WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

CYBER WATCH-AN OPEN SOURCE SIEM TOOLS

SANJAY E

MSC INFORMATION SECURITY AND CYBER FORENSICS RATHINAM COLLEGE OF ARTS AND SCIENCE, INDIA
sanjaye20112001@gmail.com

ABSTRACT :

Security Information and Event Management (SIEM) systems have seen widespread deployment as a robust tool for preventing, detecting, and responding to cyber- attacks. The evolution of SIEM solutions has resulted in comprehensive systems that offer extensive visibility, allowing for the identification of high-risk areas. Proactive mitigation strategies are then employed to reduce costs and expedite incident response times.

At present, there is a gradual convergence of SIEM systems and associated solutions with big data analytics tools. Our analysis encompasses an overview of the most commonly used SIEMs, focusing on their critical functionalities. Additionally, we conduct an examination of external factors influencing the SIEM landscape in both the medium and long term. Within the scope of reviewing existing solutions, we present a compilation of potential enhancements for the next generation of SIEMs. This includes an assessment of their benefits and applicability in critical infrastructures

Keywords: SIEM, EDR, LOGANALYSIS, FLEXIBLE, THREAT, DETECT, MONITORING, ALERTING

Introduction :

Cybersecurity solutions in industrial control systems must offer real-time behavioral anomaly detection, facilitate swift incident management, and support intelligent visualization of the network and its interconnected nodes. Security Information and Event Management (SIEM) systems are designed to encompass these capabilities as integral features.

In essence, SIEMs possess the capability to collect, aggregate, store, and correlate events originating from a managed infrastructure. They serve as the central hub in modern security operations centers, gathering events from various sensors such as intrusion detection systems, antivirus software, firewalls, etc. These systems correlate the events and provide synthesized views of alerts for threat handling and security reporting. While these core capacities are shared, variations exist among different systems, reflecting their diverse positions in the market.

Traditionally, SIEM solutions have been associated with proprietary software characterized by high costs, vendor
lock-in, and limited flexibility. However, the landscape is evolving rapidly, witnessing the emergence of an ecosystem of open-source SIEM tools as compelling alternatives. These open-source solutions democratize access to potent security capabilities, providing organizations of all sizes with the opportunity to enhance their defenses without incurring exorbitant costs.

Cost-Effectiveness:

Open-source SIEM tools offer a budget-friendly solution, eliminating licensing fees and allowing organizations to allocate resources more efficiently without compromising security.

Community Collaboration:

The collaborative nature of open source promotes community-driven development and continuous improvement, enhancing features, security capabilities, and overall effectiveness of SIEM tools.

Customization and Flexibility:

Open-source SIEM tools provide unparalleled flexibility, enabling organizations to tailor solutions to their specific needs. This adaptability allows seamless integration with existing security infrastructure and customization based on unique security requirements.

This introduction establishes the groundwork for an exploration into the domain of open-source SIEM tools, examining their significance, features, and

benefits for contemporary cybersecurity initiatives. By comprehending the principles and advantages of open- source SIEM, organizations can leverage community- driven innovation to fortify their resilience against cyber threats. In an era marked by persistent cyber threats, organizations across industries face the imperative of safeguarding their digital assets and maintaining the trust of stakeholders. Security breaches, data thefts, and malicious intrusions pose formidable challenges, emphasizing the critical need for robust cybersecurity measures. At the forefront of this defense is the concept of Security Information and Event Management (SIEM), a foundational technology empowering organization to monitor, detect, and respond to security incidents in real- time.

2 Existing system :

The existing system for our open-source SIEM (Security Information and Event Management) tool project

encompasses a diverse landscape of cybersecurity solutions that organizations currently deploy to safeguard their digital environments. In many cases, proprietary SIEM tools dominate the market, offering robust capabilities for collecting, analyzing, and responding to security events. However, these solutions often come with significant licensing costs, limiting accessibility for smaller organizations with budget constraints. Additionally, some organizations rely on a patchwork of individual security tools, such as intrusion detection systems, log management systems, and endpoint protection solutions, which may lack seamless integration and centralized management.

The challenges within the existing system also include a lack of transparency and adaptability. Many proprietary solutions operate as black-box systems, making it difficult for organizations to scrutinize the underlying algorithms and mechanisms for potential vulnerabilities. Moreover, the one-size-fits-all nature of these tools may not adequately address the unique requirements of different organizations, hindering customization to specific IT infrastructures, industry regulations, or compliance standards.

Our open-source SIEM tool project aims to disrupt this existing paradigm by offering a transparent, customizable, and cost-effective alternative. By building on the strengths of open-source principles, we intend to create a platform that not only competes with proprietary solutions in terms of functionality but also addresses the limitations of the current landscape, providing organizations with a dynamic and adaptable SIEM solution that empowers them to enhance their cybersecurity posture effectively

SIEM Architecture :

1.Components of SIEM products: A typical SIEM architecture includes the following basic component

Data aggregation: Collects and aggregates data from security systems and network devices.
Threat intelligence feeds: Combines internal data with third-party data on threats and vulnerabilities.

Correlation and security monitoring: Links events and related data into security incidents, threats, or forensic findings
.
Analytics: uses statistical models and machine learning to identify deeper relationships between data elements
Alerting: Analyses events and sends alerts to notify security staff of immediate issues

Dashboards: Creates visualizations to let staff review event data, identify patterns and anomalies.

Retention: Stores long-term historical data, useful for compliance and forensic investigations.
Forensic analysis: Enables exploration of log and event data to discover details of a security incident.

Threat hunting: Enables security staff to run queries on log and event data to proactively uncover threats.

Incidentresponse: Helps security teams identify and respond to security incidents, bringing in all relevant data rapidly.

SOC automation: Advanced SIEMs can automatically respond to incidents and orchestrate security systems, known as Security Orchestration and Response (SOAR).

Capabilities of SIEM productsAtraditional SIEM system has the following basic capabilities:
Real-time security tracking: The central storage and log correlation allows real-time analysis providing alerts about live activity or attacks to take defensive measures.

Threat Intelligence: It provides comprehensive information and refining knowledge about the most common external threats that may endanger an organization.

Behaviour Profiling: learning the user activity and how an organization uses a resource, creates a regular activity profile for different event categories, so it will alert when a possible deviation from normal behaviour is observed.

Data & User Monitoring: checks the identity and authority of a user. After the user's authentication, checks for the authorized files in database that he can access. Any access or modification of an unauthorized file, will be considered abnormal activity and will generate an alert.
Application Monitoring: targeted attacks exploit the weaknesses of an application, such as bugs or vulnerabilities. App level monitoring is the ability to analyse activity streams from applications

Analytics: Includes discovery, interpretation, and communication of important patterns in data security analysis. investigates user's activity and access to detect a threat, violation, or abuse of privileges.

Log Management and Reporting:A SIEM system, manages, stores and analyzes large log files from different sources, such as server logs, system logs, event logs, firewalls, etc. to report an alert.Traditional SIEM

solutions are limited and don't have the flexibility to scale with security requirements while the next generation fills the gaps in the functionality and growing needs about cyberthreat.

Collect and manage datafrom all available sources: This includes cloud service data, on-premise log data (security controls, databases, and application logs), and network data (flows, packets, etc.).

Big data architecture: a big data architecture is needed that can scale the amount of data being collected.

Flat pricing for log ingestion: the pricing is independently of the data you collect. You can ingest data from all sources and remain within your budget.
Automated tracking of lateral movement: it is known that most of attackers involve lateral movement to evade detection or gain access to higher privileges by changing credentials, IP addresses, and assets. To effectively follow lateral movements from beginning to end, the SIEM must be able to tie such related events together.

Improved security information model: security data stored in a useful form factor such as a timeline that contains a complete overview of each entity we are monitoring while legacy SIEM's model mostly based on discrete events. Thus when surfacing abnormal events, expertsystems immediately provide their complete context

Prebuilt incident timelines: using a legacy SIEM usually requires a combination of complex queries which is time consuming and requires deep security domain expertise, mastery of query languages, and theability to interpret results. A modern SIEM can present all available context in a concise and friendly UI.

Enrichment of user and asset context: advances in data science provide many insights that previously had to be correlated by experienced analysts. By using a SIEM that understands context and intent, you can look up asset ownership, user login location, peer groups, and other information that can help you discover abnormal behaviors.

Incident prioritization: large companies generate hundreds of millions of log entries every day that must manage a SIEM. The ability to eliminate false positives and focus only on events with abnormal behaviors is essential for robust security.

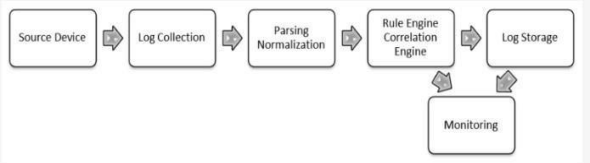
User Event Behavioural Analysis (UEBA): advanced SIEMs use Artificial Intelligence (AI) and deep learning techniques to test human behaviour patterns to detect threats of internal users that are the major threat in an organisation UEBA technique can help to identify

malicious activity before it leads to the theft of sensitive data from corporate networks or servers

Security Orchestration, Automationand response(SOAR): SIEMs integrate with enterprise systems and automate incident response before the attacker acts devastatingly

Problem Solution :

These tools will enable us to create and customize solutions according to user needs, leveraging the advantages of open-source tools with multiple dashboard options for user accessibility.

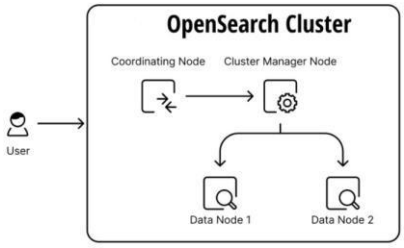


The adaptability of open-source solutions allows us to tailor every aspect to the specific requirements of our unique networks and needs.

Throughout this series, we will extensively explore each of these tools, offering guidance as you embark on building an in-house Security Operations Center (SOC) that aligns with commercial tools available in the market.
The focus extends to the customization and adaptation of the SIEM tool to suit the specific needs and nuances of different organizations. This involves establishing a flexible architecture for seamless integration with various IT infrastructures and compliance with diverse industry regulations and standards. The aim is to provide organizations with a personalized solution that not only meets their current cybersecurity needs but also scales and evolves with their changing security requirements.
Our project involves cultivating a collaborative community around the open-source SIEM tool. This community-driven approach broadens the project's scope by encouraging contributions, feedback, and knowledge- sharing among developers, security professionals, and organizations. It aims to create a dynamic ecosystem where the tool can benefit from diverse perspectives, expertise, and continuous improvement, ensuring its relevance and effectiveness against emerging cyber threats.

Backend Storage: For effective storage of security logs, a backend system is essential. OpenSearch DB is an open-source, distributed search and analytics engine derived from Elasticsearch. It offers high-performance and scalability for indexing and searching large volumes of data. With a vibrant community and compatibility with Elasticsearch APIs, OpenSearch DB is a robust solution for diverse search and analytics applications. This system allows security analysts to search for security events within their desired timeframe. The chosen solution must be fast, reliable, and easily scalable to accommodate the load of collected logs.

The backbone storage component in our SIEM stack is a pivotal element, arguably the most substantial, as it facilitates the storage and visualization of all the security events we collect.
Ensuring a highly available cluster and effective monitoring of system resources (CPU, RAM, Disk) is imperative d urging the deployment of our SIEM stack in a production environment.



Log Intention: Having established the backend storage, we require a tool to dispatch logs to the Indexer. Graylog is a powerful open-source log management and analysis platform. It collects, indexes, and analyzes log data from various sources, providing real-time insights. With user- friendly dashboards and robust search capabilities, Graylog enhances operational visibility, enabling efficient monitoring, troubleshooting, and response to security events in diverse IT environments. Graylog proves to be an optimal choice for this task. It accepts logs from diverse origins such as the tool Manager, network devices, or services supporting syslog forwarding options.

Log Analysis: Log analysis is the systematic examination of log data generated by systems and applications. It involves collecting, processing, and interpreting logs to gain insights into system performance, user activities, and security events. This practice aids in identifying anomalies, troubleshooting issues, and enhancing overall operational efficiency in IT environments

wazuh collects, analyzes, and stores logs from endpoints, network devices, and applications. The wazuh agent, running on a monitored endpoint collects and forwards system and application logs to the wazuh server for analysis. Additionally, you can send log messages to the wazuh server via syslog or third-party API integrations.

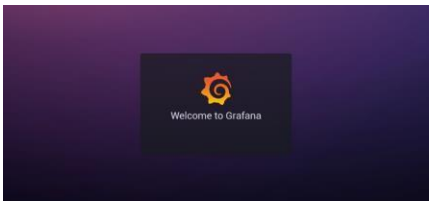
Following the deployment of the backend, an Endpoint Detection and Response (EDR) solution is necessary to record activities on endpoints and workloads in real-time. EDR comprises an Endpoint Agent collecting logs and a Collection Manager analyzing logs for malicious activity.

Endpoint Monitoring: Sysmon (System Monitor) is a Windows utility offering advanced system activity monitoring. Sysmon records detailed information about processes, network connections, and registry modifications. It enhances threat detection, aids in forensic analysis, and is a valuable tool for security professionals in identifying malicious activities on Windows systems.

Utilizing Packet beat enables real-time analysis of network traffic. By deploying Packet beat on our endpoints, we gain the capability to scrutinize incoming and outgoing network traffic associated with these endpoints.
Endpoint monitoring is crucial for real-time visibility into endpoint activities and proactive threat detection. The Agent is deployed on endpoints, offering multi-platform support and a lightweight footprint for effective endpoint monitoring.

SIEM Dashboards: Grafana serves as the visualization tool for building precise dashboards or widgets that enable the visualization of security events, aiding in quick decision-making
it excels in visualization, offering a robust open-source platform for creating dynamic, interactive dashboards. With support for various data sources, including databases and monitoring tools, and also enables users to craft visually compelling representations of data. Its flexibility and rich features make it a preferred choice for real-time analytics and monitoring.

Grafana is an open-source analytics and monitoring platform. It offers dynamic, customizable dashboards to visualize and analyze data from various sources, including databases, logs, and cloud services. Grafana supports data querying, alerting, and collaboration, making it a versatile tool for tracking and interpreting metrics in real-time.



Firewall Log Collection:

Next-Generation Firewalls (NGFW) are advanced security solutions that combine traditional firewall capabilities with advanced features such as intrusion prevention, deep packet inspection, and application awareness. They offer enhanced protection against evolving cyber threats by analyzing and filtering network traffic based on application, user, and content, providing comprehensive security for modern networks Storing network logs is essential for any SIEM stack. We will ingest, parse, and enrich network logs collected from a sense firewall.

SIEM Solutions:

SIEM systems, designed for security policy creation and event management, consist of separate blocks working in tandem. A SIEM platform offers real-time analysis of security events generated by network devices and applications. The new generation of SIEMs provides response abilities, automating the process of selecting and deploying countermeasures. However, current response systems may lack a comprehensive impact analysis of attacks and response scenarios.

Future works:

Potential Advancements in Future SIEMs

Security Information and Event Management (SIEM) tools are predominantly utilized in IT infrastructures where automated detection and response mechanisms are feasible. However, when applied to critical infrastructures, these tools often necessitate manual intervention and in-depth analysis of events before implementing security countermeasures. This section outlines potential enhancements for the next generation of SIEMs, considering

various aspects:

Embracing Diverse Security Measures

Augmenting SIEMs with diversity-related technologies represents a significant leap forward from current solutions. Notably, attention must be directed towards diversity measures, gauging the similarity or dissimilarity of security protection systems, vulnerabilities, and attacks. Unlike metrics for individual components, diversity metrics are relatively underexplored in the literature.

Defining Comprehensive Security Metrics

Future SIEMs should establish security metrics that incorporate quantitative and probabilistic methods. These metrics would aid in decision-making processes, determining the most effective way to combine multiple defences in a given threat environment. This necessitates a profound understanding of how the strengths and weaknesses of diverse defences contribute to the overall robustness of the system.

Addressing the Gap in Diversity Metrics Research While the security community acknowledges the potential value of diversity, there is a dearth of research on diversity metrics compared to metrics for individual components. SIEMs of the future should rectify this imbalance by prioritizing the development of metrics that focus on diverse inputs rather than merely aggregating diverse machine learning techniques.

Moving Beyond Ensemble Methods

While the literature has explored ensemble methods for assessing classification systems in security, the emphasis in future SIEMs should shift towards diverse inputs. This entails a focus on how various security elements, such as protection systems and vulnerability assessments, can contribute distinctively to the overall resilience of the system.

In conclusion, the evolution of SIEMs should encompass a paradigm shift towards embracing and quantifying the diversity of security measures. This not only involves defining robust security metrics but also filling the gap in diversity metrics research to ensure future SIEMs can effectively navigate the complexities of modern threat landscapes.

Conclusion :

In conclusion, the evolution of SIEMs should undergo a transformative shift towards acknowledging and quantifying the diversity of security measures. This necessitates not only the establishment of robust security metrics but also addressing the research void in diversity metrics. The objective is to ensure that forthcoming SIEMs can adeptly navigate the intricate landscapes of modern threat scenarios.

A plethora of open-source tools is at our disposal, providing a cost-effective avenue for constructing our own SIEM stack. The adaptability inherent in open- source solutions enables customization tailored to the unique requirements of individual networks. Throughout this series, we will extensively explore each of these tools, offering guidance as you embark on building an in- house Security Operations Center (SOC) that rivals commercially available solutions.

The advantages of utilizing open-source SIEM tools significantly outweigh any potential risks. Through the embrace of open-source solutions, organizations can enhance visibility into their digital environments, proactively detect security threats, and respond promptly to mitigate risks. Furthermore, open-source SIEM tools embody the principles of transparency, collaboration, and innovation, aligning seamlessly with the modern ethos of cybersecurity practices.

The adoption of open-source SIEM tools signifies a paradigm shift in cybersecurity, empowering organizations to seize control of their security destinies and construct resilient defenses in an ever-evolving threat landscape. By embracing the spirit of open-source innovation, organizations unlock new possibilities, drive meaningful change, and secure their digital assets for the years to come.

REFERENCES:

1. Y. Aillerie, S. Kayal, J. Mennella, R. Samani, S. Sauty, and L. Schmitt, “Smart Grid Cyber Security,” 2013.
2. A.Carcano, A. Coletta, M. Guglielmi, M. Masera, I. N. Fovino, and A. Trombetta, “A Multidimensional Critical State Analysis for Detecting Intrusions in SCADA Systems,” Ind. Informatics, IEEE Trans., vol. 7, no. 2, pp. 179–
3. 186, 2011.
4. ENISA, “Smart Grid Security: Recommendations for Europe and Member States,” 2012.
5. M. Cheminod, L. Durante, and A. Valenzano, “Review of Security Issues in Industrial Networks,” Ind. Informatics, IEEE Trans,2013.
6. H. Khurana, M. Hadley, and D. A. Frincke, “Smart-grid security issues,” IEEE Secur. Priv. Mag., vol. 8, no. 1, pp. 81–85, Jan. 2010.
7. NIST, “NIST Special Publication 1108R2 NIST Framework and Roadmap for Smart Grid Interoperability Standards,” NIST, 2012.
8. C. Alcaraz and J. Lopez, “WASAM: A dynamic wide-area situational awareness model for critical domains in Smart Grids,” Futur. Gener. Comput. Syst., vol. 30, pp. 146–154, 2014.

9. ICS ISAC, “Situational Awareness Reference Architecture (SARA).” [Accessed: 26-Jan- 2014].
10. M. Vidulich, C. Dominguez, E. Vogel, and G. McMillan, “Situation Awareness: Papers and Annotated Bibliography,” Jun. 2006
11. G. P. Tadda and J. S. Salerno, “Overview of Cyber Situational Awareness,” in Cyber Situational Awareness, vol. 46, S. Jajodia, P. Liu, V. Swarup, and C. Wang, Eds. Boston, MA: Springer US, 2010.
12. M. R. Endsley, “Toward a theory of situation awarenss in dynamic systems,” Hum. Factors, 2004.B. McGuinness and L. Foy, “A Subjective Measure of SA The Crew Awareness Rating Scale - GetInfo,” in Proceedings of the first human performance, situation awareness, and automation conference, 2000.
13. E. Zampou, S. Plitsos, A. Karagiannaki, and I. Mourtos, “Towards a framework for energy- aware information systems in manufacturing,” Comput. Ind, Apr. 2014.
14. K. Brancik and G. Ghinita, “The Optimization of Situational Awareness for Insider Threat Detection,” in Proceedings of the first ACM conference on Data and application security and privacy – 2011.
15. F. Baader, A. Bauer, P. Baumgartner, A. Cregan,
    A. Gabaldon, K. Ji, K. Lee, D. Rajaratnam, and
16. R. Schwitter, “A Novel Architecture for Situation Awareness Systems,” in Automated Reasoning with Analytic Tableaux and Related Methods, Springer, 2009.
17. K. A. Stouffer, J. A. Falco, and K. A. Scarfone, Guide to Industrial Control Systems (ICS) Security - Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC). National Institute of Standards and Technology, 2011.
18. G. Suarez-Tangil, E. Palomar, A. Ribagorda, and

I. Sanz, “Providing SIEM systems with self- adaptation,” Inf. Fusion, May 2013.

19. I.Aguirre and S. Alonso, “Improving the Automation of Security Information Management: A Collaborative Approach,” IEEE Secur. Priv. Mag., vol. 10, no. 1, pp. 55–59, Jan. 2012.
20. “Cyberoam iView : The Intelligent Logging & Reporting Solution.”
21. “Prelude-IDS: Prelude Universal Open-Source SIEM project.” .
22. R. H. Syed, M. Syrame, and J. Bourgeois, “Protecting Grids from Cross Domain Attacks Using Security Alert Sharing Mechanisms,” Futur. Gener. Comput. Syst, Feb. 2013.
23. E.Anderson and Y.Chen, “Microcomputer software evaluation: An econometric model,” Decis. Support Syst., Feb.2009.