Automating Security with Wazuh to SOAR Implementation

Dr.R.Umamaheswari [1] , Ajay.L [2],M.S.Sabari [3]

[1], *Professor &Head of The Department, Department of CSE, Gnanamani College of Technology, Namakkal,Tamilnadu, India*[2], *UG Students, Department of CSE, Namakkal, Tamilnadu, India.*

[3], *Assistant Professor, Department of CSE, Gnanamani College of Technology, Namakkal,Tamilnadu, India*

ABSTRACT- Cybersecurity is a critical concern in the contemporary digital landscape, demanding efficient and effective solutions for threat detection, incident response, and remediation. The implementation of automated security practices through the integration of Wazuh and Security Orchestration, Automation, and Response (SOAR) technologies addresses this pressing need. In an increasingly complex and dynamic cybersecurity environment, organizations require streamlined approaches for threat detection, incident response, and remediation. By leveraging the capabilities of Wazuh, a robust open-source security monitoring platform, and integrating it with SOAR frameworks, this project aims to optimize security operations, enhance threat visibility, and expedite incident response times. The abstract outlines the objectives, methodology, key findings, and implications of the integration, shedding light on its potential to fortify cybersecurity posture and resilience in the contemporary digital environment

Index Terms- Wazuh, Automation, Threat detection, Open-source security monitoring, Securitty incident management, security automation , SOAR

I.INTRODUCTION

In the contemporary digital landscape, safeguarding against cyber threats has become paramount for organizations spanning various industries. As cyber adversaries deploy increasingly sophisticated tactics, organizations face the challenge of fortifying their defenses with adaptive security solutions. The amalgamation of Wazuh and Security Orchestration, Automation, and Response (SOAR) technologies emerges as a pivotal stride in fortifying cybersecurity posture. This integration furnishes a holistic approach towards threat detection, incident response, and resolution, catering to the dynamic threat landscape. Within the realm of cybersecurity, the integration of Security Orchestration, Automation, and Response (SOAR) platforms stands as a cornerstone, revolutionizing security operations with its ability to amalgamate disparate tools, streamline workflows, and automate mundane tasks. Embarking on the endeavor titled "Automating Security with Wazuh to SOAR Implementation," this project intricately merges two formidable

Cybersecurity arsenals: Wazuh and TheHive. Wazuh, a robust open-source security monitoring platform, distinguishes itself through its prowess in real-time threat detection, incident response, and compliance management. In contrast, TheHive emerges as a dynamic and scalable security incident response platform, fostering collaborative analysis and automating responses to security incidents. By fusing Wazuh and TheHive, the project endeavors to streamline security operations, automate incident response workflows, and augment overall cybersecurity efficacy. This integration harnesses the collective prowess of both platforms, leveraging Wazuh's robust threat detection capabilities alongside Now. Automatic generation of threat intelligence can also be proved beneficial to security teams. While there are progress going on taking these things into consideration now as well. The Hive's sophisticated incident management features. The integration journey entails seamless exchange of security alerts and incident data between Wazuh and TheHive, fostering efficient triage, analysis, and response to security incidents. Configurable automated playbooks and workflows within TheHive orchestrate incident response actions based on predefined criteria and response protocols. Moreover, the integration amplifies threat visibility and situational awareness by consolidating security data and furnishing comprehensive dashboards and reports for monitoring and analysis. This empowers security teams to discern and counteract security threats expeditiously, thereby curtailing response times and mitigating the repercussions of cyber onslaughts.

II.LITERATURE SURVEY

[11] As part of modern digital development, incident management in companies requires an automated approach that will reduce the time staff is involved in routine information security incident processing.

[10] Thus, automating such things can help security teams to deal with more important matters which really need their attention. Automating tasks which are repetitive in nature, filtering, classification, etc. can be done using the

various new technologies and by utilizing better computation power we have out large amount of necessary activities which traditional firewalls can't do. Smart threat detection, Malware behaviour analyses and pattern recognition, etc.

[4] A predefined template was used within TheHive. TheHive supports the ability to create specific templates matching specific types of incoming alerts, such as spear phishing. A template will assist the responsible party in predefined attributes such as title prefixes, severity, TLP, tags, description and required tasks or custom fields. Instead of having to create a case manually, the analyst is capable of configuring a workflow that is required to be followed when a specific scenario has occurred.

[10]SOAR stands for Security Orchestration, Automation, and Response. The main focus of this technology is to automate various security processes like network security audit, privileged password management and coordination and execution of tools between various tools and security groups. It does this by using various playbooks that has required steps need to be performed developed by experts themselves.

[8]Open-source SIEM software is becoming very popular, and thus used by many public and private institutions. Its cost is the main factor that small to medium-sized organizations should consider in opting for open-source solutions. An open-source solution allows them to explore and assess various capabilities before pursuing proprietary solutions.

PROBLEM STATEMENT

Cybersecurity system security incident management relies on disparate cybersecurity tools and manual processes. Organizations deploy various monitoring tools to detect security events, which generate alerts stored in separate systems. Security analysts then manually triage and respond to these alerts, facing challenges in correlating data and executing response actions efficiently. Limited collaboration among security teams further complicates incident response efforts. As the volume and complexity of security incidents increase, scalability and efficiency become significant challenges. The lack of integration, automation, and centralized collaboration underscores the need for a more streamlined and automated approach to security incident management. Integrating Wazuh and TheHive aims to address these shortcomings by providing a centralized platform for automated incident response, enhanced collaboration, and improved scalability, ultimately bolstering the organization's cybersecurity posture

ALGORITHM

Event Correlation Algorithms: Wazuh employs event correlation algorithms to analyze security events and identify potential threats or anomalies. These algorithms analyze multiple data sources, including logs, network traffic, and endpoint activity, to correlate events and detect suspicious patterns indicative of security incidents. Normalization Algorithms: Wazuh normalizes security event data from different sources into a standardized format suitable for analysis and processing. Normalization algorithms ensure consistency and uniformity in the representation of security events, regardless of the source or format in which they are generated. Data Enrichment Techniques: Wazuh enriches security event data with additional contextual information to enhance its relevance and usefulness for incident response. This may include enriching security alerts with threat intelligence feeds, asset information, historical data, and other relevant metadata to provide analysts with comprehensive insights into security incidents. Alert Routing and Prioritization: Wazuh employs routing and prioritization algorithms to determine the appropriate destination for security alerts within TheHive. These algorithms consider factors such as alert severity, type of security incident, organizational policies, and analyst assignments to route alerts to the most relevant teams or individuals for further investigation and response. Automated Response Playbooks: Wazuh integrates with TheHive to enable automated incident response actions based on predefined playbooks or workflows. These playbooks leverage decision-making logic and response actions to automate incident handling processes, such as containment, remediation, and notification, based on the analysis of security alerts and contextual information.

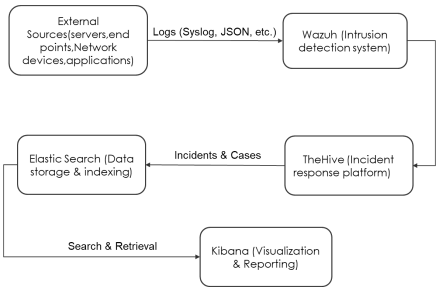
Block diagram

This process automates security incident response by leveraging Wazuh for central log collection and analysis. Wazuh stores the enriched data in ElasticSearch, enabling efficient search and retrieval using Kibana. Security alerts can also be forwarded to theHive, an incident response platform, for investigation, collaboration, and streamlined resolution of security incidents.

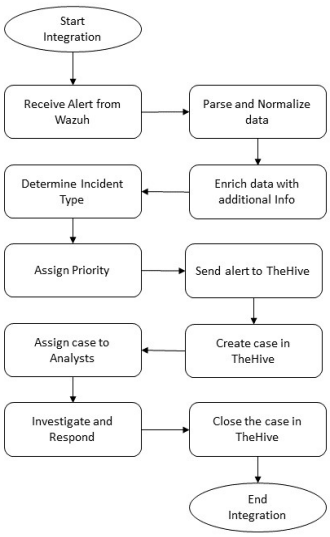
A. Working

Wazuh agents deployed across your network infrastructure continuously collect security events and logs from various sources like servers, endpoints, and network devices. These agents act as the eyes and ears of your security posture, forwarding the collected data to the central Wazuh manager. The Wazuh manager then transforms from a simple repository into an active security analyst.

It parses and analyzes the collected logs using predefined security rules, functioning like filters that identify potential threats or suspicious activities. These rules might search for excessive login attempts, unauthorized file access, or known malware signatures within the logs.



When a security event triggers a rule or exceeds a specific severity level, Wazuh doesn't just raise a basic notification; it generates a rich security alert. This alert is packed with context extracted from the logs, including details like the source of the event, the affected system, timestamps, and relevant log snippets. Wazuh doesn't operate in isolation however. It leverages Elastic Search, a powerful search and analytics engine, for data storage and indexing. The enriched security alerts and processed security data are meticulously stored within Elastic Search. This meticulous organization allows security analysts to easily search and retrieve specific security events using Kibana, a visualization and reporting tool. Kibana transforms the raw data into insightful formats like charts, graphs, and timelines, empowering analysts to identify trends and patterns within the security landscape. The integration with theHive takes security incident response a step further. Wazuh can be configured to not only store alerts but also forward them to theHive. Functioning as a dedicated incident response platform, theHive transforms a Wazuh security alert into a full-fledged security incident case within its interface. This case includes all the relevant details from the Wazuh alert, providing a springboard for security analysts to launch their investigation. The Hive empowers these analysts with the tools they need to delve deeper. They can add notes, collaborate with team members, assign tasks, and track the progress of the investigation all within the confines of the Hive case. Additionally, the Hive's ability to integrate with other security tools allows analysts to take decisive actions to resolve the incident, such as isolating compromised systems or deploying patches. In essence, this integrated approach automates several critical tasks in security incident response. Wazuh automates log collection, analysis, and alert generation, freeing up valuable analyst time for more strategic tasks. Additionally, the Hive streamlines the investigation and collaboration process, facilitating a faster and more effective response to security incidents.



CONCLUSION

In conclusion, the integration of Wazuh and TheHive presents a significant advancement in cybersecurity incident response capabilities. By seamlessly combining the capabilities of these two powerful platforms, organizations can streamline their security operations, enhance collaboration among security teams, and improve their overall cybersecurity posture. The integration facilitates automated incident response workflows, reduces manual intervention, accelerates response times, and provides comprehensive visibility into security incidents. Through centralized dashboards, enriched data, and automated response playbooks, security teams can effectively detect, investigate, and remediate security threats, ultimately bolstering the organization's resilience against cyber attacks. Furthermore, the integration lays the foundation for proactive threat mitigation, continuous improvement, and adaptation to evolving cyber threats, ensuring that organizations can effectively defend against the ever-changing threat landscape.

REFERENCES

[1] Anish Sridharan, V Kanchana, (2022), "SIEM integration with SOAR " . IEEE 2022 International Conference on Futuristic Technologies (INCOFT).

[2] Anne Connell, Tim Palko, and Hasan Yasar, (2013) ,"Cerebro: A platform for collaborative incident response and investiga tion". IEEE international conference on technologies for homeland security (HST). IEEE. pp. 241–245

[3] Abdelmajid Lakbabi ,Moukafih Nabil, Sabir Soukainat, Orhanou Ghizlane. (2017),"SIEM selection criteria for an efficient contextual security", IEEE 2017 International Symposium on Networks, Computers and Communications (ISNCC).

[4] Anand groenewegen , Joris janssen , (2021), TheHive Project: The maturity of an open-source Security Incident Response platform

[5] Bhatt S., Manadhata P.K., Zomlot L. (2014),"The operational role of security information and event management systems" ,IEEE Secur. Priv. pp. 35-41

[6] Chadni islam, M Ali Babar, Surya Nepal. (2024), Design and Generation of a Set of Declarative APIs for Security Orchestration , IEEE Transactions on Services Computing ,Volume: 17, pp . 127 – 141.

[7] C.Nagarajan and M.Madheswaran - 'Experimental verification and stability state space analysis of CLL-T Series Parallel Resonant Converter' - Journal of ELECTRICAL ENGINEERING, Vol.63 (6), pp.365-372, Dec.2012.

[8] C.Nagarajan and M.Madheswaran - 'Performance Analysis of LCL-T Resonant Converter with Fuzzy/PID Using State Space Analysis'- Springer, Electrical Engineering, Vol.93 (3), pp.167-178, September 2011.

[9] C.Nagarajan and M.Madheswaran - 'Stability Analysis of Series Parallel Resonant Converter with Fuzzy Logic Controller Using State Space Techniques'- Taylor & Francis, Electric Power Components and Systems, Vol.39 (8), pp.780-793, May 2011.

[10] C.Nagarajan and M.Madheswaran - 'Experimental Study and steady state stability analysis of CLL-T Series Parallel Resonant Converter with Fuzzy controller using State Space Analysis'- Iranian Journal of Electrical & Electronic Engineering, Vol.8 (3), pp.259-267, September 2012.

[11] Nagarajan C., Neelakrishnan G., Akila P., Fathima U., Sneha S. "Performance Analysis and Implementation of 89C51 Controller Based Solar Tracking System with Boost Converter" Journal of VLSI Design Tools & Technology. 2022; 12(2): 34–41p.

[12] C. Nagarajan, G.Neelakrishnan, R. Janani, S.Maithili, G. Ramya "Investigation on Fault Analysis for Power Transformers Using Adaptive Differential Relay" Asian Journal of Electrical Science, Vol.11 No.1, pp: 1-8, 2022.

[13] G.Neelakrishnan, K.Anandhakumar, A.Prathap, S.Prakash "Performance Estimation of cascaded h-bridge MLI for HEV using SVPWM" Suraj Punj Journal for Multidisciplinary Research, 2021, Volume 11, Issue 4, pp:750-756

[14] G.Neelakrishnan, S.N.Pruthika, P.T.Shalini, S.Soniya, "Perfromance Investigation of T-Source Inverter fed with Solar Cell" Suraj Punj Journal for Multidisciplinary Research, 2021, Volume 11, Issue 4, pp:744-749

[15] C.Nagarajan and M.Madheswaran, "Analysis and Simulation of LCL Series Resonant Full Bridge Converter Using PWM Technique with Load Independent Operation" has been presented in ICTES'08, a IEEE / IET International Conference organized by M.G.R.University, Chennai.Vol.no.1, pp.190-195, Dec.2007

[16] M Suganthi, N Ramesh, "Treatment of water using natural zeolite as membrane filter", Journal of Environmental Protection and Ecology, Volume 23, Issue 2, pp: 520-530,2022

[17] M Suganthi, N Ramesh, CT Sivakumar, K Vidhya, "Physiochemical Analysis of Ground Water used for Domestic needs in the Area of Perundurai in Erode District", International Research Journal of Multidisciplinary Technovation, pp: 630-635, 2019

[18] Jani, Purujoki, (2020),"SOAR Playbook Implementation - Incident Deduplication and Its Effects" , Bachelor's Thesis.

[19] Muhammad Sheeraz , Muhammad Arsalan Paracha , Mansoor Ul Haque , Muhammad Hanif Durad , Syed Muhammad Mohsin, Shahab S. Band, Amir Mosavi, (2023), "Effective Security Monitoring Using Efficient SIEM Architecture" , Human-centric Computing and Information Sciences .

[20] Panagiotis Radoglou-Grammatikisa, Panagiotis Sarigiannidisa and Eider Iturbeb. (2021), SPEAR SIEM: A Security Information and Event Management system for the Smart Grid

[21] Rahul vast ,Shruthi Sawant, Aishwarya Thorbole, Vishal Badgujar,(2021), Artificial Intelligence based Security Orchestration, Automation and Response System, IEEE 2021 6th International Conference for Convergence in Technology (I2CT).

[22] Ruslan Gibadullin,V.V. Nikonorov ,(2021). Development of the System for Automated Incident Management Based on Open-Source Software , IEEE 2021 International Russian Automation Conference (RusAutoCon).

[23] Zarzosa S.G. (2017), D2.1 in-depth analysis of SIEMs extensibility ,DiSIEM Project .