologies such as artificial intelligence and machine learning are being integrated to improve threat detection. Their study provides an in-depth look at how advanced threat-hunting strategies are becoming crucial in detecting hidden or evolving threats within networks, offering a forward-looking perspective on how organizations can enhance their cyber defenses.

Jin et al. [11] analyze the impact of CTI sharing across organizations, with a focus on the volume, timeliness, and quality of shared data. Their findings reveal that while the volume of shared CTI has increased, the depth of shared data — such as TTPs — is still limited, often resulting in less actionable intelligence. This highlights the importance of improving both the quality and the scope of CTI sharing to enhance its practical value in mitigating cyber threats.

Ainslie et al. [12] examine the essential role of Threat Intelligence Platforms (TIPs) in operationalizing Cyber Threat Intelligence (CTI), emphasizing TIPs' potential in transforming threat data into actionable insights. However, they note TIPs often fall short, primarily serving as static data repositories rather than enhancing real-time threat detection and response. The authors stress the need for TIPs to evolve in data standardization and analytical capabilities to meet modern cybersecurity demands and effectively support comprehensive threat management.

González-Granadillo et al. [13] analyze the evolution and performance of Security Information and Event Management (SIEM) systems, focusing on their application in critical infrastructures. The study reviews commercial and open-source SIEM tools, providing an extensive evaluation of their capabilities, limitations, and future enhancements. The authors emphasize the need for improved real-time detection, behavioral analysis, and incident response to address increasingly sophisticated cyber threats. This research is particularly relevant to our work as it outlines key trends and challenges for SIEM systems in complex environments, offering a roadmap for future development.

Finally, Leite et al. [14] propose an automated approach for using Cyber Threat Intelligence (CTI) during incident response, mapping TTPs in network incidents. The methodology presented allows for the creation of specific attack patterns for identified threats, facilitating the correlation between network events and CTI reports. The study demonstrated that this approach can increase the accuracy of incident detection and make responses more efficient.

In addition to these works, it is important to highlight that the integration and enhancement of TIP platforms and the detection of APTs are ongoing research areas. New approaches and technologies are constantly being developed to improve the effectiveness of cyber intelligence and system security. This work aims to contribute to this research area by proposing a methodology for detecting and preventing cyber threats that addresses the limitations of current approaches and enhances the accuracy of CTI.

## 3 Methodology

The methodology for detecting and responding to cyber incidents follows a structured cycle, consisting of steps that integrate data from various sources, enrich this information with additional intelligence, and use these correlations to identify and mitigate threats. The process described here is an evolution of that present in [14], covering a specific context of data and tools. Below, we describe the main phases of our methodology, which is generally represented in Figure 1.

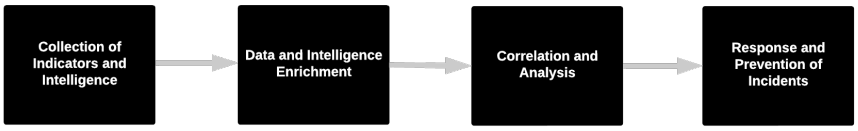


**Fig. 1.** Methodology Used

### 3.1 Collection of Indicators and Intelligence

The first step consists of collecting raw data from multiple sources, internal and external. These sources include security event logs, Indicators of Compromise (IoCs), as well as cyber threat intelligence reports. This collection encompasses structured and unstructured data, obtained from Threat Intelligence platforms and client machines used for malware execution.

The cyber intelligence platform is configured to be populated with structured security reports from public intelligence sources. This step is critical as data from various sources are collected, and queries are made to the data available through the threat reports. Sensors are installed on client machines to collect logs and indicators, and these are sent to a centralized log management tool.

### 3.2 Data and Intelligence Enrichment

As intelligence reports are imported into the TIP tool, they are enriched with data extracted from other open-source intelligence feeds, which enhances the contextualization of events and improves the accuracy of potential detections. However, since the quality and authenticity of the data used during the enrichment process significantly affect the reliability of the resulting threat intelligence, it is important to enrich threat data with verified or high-quality feeds, such as VirusTotal [15], Hybrid Analysis [16], and AlienVault OTX [17]. The enrichment with low-quality feeds can lead to inaccurate correlations, generating false positives or false negatives. Such inaccuracies may result in ineffective incident response, wasting resources, and increasing the vulnerability of the system.

The raw data received in the centralized tool is processed and further enriched with additional information. This phase involves correlating the captured indicators with known TTPs, using the MITRE ATT&CK framework as a reference [18].

### 3.3 Correlation and Analysis

At this stage, enriched data is analyzed for malicious behavior patterns and TTPs that correspond to known threats. This analysis uses a threat intelligence-based approach to correlate security events with previously documented attacks. The process involves predefined rules that utilize pattern-matching techniques, specifically regular expressions (regex), to search for specific occurrences of actions within the collected logs. These actions are then mapped to corresponding TTPs, allowing for the identification of potential threats based on observed behaviors and facilitating the proactive detection of threats, by correlating observed indicators with known adversarial tactics.

Thus, TTPs that have been correlated with an indicator are compared against the information base of attacks and cyber threats obtained from security reports. If TTPs originating from an indicator are found among the previously listed TTPs in the reports, a second level of verification is performed, where the suspicious indicator is compared against a list of indicators related to the identified TTPs.

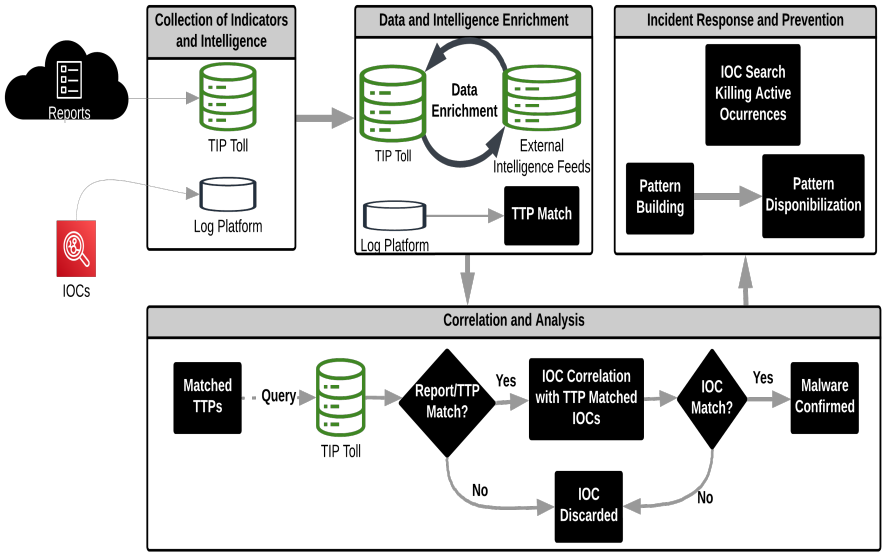


**Fig. 2.** Proposed Solution Flow

### 3.4 Incident Response and Prevention

The final phase involves response actions based on the correlations found. Detected incidents can be prioritized based on the threat level and criticality, enabling a more agile and efficient response. According to the TTPs and indicators found, blocking rules can be created in the centralized log management tool to prevent new occurrences, as well as to terminate ongoing cases in real time.

## 4 Case Study

The case study of the proposed methodology involved the integration of various open source cyber threat detection tools, which provided some of the functionalities needed. The solution is represented in Figure 2, and the main stages are described below:

### 4.1 Configuration of Threat Intelligence Platform

As a TIP tool for storing and managing cyber threat intelligence reports, the OpenCTI [19] platform was chosen. This open-source platform is designed to structure, store, and visualize both technical and non-technical information about cyber threats, enabling efficient management of cyber intelligence knowledge and observables. Approximately 1,500 reports were imported from the AlienVault OTX database.

As additional sources of information used to enriching the CTI reports (Figure 3), integration with VirusTotal and Hybrid Analysis was configured via connectors in OpenCTI. As the reports were added to the OpenCTI database, queries were made to the other two sources to gather relevant and correlated information. This information was then added to the OpenCTI reports, enriching the initial reports to improve detection accuracy and provide deeper context about the threats.

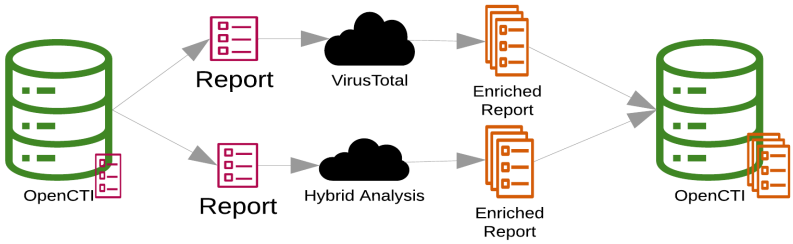


**Fig. 3.** Enrichment Process

### 4.2 Installation and Configuration of Log Platform

To provide a contextualized source of sensor information, the centralized log platform Wazuh, an open-source tool that combines SIEM (Security Information and Event Management) and XDR (Extended Detection and Response) functionalities [20] was used, performing monitoring, detection, and alert activities. Its main function is to collect, correlate, and analyze logs from endpoints, providing a consolidated, real-time view of network security. Wazuh sensors were installed on virtual machines configured with Windows 10 to capture events and logs from the endpoints. To enhance data collection, Sysmon was configured according to the recommendations in [21], enabling the collection of detailed system logs.

### 4.3 Collection and Analysis of Malware Samples

For acquiring malware samples, the Malware Bazaar repository, maintained by Abuse, was used. This repository is a source of malware samples that are shared with the information security community. The samples were used to test the effectiveness of the proposed methodology in identifying threats. The malware used to validate the methodology was Agent Tesla. The samples were executed on the virtual machines, and as security logs were generated, the sensors installed on the machines forwarded the corresponding information to Wazuh, which automatically interpreted them and provided the TTPs associated with the events that occurred during the malware execution.

### 4.4 Validation and Results

During the execution of a random sample of the malware, the logs generated on the client stations were sent through the sensors to the Log Platform tool. Automatically, Wazuh checked the received logs for the presence of known tactics, techniques, and procedures, and correlated the observed TTPs during the malware execution, generating the list $l_{TTPs}$. With the list $l_{TTPs}$ in hand, a search was conducted in the TIP report database, listing all reports that contained at least one of the previously mentioned TTPs, which generated the list $l_{Rep}$, containing approximately 640 reports. Once the creation of the list $l_{Rep}$ was completed, the reports in it were ranked based on the number of associated TTPs, producing the ranking $R_1$:

$$R_1 = f(L_{Rep}) \tag{1}$$

$$f(i) = |TTP_i \cap L_{TTPs}| \tag{2}$$

Here, the function f serves as a scoring mechanism that ranks the reports in $l_{Rep}$ according to how many TTPs from the observed list $l_{TTPs}$ they share. The more TTPs a report shares with the observed behavior, the higher its score. This allows for the identification and prioritization of reports that provide the most relevant information regarding the threat. In this way, the function f helps streamline the investigation process by focusing attention on the reports that have the highest likelihood of containing useful details about the observed threat.

It was expected that the reports present in $R_1$ would have direct references to the malware used. However, upon analyzing the top reports in $R_1$, that is, those that had the most TTPs associated with the malware execution, we found that none of them mentioned it. Formally, we defined $A_1$ as the set of reports that mention the malware, and we observed that this set was empty:

$$A_1 = \{r \in R_1 : r \text{ mentions } \mathit{Malware}\} = \emptyset \tag{3}$$

The second approach involved checking the Indicators of Compromise (IoCs) present in the reports from list $L_{Rep}$. An Indicator of Compromise (IoC) is defined as a piece of data or evidence that suggests a potential security breach within a system[22], and help security professionals identify suspicious activity and respond to possible threats by looking for patterns like malicious IP addresses, file hashes, domain names, or abnormal network behaviors. All the IoCs were searched in Wazuh during the malware execution period, but no correlations were found either. Formally, the correlation $C_1$ between the IoCs $I_1$ and the Wazuh logs was null:

$$C_1 = \{i \in I_1 : i \text{ corresponds to the Logs}\} = \emptyset \tag{4}$$

This lack of correlation raised questions about the timeliness and relevance of the analyzed reports.

Finally, a second validation was conducted with a different version of the malware, which we knew was referenced in one of the existing TIP reports. The

same steps were repeated, where the list of TTPs observed during the malware execution $l_{TTPs2}$ was first generated, then the reports referencing these TTPs were listed, generating the list $l_{Rep2}$, and the reports were ranked using $R_2$. This time, the report corresponding to the executed malware was found in the ranking $R_2$. Thus, we now define $A_2$ as the set of reports that mention the new malware version, and we observed that this set was no longer empty:

$$R_2 = f(L_{Rep2}) \tag{5}$$

$$A_2 = \{r \in R_2 : r \text{ mentions } \textit{Malware2}\} \neq \emptyset \tag{6}$$

Finally, the IoCs present in the reports from list $L_{Rep2}$ were checked, and as expected, the IoC of the executed malware version appeared in previous reports. Thus, the new correlation $C_2$ indicated a positive match:

$$C_2 = \{i \in I_2 : i \text{ corresponds to the Logs}\} \neq \emptyset \tag{7}$$

Once in possession of the IoCs that confirmed the presence of the malware in $C_2$, a CDB (Constant Database) list is populated with the respective IoCs in the 'Key:Value' format, indicating the malware in question. This list can be populated with various indicators, such as file hashes, IP addresses, domain names, among others.

$$\begin{aligned} &Key : Value \\ &i_1 : Malware \\ &i_2 : Malware \\ &\vdots \\ &i_n : Malware \end{aligned} \tag{8}$$

Where, for the execution of Malware2, the following list is created:

$$\begin{aligned} &Key : Value \\ &ab9cd59d789e6c7841b9d28689.....1606f184889cc7e6acadcc : AgentTesla \end{aligned} \tag{9}$$

At this point, any set of actions such as file creation or modification started to be monitored in the environment through the File and Integrity Monitoring (FIM) module, preventing future executions. The properties of the files were retrieved and compared against the CDB list produced, and, in conjunction with the Active Response module, the file corresponding to the malware used was deleted, completing all the cycle of the proposed methodology.

### 4.5 Discussion

In the first attempt to validate the methodology, where a random sample of the sample malware (*Agent Tesla*) was executed, it was possible to correlate

the detected TTPs with the available reports. However, it was not possible to attribute the sequence of TTPs to a specific malware. This was achieved in the second validation attempt of the methodology, where among the TTPs listed during the execution of the sample malware (*Agent Tesla*), the listed TTPs could be correlated with the available reports, as well as a second verification factor, in which the correlation of IoCs with the reports was also observed.

Thus, the proposed methodology is demonstrated to be effective in identifying TTPs and correlating them with reports, playing the role of a recommendation system as it suggests possible avenues of investigation where the sequence of TTPs used could potentially be attributed to a specific malware. The results observed in the second validation attempt indicate that, depending on the timeliness of detecting TTPs and correlating them with reports, the convergence of an investigation can be accelerated, leading to a faster attribution of the malicious entity. Therefore, the presented methodology has the potential to go beyond scalability in the process of detecting and identifying TTPs, possibly leading to attribution, and contributing to the detection and prevention of current or future incident ocurrences, as demonstrated during the last phase of the validation, where the active Agent Tesla instance was finished. However, this is contingent on the quality and specificity of the reports loaded into the TIP.

## 5 Conclusions

The integration of cyber intelligence sources within the context of Security Information and Event Management systems has proven to be an effective approach for improving the detection and prevention of advanced cyber threats. The research demonstrated that combining different sources, such as Cyber Threat Intelligence reports and Indicators of Compromise, provided substantial improvements in the ability to identify attack patterns and correlate malicious behaviors. However, this integration requires continuous effort to ensure the quality, relevance, and timeliness of the collected data to maximize its effectiveness.

The data enrichment process proved particularly effective in proactively detecting threats, especially by correlating TTPs with security events. The research showed that by adding additional layers of context to known TTPs, it was possible to significantly improve detection accuracy and speed up incident responses. However, this enrichment process still largely depends on manual interventions, suggesting that future research should focus on automating this step to increase the system's scalability and efficiency.

Additionally, the analysis of IoCs proved effective in detecting advanced malware such as Agent Tesla, but the volatility of these indicators, such as IP addresses and domains, may limit their long-term usefulness. The research indicated that to maximize the efficiency of tools like Wazuh, it is crucial that IoCs are updated in real-time to ensure their timeliness, and that security reports are created and made available promptly to the security community as quickly as possible.

## 6 Future Work

It is recommended to explore automated methods for integrating cyber intelligence sources with SIEM systems, focusing on automating data enrichment, validation, and correlation. Automating these tasks will help ensure that threat intelligence remains timely and accurate, as the quality and authenticity of data are crucial to effective threat detection. Unreliable information can hinder proactive defense measures, leading to inaccurate correlations, false positives, or false negatives. Developing a universal standardization framework for data sharing between TIP and SIEM platforms is also a promising avenue for future research.

Another area deserving attention is the use of machine learning algorithms to automate the data enrichment process, enabling artificial intelligence models to learn from large volumes of historical TTP data and provide real-time insights. Domain-specific LLMs can improve the identification of unknown threats by detecting emerging TTPs and extracting relevant IoCs from unstructured data, such as threat reports, enhancing both accuracy and contextualization in threat detection.

Finally, it is crucial to develop automated mechanisms for updating and correlating IoCs. NLP-driven tools can streamline IoC extraction from reports and forums, ensuring that the threat intelligence remains actionable. Tools that continuously monitor the validity of IoCs and automatically correlate them with system logs, like Wazuh, will enhance malware detection rates, especially when combined with behavioral analysis. Thus, future research could focus on implementing solutions that make these processes more agile, ensuring more effective and scalable threat detection while also addressing the challenge of attribution.

## References

1. Abu, M.S., Selamat, S.R., Ariffin, A., Yusof, R.: Cyber threat intelligence – issues and challenges. In: Indonesian Journal of Electrical Engineering and Computer Science, vol. 10, pp. 371–379 (2018). https://doi.org/10.11591/ijeecs.v10.i1.pp371-379
2. Aslan, Ö.A., Samet, R.: A Comprehensive Review on Malware Detection Approaches. In: IEEE Access, vol. 8, pp. 6249-6271 (2020). doi:10.1109/ACCESS.2019.2963724
3. Wu, J.: New approaches to cyber defense. In: Cyberspace Mimic Defense. Springer (2020), pp. 113–157. ISBN: 978-3-030-29844-9.
4. Imperva: Advanced persistent threat (APT). In: Advanced persistent threat (APT) (2024). Accessed on: August 21, 2024. https://www.imperva.com/learn/application-security/apt-advanced-persistent-threat/
5. Sagar, S.: Developing Proactive Cyber Threat Intelligence from the Online Hacker Community: A Computational Design Science Approach. In: The University of Arizona (2018). http://hdl.handle.net/10150/628454
6. Tounsi, W., Rais, H.: A survey on technical threat intelligence in the age of sophisticated cyber attacks. In: Computers & Security, Elsevier BV, vol. 72, pp. 212-233 (2018). https://doi.org/10.1016/j.cose.2017.09.001
7. Silva, A.D.M.: Metodologia integrativa para produção de inteligência de ameaças cibernéticas utilizando plataformas de código aberto. In: Dissertação (Mestrado

Profissional em Engenharia Elétrica) — Universidade de Brasília, Brasília (2020). https://repositorio.unb.br/handle/10482/40541
8. Sauerwein, C., Sillaber, C., Mussmann, A., Breu, R.: Threat intelligence sharing platforms: An exploratory study of software vendors and research perspectives. In: The 13th International Conference on Wirtschaftsinformatik, pp. 837–851 (2017). https://wi2017.ch/images/wi2017-0188.pdf
9. Ghafir, I., Kyriakopoulos, K.G., Lambotharan, S., Aparicio-Navarro, F.J., Assadhan, B., Binsalleeh, H., Diab, D.M.: Hidden Markov Models and Alert Correlations for the Prediction of Advanced Persistent Threats. In: IEEE Access, vol. 7, pp. 99508-99520 (2019). doi:10.1109/ACCESS.2019.2930200
10. Mahboubi, A., Luong, K., Aboutorab, H., Thanh Bui, H., Jarrad, G., Bahutair, M., Camtepe, S., Pogrebna, G., Ahmed, E., Barry, B., Gately, H.: Evolving techniques in cyber threat hunting: A systematic review. In: Journal of Network and Computer Applications, vol. 232, article no. 104004 (2024). https://doi.org/10.1016/j.jnca.2024.104004
11. Jin, B., Kim, E., Lee, H., Bertino, E., Kim, D., Kim, H.: Sharing cyber threat intelligence: Does it really help? In: NDSS (2024). doi:10.14722/ndss.2024.24228
12. Ainslie, S., Thompson, D., Maynard, S., Ahmad, A.: Cyber-threat intelligence for security decision-making: A review and research agenda for practice. In: Computers & Security, vol. 132, article no. 103352 (2023). https://doi.org/10.1016/j.cose.2023.103352
13. González-Granadillo, G., González-Zarzosa, S., Diaz, R.: Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. In: Sensors, vol. 21, article no. 4759 (2021). https://www.mdpi.com/1424-8220/21/14/4759
14. Leite, C., den Hartog, J., dos Santos, D.R., Constante, E.: Actionable Cyber Threat Intelligence for Automated Incident Response. In: Secure IT Systems: 27th Nordic Conference, NordSec 2022, Reykjavik, Iceland, November 30–December 2, 2022, Proceedings, pp. 368–385. Springer-Verlag, Berlin, Heidelberg (2023). https://doi.org/10.1007/978-3-031-22295-5_20
15. VirusTotal: Reports. In: VTDoc (2024). Accessed on: October 5, 2024. https://docs.virustotal.com/docs/results-reports
16. Hybrid Analysis: Public Knowledge Base. In: Free Automated Malware Analysis (2024). Accessed on: October 5, 2024. https://www.hybrid-analysis.com/knowledge-base
17. Level Blue: The World's First Truly Open Threat Intelligence Community. In: Level Blue - Open Threat Exchange (2024). Accessed on: October 5, 2024. https://otx.alienvault.com
18. MITRE ATT&CK: Matrix - Enterprise. In: Enterprise Matrix (2024). Accessed on: September 9, 2024. https://attack.mitre.org/matrices/enterprise/
19. Filigran: OpenCTI Documentation Space. OpenCTI Documentation (2024). Accessed on: August 24, 2024. https://docs.opencti.io/latest/
20. Wazuh: The Open Source Security Platform (2024). Accessed on: August 25, 2024. https://wazuh.com
21. Hartong, O.: A Sysmon configuration repository for everybody to customise. In: sysmon-modular (2023). Accessed on: September 1, 2024. https://github.com/olafhartong/sysmon-modular
22. Preuveneers, D., Joosen, W.: Sharing Machine Learning Models as Indicators of Compromise for Cyber Threat Intelligence. In: Journal of Cybersecurity and Privacy, vol. 1, no. 1, pp. 140–163 (2021). https://www.mdpi.com/2624-800X/1/1/8