International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

SOAR Automation: Palo Alto Cortex XSOAR Playbooks for MISP Threat Intel Enrichment and TheHive Project Integration

Sandhya Guduru

Masters in Information Systems Security, Software Engineer - Technical Lead

Abstract: ***This paper explores the integration of Palo Alto Cortex XSOAR playbooks with MISP (Malware Information Sharing Platform) for threat intelligence enrichment and TheHive Project for case management. The integration aims to automate and streamline security operations by enriching threat indicators and facilitating effective incident response. Additionally, the paper discusses the automation of Tanium-driven endpoint isolation and its mapping to the MITRE ATT&CK framework for better prioritization of threats. This integration allows security teams to improve their operational efficiency by leveraging automation and intelligence sharing, ultimately enhancing the detection, response, and remediation of security incidents in real-time. Through a detailed analysis, we explore how these automated playbooks can create a more efficient and coordinated response to cyber threats.***

Keywords: SOAR, Cortex XSOAR, MISP, TheHive, Tanium, endpoint isolation, MITRE ATT&CK, automation, threat intelligence enrichment, security operations

1. Introduction

Integrating Security Orchestration, Automation, and Response (SOAR) platforms, such as Palo Alto's Cortex XSOAR, into existing security workflows transforms how organizations detect, respond to, and mitigate cyber threats. Security operations teams often face an overwhelming volume of alerts, requiring manual investigation and response. This leads to delays, errors, and a slower overall response time. By integrating automated tools, such as MISP (Malware Information Sharing Platform) for threat intelligence enrichment and TheHive Project for case management, these tasks can be streamlined, improving both efficiency and effectiveness in handling security incidents [1].

The MISP platform is widely used for sharing and correlating threat intelligence. It provides a repository of enriched indicators that security teams can use to better understand the scope and impact of a potential threat. When automated in the Cortex XSOAR playbooks, these indicators offer real-time updates on threat activity, making it easier for security teams to respond quickly to evolving threats.

TheHive Project, a scalable and open-source incident response platform, is designed to improve case management and investigation workflows. By integrating TheHive with Cortex XSOAR, organizations can automate the creation and management of incident cases, providing better collaboration across teams and improving the overall incident response process
Furthermore, Tanium, an endpoint management tool, can be integrated into the playbooks to isolate endpoints and prevent lateral movement during an active security incident. Automating Tanium-driven endpoint isolation ensures rapid containment of threats, reducing potential damage from a security breach [2].

Incorporating MITRE ATT&CK, a knowledge base of adversary tactics, techniques, and procedures, helps security teams prioritize threats based on their potential impact and likelihood of occurrence. By mapping STIX/TAXII feeds to MITRE ATT&CK, Cortex XSOAR playbooks can identify which tactics or techniques are being exploited and prioritize response efforts accordingly [3].

2. Literature Review

The landscape of cybersecurity has evolved significantly in recent years, necessitating more efficient and automated solutions for incident response and threat management. Security Orchestration, Automation, and Response (SOAR) platforms, such as Palo Alto Cortex XSOAR, have become essential for automating security processes and improving response times. SOAR platforms integrate disparate security tools, coordinate response activities, and automate manual tasks. By integrating playbooks into these platforms, organizations can standardize and streamline their incident response procedures, reducing human error and improving operational efficiency. A 2021 report by ISACA highlighted that SOAR solutions enable organizations to automate, orchestrate, and respond to cybersecurity incidents with minimal human intervention, making threat detection and resolution more effective and agile [4].

A core component of modern security operations is the Malware Information Sharing Platform (MISP), which facilitates the sharing and correlation of threat intelligence among different organizations and security platforms. MISP enables the collection of structured threat information, which can be shared in real-time across various stakeholders This collaboration enhances the collective understanding of cyber threats, allowing organizations to improve their threat detection and response capabilities. By automating the enrichment of threat indicators with MISP, security teams can receive up-to-date, relevant information on the latest threats and vulnerabilities

In incident response management, TheHive Project has emerged as a powerful open-source platform. It is designed to assist security teams in managing and investigating security

incidents by providing a centralized platform for case management. TheHive integrates with a wide range of security tools and allows security teams to automate workflows, assign tasks, and track case progress. This integration enables a more collaborative and efficient response to incidents, ensuring that critical tasks are prioritized and addressed promptly [5].

Endpoint management is another crucial aspect of modern cybersecurity practices. Tanium is a widely used tool for endpoint visibility and management, allowing organizations to monitor and control endpoints across their network. By integrating Tanium with SOAR platforms like Cortex XSOAR, organizations can automate actions such as endpoint isolation during an active threat, ensuring quick containment and preventing further compromise. Tanium's ability to provide real-time endpoint data helps security teams make informed decisions and respond rapidly to threats [6].

The MITRE ATT&CK framework is an invaluable resource for cybersecurity professionals, offering a comprehensive knowledge base of adversary tactics, techniques, and procedures (TTPs). It is widely used to map attack techniques and understand the behaviors of cyber adversaries. Integrating MITRE ATT&CK with SOAR platforms allows security teams to prioritize and respond to attacks based on the tactics and techniques being exploited. By mapping incoming threat data from tools like MISP to MITRE ATT&CK, organizations can assess the severity of threats and focus their efforts on addressing the most critical risks first. This integration improves the efficiency of threat response and enhances overall cybersecurity posture

Lastly, STIX (Structured Threat Information Expression) and TAXII (Trusted Automated Exchange of Indicator Information) are key standards for sharing threat intelligence. These frameworks enable the structured exchange of threat data between organizations and security platforms. STIX defines how to represent threat intelligence, while TAXII provides a secure method for sharing this information. Integrating STIX/TAXII with SOAR platforms like Cortex XSOAR allows automated threat intelligence enrichment, improving the effectiveness of incident response efforts and helping organizations stay ahead of evolving threats [7].

3. Problem Statement

Modern security operations face growing challenges due to the increasing complexity and volume of cyber threats. Organisations often rely on a patchwork of disconnected tools and manual processes that are too slow and inefficient to respond to real-time incidents effectively. The following table outlines the key problems that hinder timely and coordinated incident response, highlighting the need for an integrated, automated approach.

Challenge	Explanation
High Volume of Security Alerts	Security teams face alert fatigue due to a constant influx of alerts, leading to slower incident response times.
Lack of Tool Integration	Threat detection, case management, and endpoint control systems operate in silos, making coordinated response difficult.
Manual Workflows	Absence of automated enrichment and remediation processes results in delayed and error-prone responses.
Disjointed Threat Intelligence Use	Tools like MISP and TheHive are often not connected, reducing the usefulness of shared threat data.
Limited Framework Integration	Security frameworks (e.g., MITRE ATT&CK, STIX/TAXII) are not fully embedded into workflows, hindering prioritisation of threats.

As cyber threats continue to evolve in sophistication and scale, security operations teams are increasingly overwhelmed by the sheer volume of security alerts and incidents. This flood of alerts, often coming from diverse sources and requiring manual intervention, leads to inefficiencies and delays in response times, leaving organizations vulnerable to attacks. Traditional, reactive approaches to threat detection and incident response are no longer sufficient to handle modern threats, which demand faster, more coordinated, and automated responses.

A major challenge is the lack of integration across the various tools and platforms used for threat detection, case management, and endpoint control. Many organizations still struggle to centralize and automate their security workflows, relying on fragmented systems that do not communicate effectively with each other. This makes it difficult for security teams to track incidents, enrich threat data in real time, or take appropriate actions quickly [8].

In particular, the absence of seamless automation between threat intelligence platforms like MISP and incident response systems like TheHive, compounded by the lack of integrated endpoint management (e.g., Tanium), exacerbates the problem. Without automated playbooks to enrich threat intelligence, isolate compromised endpoints, and prioritize response efforts, security teams are left with manual processes prone to errors and delays, hindering their ability to respond effectively to critical incidents [9].

Moreover, while MITRE ATT&CK and STIX/TAXII provide valuable frameworks for understanding and sharing threat intelligence, their integration into real-time workflows remains a challenge. Security operations teams need to be able to map incoming data against these frameworks automatically to prioritize threats based on their severity and relevance, allowing them to take timely and informed action. The lack of automation and integration across these areas further impedes the efficiency of incident response and overall security posture [10].

Thus, there is a critical need for an automated solution that integrates these various security tools, enabling organizations to efficiently process threat intelligence, manage incidents, isolate endpoints, and prioritize responses based on the most relevant and severe threats. This paper aims to explore how the integration of Palo Alto Cortex XSOAR playbooks with MISP, TheHive, Tanium, and MITRE ATT&CK can address these challenges and improve the overall security response.

Proposed Solution

To address these limitations, this paper proposes a unified solution that leverages Palo Alto Cortex XSOAR playbooks to integrate key security tools. By automating threat enrichment, case management, endpoint isolation, and threat prioritisation, the framework improves the speed, consistency, and accuracy of incident response. The table below summarises the core components of this solution and their respective contributions to a streamlined and effective security workflow.

Solution Component	Functionality
MISP Integration	Automates threat intelligence enrichment by retrieving context on indicators like IPs, hashes, and domains.
TheHive Integration	Enables automatic case creation, assignment, and tracking of incidents in a centralised system.
Tanium Integration	Allows for real-time endpoint isolation, reducing the risk of threat propagation.
MITRE ATT&CK Mapping	Automates mapping of threat indicators to adversary techniques for prioritised response.
Cortex XSOAR Playbooks	Unifies all components into a standardised, automated incident response workflow.

Automation of Threat Intelligence Enrichment with MISP

The integration of MISP with Cortex XSOAR allows for automated enrichment of threat indicators. As new threat data is ingested into the system, Cortex XSOAR can trigger playbooks that automatically retrieve relevant enrichment data from MISP, such as additional context about IP addresses, URLs, or file hashes. This enriched data enables security teams to better understand the nature of the threat and its potential impact. Automating this process reduces the time required to gather intelligence, helping teams make more informed decisions quickly [11].

Streamlining Case Management with TheHive

Integrating TheHive Project into the playbooks enables the automated creation and management of incident cases. When a potential threat is detected, Cortex XSOAR can automatically create a case in TheHive, assigning it to the appropriate team members for investigation. This integration not only saves time but also ensures that cases are tracked systematically, with all relevant information and actions recorded in one centralized location. Furthermore, automation can prioritize incidents based on their severity, ensuring that the most critical threats are handled first [12].

Automated Endpoint Isolation with Tanium

To mitigate the risks posed by compromised endpoints, the solution incorporates Tanium for endpoint isolation. Tanium's real-time endpoint visibility allows for immediate action when a threat is detected. By automating Tanium's response within Cortex XSOAR playbooks, security teams can isolate affected endpoints swiftly, preventing further spread of the attack. This automation is crucial in reducing the time to containment, which is critical in minimizing the damage caused by cyber incidents [9].

Leveraging MITRE ATT&CK for Threat Prioritization

The MITRE ATT&CK framework provides a structured approach to understanding adversary tactics, techniques, and procedures. Integrating MITRE ATT&CK with Cortex XSOAR enables automated mapping of threat indicators to the relevant tactics and techniques, helping security teams prioritize responses. This prioritization allows for a more efficient allocation of resources, ensuring that the most relevant threats are addressed first. By automating this mapping, organizations can avoid the manual work involved in mapping indicators to MITRE ATT&CK, improving the overall efficiency of their security operations.

Standardizing and Automating Incident Response

The integration of all these tools into a cohesive SOAR workflow standardizes and automates the incident response process. By leveraging predefined playbooks, security teams can ensure that all necessary steps are taken in response to a security event, from enrichment to endpoint isolation, case management, and threat prioritization. This reduces the risk of human error and accelerates response times, allowing organizations to address threats faster and more effectively.

4. Conclusion

The integration of Palo Alto Cortex XSOAR with key security tools like MISP, TheHive, Tanium, and MITRE ATT&CK offers a comprehensive solution to the challenges faced by modern cybersecurity teams. By automating threat intelligence enrichment, incident management, endpoint isolation, and threat prioritization, organizations can significantly improve their response times and operational efficiency. This automation not only reduces the risk of human error but also enables a more proactive approach to cybersecurity, allowing security teams to address emerging threats swiftly and with greater accuracy.

The combination of SOAR platforms, threat intelligence frameworks, and endpoint management solutions creates a robust ecosystem for security operations. By adopting an integrated, automated approach, organizations can streamline their workflows, reduce the complexity of managing multiple security tools, and ultimately enhance their overall security posture. As the landscape of cybersecurity continues to evolve, such integrations will become increasingly essential

for organizations striving to stay ahead of sophisticated cyber threats.

In conclusion, this paper demonstrates the potential of Palo Alto Cortex XSOAR to transform incident response workflows by integrating critical security tools and automating key processes. With further advancements in automation and artificial intelligence, this approach will continue to evolve, offering even greater capabilities for managing cybersecurity threats in real time.

References

[1] C. Badeau, "Leveraging MISP and TheHive When You Create Your CTI Practice," *ThreatQuotient*, Sep. 07, 2021. Available: https://www.threatq.com/leveraging-misp-hive-create-cti-practice/

[2] "Tanium v2 | Cortex XSOAR," *Pan.dev*, 2019. Available: https://xsoar.pan.dev/docs/reference/integrations/tanium-v2?

[3] *Paloaltonetworks.com*. Available: https://www.paloaltonetworks.com/blog/security-operations/mitre-attck-for-cortex-xsoar/.

[4] "2021 Volume 2 Benefits of Using a SOAR Solution," *ISACA*, 2021. Available: https://www.isaca.org/resources/isaca-journal/issues/2021/volume-2/benefits-of-using-a-soar-solution?

[5] "Malware Information Sharing Platform (MISP)," *FIRST — Forum of Incident Response and Security Teams*, 2015. Available: https://www.first.org/global/sigs/information-sharing/misp?

[6] A. Mars and W. Adi, "New Concept for Physically-Secured E-Coins Circulations," vol. 2013, pp. 333–338, Aug. 2018, doi: https://doi.org/10.1109/ahs.2018.8541493. Available: https://ieeexplore.ieee.org/document/8541493.

[7] "Tanium for Automation ," 2021. Available: https://site.tanium.com/rs/790-QFJ-925/images/SB-Tanium-for-Automation-2021.pdf?

[8] "TAXII Feed | Cortex XSOAR," *Pan.dev*, 2021. Available: https://xsoar.pan.dev/docs/reference/integrations/taxii-feed?utm_source=chatgpt.com.

[9] M. Zhou, L. Han, H. Lu, C. Fu, and D. An, "Cooperative malicious network behavior recognition algorithm in E-commerce," *Computers & Security*, vol. 95, p. 101868, Aug. 2020, doi: https://doi.org/10.1016/j.cose.2020.101868

[10] Anand Groenewegen and J. S. Janssen, "TheHive Project: The maturity of an open-source Security Incident Response platform," Jun. 24, 2021. Available: https://www.researchgate.net/publication/352715439_TheHive_Project_The_maturity_of_an_open-source_Security_Incident_Response_platform

[11] V. Mavroeidis and S. Bromander, "Cyber Threat Intelligence Model: An Evaluation of Taxonomies, Sharing Standards, and Ontologies within Cyber Threat Intelligence," *IEEE Xplore*, Sep. 01, 2017. doi: https://doi.org/10.1109/EISIC.2017.20. Available: https://ieeexplore.ieee.org/document/8240774/.

[12] M. Gschwandtner, L. Demetz, M. Gander, and R. Maier, "Integrating Threat Intelligence to Enhance an Organization's Information Security Management," *Proceedings of the 13th International Conference on Availability, Reliability and Security*, Aug. 2018, doi: https://doi.org/10.1145/3230833.3232797