Security Information and Event Management (SIEM) Performance in on-Premises and Cloud Based SIEM: A Survey

Ranjithkumar S* and M. Mohankumar†
Department of Computer Science, Karpagam Academy of Higher Education, India

Keywords: SIEM, On-Prem SIEM, Cloud SIEM.

Abstract: Security information and event management as a software product for enterprises, medium communities, and small communities. This product has been used for log management, event correlation, incident monitoring. It also checks and analyses the enterprise's hardware, software, and network devices. Now my survey focused on the SIEM product provides various services depending under the category of on-prem and cloud based SIEM, and I classified the products like general information and its performances. On-premises and Cloud SIEM both provide the same services but various platforms. My survey covered how the SIEM are performed under this category and analysis the domain name using selective tools.

1 INTRODUCTION

The ultimate goal of any Security information and event management (SIEM) software is used for to improve an enterprise's security. It performs and analysis the enterprises, event as well as tracking and logging of secured information or data for consistency or inspecting purposes. SIEM is a security solution that assists enterprises with perceiving potential security threats and vulnerabilities before they get incidental to disturb business tasks (Miloslavskaya 2017). This process is associated with threat detection and incident response like provides reports regarding security incidents and event, for example, effective and failed logins malware movement and other potentially malicious activity and send alerts assuming investigation shows that an activity run opposed to predetermined rule sets and event has become a modern-day security operation center for security and compliance management use case (González-Granadillo et al 2021, Pavlik et al 2014, Eswaran et al 2021, Majeed et al 2018). In SIME have some modules that modules performed such as analytics a communities data and monitoring. An SIEM have some modules each modules has performed various activity for enterprise.

2 BACKGROUND

A) Needs of security information and event management (SIEM)

Many industries, enterprises have lots of sensitive data, they are transferring every second so the SIEM has used for monitoring the data from threat attacks and analysis the log collection. This process are categorized three part.

SIM: Security Information Management it performed like log collection, archiving, historical reporting and forensics analysis.

SEM: Security Event Management are used for real-time reporting, log collection, normalization, correlation, aggregation.

SIEM: Security Information and Event Management are performed like log collection, normalization, correlation, aggregation and reporting that anticipate your paper as one part of the entire proceedings, and not as an independent document. Please do not revise any of the current designations.

B. Modules are used in SIEM

SIEM have modules they are performed for monitoring, reporting and collecting a log data in enterprises.

* MSc
† Associate Professor

S, R. and Mohankumar, M.
Security Information and Event Management (SIEM) Performance in on-Premises and Cloud Based SIEM: A Survey.
DOI: 10.5220/0012613800003739

In *Proceedings of the 1st International Conference on Artificial Intelligence for Internet of Things: Accelerating Innovation in Industry and Consumer Electronics (AI4IoT 2023)*, pages 627-633
ISBN: 978-989-758-661-3

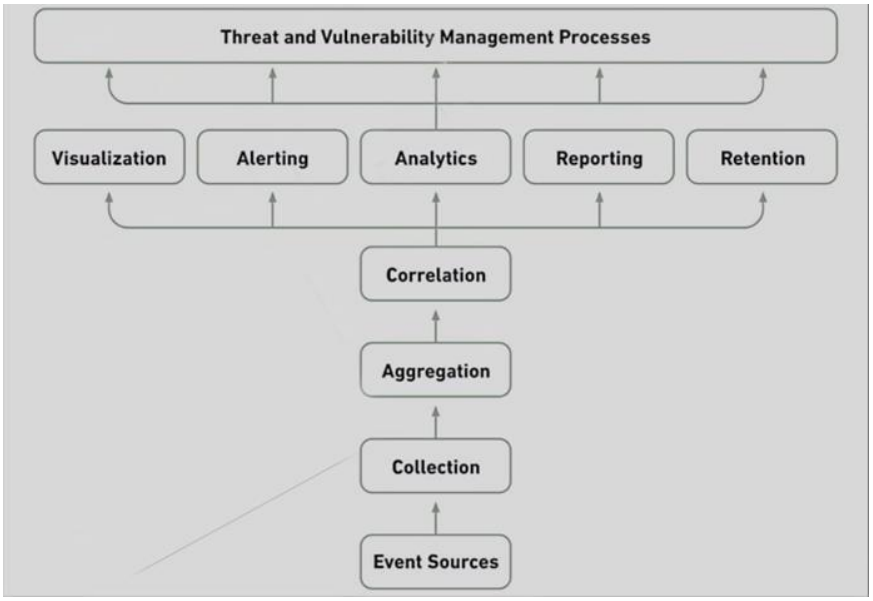


Figure 1: SIEM Architecture.

1) Log Management or Data Aggregation
Log management is primarily used for collecting log data for monitoring their security posture using log

files and SIEM is primarily used for security they check and analyses the logging event for possible attacks. It has two methods:

Pull Method: The way of acquiring the log data is difficult to configure since SIEM connects to data sources on request. SIEM known exactly what data is collected so this method generally safe (Pavlik et al 2014).

Push Method: The data or information sent to source device itself so this is easier method for configure SIEM. The SIEM role only recipient of data and does not directly manage the devices but this method has drawback in security vulnerability (Pavlik et al 2014).

2) Event Correlation
Event correlation is a process of normalizing and correlation of incoming logs to help easily detect a security threat in our system like it detect problems and uncover their root cause. Using an event correlation helps monitoring the system in organization or enterprises more effectively while improving their up-time performance. The devices with high event rates, excessive database connection and excessive firewall accepts from multiple sources to a single destination and authentication like login failure attempt to disabled account, login failure to expired account, and multiple login failure for single username (Majeed et al 2018).

3) Incident Monitoring
It is mainly used to keep running an organization service smoothly, while an incident as happen, they are system outage and at the same time the cost of the system outage is higher for recovery. For example, in up time institute 2022 outage analysis report says, more than 60% of outages cost over $100,000, which is an increase from 39% in 2019 and in 2021 Facebook outage, is a best example for purpose of SIEM incident monitoring, the Facebook, WhatsApp, Instagram were unreachable for around six hours. Over 14 million people are reported. Experts estimated that each minute of downtime cost the company $163,565, that means totalling around $60 million in single day it a huge amount (Marija et al 2023).

4)Forensic Analysis
In Forensic analysis for SIEM they have some requirements like no intrusion, integrity, accuracy, justification, no assumptions, high performance, retention, data relevance, timestamps and commensurable results (Erko 2022).

5)Security Data Analysis
Security data analytics or data visualization allows the visual representation of security data like illustration, interpretation, storytelling, unlocking the sight, facilitating deep search in the data, exploration, pattern finding, extracting, details-on-demand (Majeed et al 2018).

Table 1: General information of SIEM software tools.

s.no	SIEM Tools	On-prem	Cloud SIEM	OS Platform	Pricing
01	Splunk	Y	Y	Windows, mac, Linux, Solaris	Quote based
02	Sumo logic	Y	Y	Windows, Linux, mac	$99 to $165/month
03	Manage Engine log 360	Y	-	Windows, website, mac	Quote based
04	Alien vault OTX	Y	Y	Windows, Linux, mac	Open source(on-prem)
05	IBM Qradar	Y	Y	Windows, mac, Linux	Quote based
06	Varonis	Y	Y	Windows, Linux, mac	$17,000/license
07	LogRhythm	Y	Y	Windows, CentOS, Linux	Quote based
08	Rapid 7 insight	-	Y	Windows, Linux, website	$19 to $2000
09	Solar winds	Y	Y	Windows, Linux, mac, Solaris, website	$4665
10	Salesforce	-	Y	Windows, mac, Linux, android, iOS	$25/user/month

Table 2: SIEM performances (González-Granadillo, G. et al., 2021).

	SIEM Tools				
	Splunk	Alien vault OSSIM	IBM Qradar	LogRhythm	Solar winds
Security data analytics	Advanced	Average	Advance	Advance	average
Forensic analysis	Average	Advance	Advance	Average	average
performance	Average	Average	Average	Average	Advance
UEBA	Advance	Basic	Advance	Advance	Basic
Correlation and event monitoring	Basic	Basic	Average	Advance	Advance

6) Real Time Event Response

It can detect and respond to interaction with critical data and provide an intuitive. Real time presentation of what data is being accessed by whom where and when (Eswaran et al 2021).

7)Threat Intelligence

Threat intelligence is the process of recognizing or determining any unknown threats that the organization can identify and defense mechanisms can be used to prevent such occurrences.

8)User and Event Behavior Analytics (UEBA)

User Behavior Analytics is a term that includes tracking, collecting, and categorizing user data and activities in their communication in the digital environment, respectively in a computer network environment (Makkar et al 2018). UEBA uses three module they are Data analytics, Data integration, Data presentation and visualization. UEBA uses machine learning principles to identify future user behavior (Svoboda 2021).

How has cloud SIME redefine threat detection in on-premises deployments, organizations are responsible for the whole security stack from the physical hardware infrastructure to the data stored on it. In cloud based SIEM there is split the shared responsibility models of leading cloud providers like (AWS, Microsoft azure, google) it set out that while the cloud service provider (CSP) takes responsibility for the security and maintenance of nay supporting hardware. It is the individual organizations responsibility to secure and maintain the data on those systems. If not managed correctly this creates a potential visibility gap in the business attack surface.

3 DISCUSSION

On-Prem or On Premises SIEM

On-prem or on-premises refers to IT infrastructure hardware, software applications that are hosted on-site. It is the more traditional method for working with enterprise software and typically requires a software license for each server or end user that will be working with the software (Beal 2021) and an organizations complete control over their data since the data is stored on their own premises. Many legacy

and traditional data center resources are on-premises, and they are used to everything that is done inside whereby backup, privacy, and update should be managed in house installed on server.

Cloud Based SIEM

For all intents and purposes generally driving SIEM framework began as on-prem arrangement the majority of the sellers presently support cloud SIEM or SaaS variants of their individual SIEM stage. The cloud SIEM provides an effective and efficient way to constantly monitor all devices, servers, applications users and infrastructure components on our network that are all from one central cloud SIEM (Marija, 2023). It controls monitoring systems, applications and workloads, anywhere in your network and it gets a real time alert on security incidents, server as the basics for risk analysis and audits and the event log data is automated compliance reporting. parts on our organization that are all from one focal cloud SIEM It controls monitoring systems, applications and workloads, anywhere in your network and it gets a real time.

Pros of On-Prem or On-Premises

An association keeps authority over the SIEM platform by keeping our SIEM on-premises. We can customize how the platform runs and setup to deliver the best outcome with regards to the business activity. This customization can more precisely reflect the manners in which partners associate with our system and improves overall works on in general security and effectiveness. The association keeps control over the Cyber security team by keeping the team running the SIME stages or platforms in house and furthermore keeping control over preparing the team members to explicit requirements of your business. This approach enables associations to have custom SIEM administration service take in policy's custom made to the associations business context.

Cons of On-Prem or On-Premises

Security information and event management (SIEM) platform-on-premises require financial endeavours that are restrictive for some organizations except for huge and global enterprises. The general expense isn't restricted to the consumption for buying, introducing and keeping up with the product yet incorporates the expense for collecting, storing and analyzing large amount of information from each collecting point. Recruiting, preparing and overseeing learned cyber security expert in organization is costly while IT security ability is popular and requires keeping these employees on finance An association needs to both find and recruit high point specialists in the field of Cyber security, yet it likewise needs it trained them to deal with a complex SIEM to comprehend an association plan of action that implies the most common way of executing a functional SIEM stage can requires a year or significantly really relying upon the size of association or enterprises.

Pros of Cloud Based SIEM

A significant benefit of cloud SIEM is that association promptly accesses expert knowledge, and these is no compelling reason need to prepare your workers and get a per-designed SIEM framework operated by a group that knows the intricate details of alert on security incidents, server as the basics for risk analysis and audits and the event log data is automated compliance reporting dealing with the stage it decreases the ideal opportunity for organization as these is no compelling reason need to prepare. Choosing cloud based SIEM brings about cost saving because of the SIEM sellers, taking consideration for investing resources into framework in SIEM-as-a-service situation, our association doesn't buy costly equipment to run SIEM platform.

Cloud based SIEM can likewise deal with the product upkeep backing and updates, which takes out our expenses related to having an inner IT support group to manage the SIEM upkeep.

Cons of Cloud Based SIEM

An association is continuously confronting chances while moving secret or sensitive information off-site. The risks associated with data in transit are always greatest as compared to data in transit. Some cloud SIEM sellers focus on around the monitoring and detailing elements of their system, and it is related with the absence of appropriate threat the executives and threat remediation (Data shield 2023). Cloud based SIEM solutions, we disapprove of merchants restricting your access to raw log information even though this is your information that comes from your endpoints and system having limitless access to raw log information for making your own analyses and estimate is critical.

Industrial Trends

The splunk platform removes the barriers between data and action, empowering observability, IT and security teams to ensure their organizations are secure, resilient and innovative. They are providing solutions are:

By Use Case*:* advanced threat detection, application modernization, cloud migration, incident investigation & forensics, IT modernization, SOC automation & orchestration.

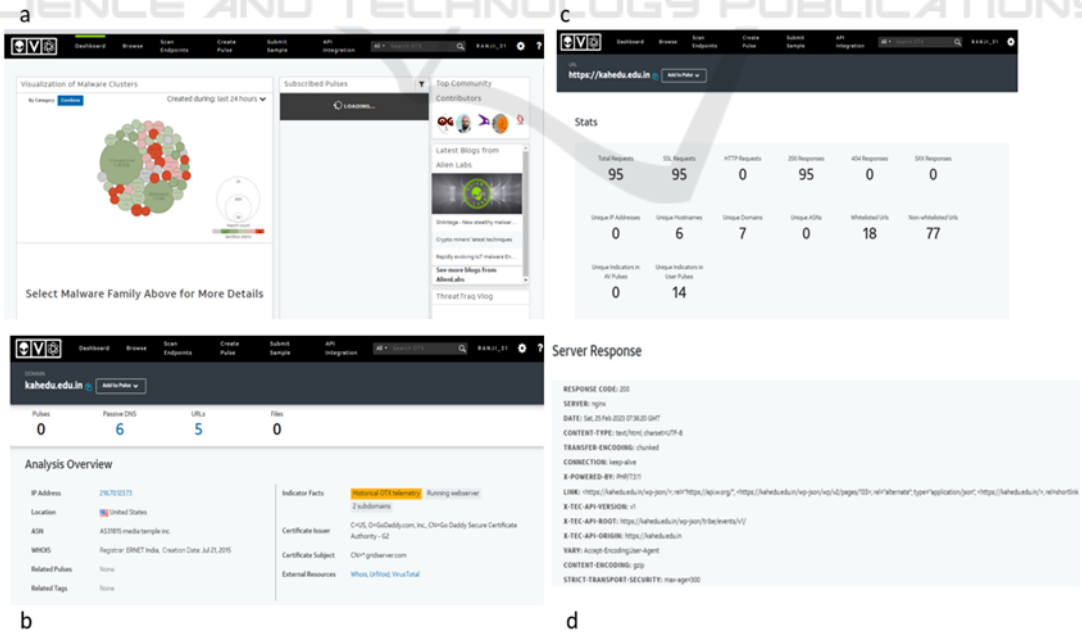
By Technology: AWS, Azure, GCP, kubernetes, open telemetry, SAP.
By Industry: Aerospace & defense, Energy & utilities, financial services, Healthcare, Higher education, public sector.

2)Alien Vault
Alien vault is product of AT&T CyberSecurity company it has providing two types of products.
OTX: Open Threat Exchange it provides open access to a global community of threat researchers and security professionals. It delivers community-generated threat data, enables collaborative research and automates the process of updating your security infrastructure with threat data from any source (Alienvault, 2023).
OSSIM: Open source SIEM (Alien Vault OSSIM) addresses this reality by providing one unified platform with many of the essential security capabilities like asset discovery, vulnerability assessment, intrusion detection, behavioral monitoring, SIEM event correlation (Marija, 2023).

3)IBM Qradar
IBM Qradar SIEM is the core module of qradar security intelligence platform that allows obtaining accurate analytical data on security events in real time (IBMOradar, 2023). IBM QRadar providing solutions are full integrated NDR, Automatic parsing and normalizing of logs, Identify and correlation, Intuitive, automatic query builder, user behavior analytics, Threat intelligence, breadth of services in threat detection of organization, Real-time threat detection, UBA (IBMOradar, 2020).

4)Log Rhythm
Log Rhythm SIEM platform delivers comprehensive security analytics, UBEA, NTA, and SOAR within a single, integrated platform for rapid detection, response and neutralization of threats. LogRhythm platform strengthens the maturity of customer security operations and processes like centralized forensic visibility, mean time to detect and mean time to respond (Siem, 2022).

5)Solar Winds
Solar winds SIEM is virtual appliance that adds value to existing security products and increase efficiencies in administering, managing and monitoring security policies and safeguard on our network, solar winds providing solutions are:
By Use Case: hybrid cloud observability, DB management, Application management, solar winds Orion platform, network management, IT Asset management, IT security, IT operation management, IT help desk, Remote monitoring, infrastructure, IT service management, IT automation, compliance, remote infrastructure management, hybrid system monitoring, secure remote access (Solar winds, 2023).



Report; (c) Status of the Domain; (d) Server Response.

Figure 2: (a) Alien Vault Dashboard; (b) Domain Analysis

By Technology: Azure, active directory, cisco, office 365, MySQL, SQL diagnostic (Solar winds, 2023).

4 ANALYSIS AND RESULTS

Domain name is important one for websites. In my analysis shows how the threat has detected in domain name using some SIEM tool. I've take a tool (AlienVault OTX) For analysis the domain.

AlienVault OTX: First we create a OTX pulse. Pulse provide is a summary of the threat, indicators of compromise (IOC) it includes IP address, Domains, Hostnames & subdomains, Emails, URL, URI, file hashes like MD5, SHA256, PEHASH, IMPHASH, CIDR Rules, File Paths, MYTEX name, CVE number (Alienvault, 2023).

An AlienVault dashboard shows the realtime visualization of malware cluster. It explain the type of malware family and its detailed information. They are classified in different colour like algae green and red. The algae green is represent negative sandbox alert and the red colour is mention by positive sandbox alert. The visualization of malware family show the detailed information of the family, number of count, feature count and the alienvault have endpoint scan, check pluse. In my case i've select random domain name for analysis purpose. It show the detailed information about the domain name, sub domain name, and URLs Domain analysis report Figure 1.2 show the given domain details and pluses, like sub domain, host address, ip address of the domain, Certificate Issuer details, and hash type.

In Figure 1.3 is show the status of the Domain like Total Request, SSL request, server Responses, Hostname, Whitelisted URLs, Non-whitelisted URLs, and pluses and Figure 1.4 as show the server status of the given domain like, connection, Encoding-type, version of the domain.

5 CONCLUSION

The needs of SIEM are higher for an organizations or enterprises, an SIEM tools are providing various platform-based services like cloud based SIEM and on-premises SIEM and it has some merits and demerits. my survey has explored how the SIEM are performed and analyses the enterprise data, and I mentioned AlienVault OTX tool performances. Why we choose this particular tool because it is an open source and it user friendly. This performance also is pretty good and detailed.

REFERENCES

Miloslavskaya, N. (2017). Analysis of SIEM Systems and Their Usage in Security Operations and Security Intelligence Centers. Advances in Intelligent Systems and Computing, 282–288. https://doi.org/10.1007/978-3-319-63940-6_40

González-Granadillo, G.; González-Zarzosa, S.; Diaz, R. Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. Sensors 2021, 21, 4759. https://doi.org/10.3390/s21144759 (for table)

Pavlik, Jakub, et al. "Security Information and Event Management in the Cloud Computing Infrastructure." 2014 IEEE 15th International Symposium on Computational Intelligence and Informatics (CINTI), IEEE, Nov. 2014. Crossref, https://doi.org/10.1109/cinti.2014.7028677. (background->architecture of siem)

Eswaran, Sivaraman, et al. "A Threshold-based, Real-time Analysis in Early Detection of Endpoint Anomalies Using SIEM Expertise." Network Security, vol. 2021, no. 4, Mark Allen Group, Apr. 2021, pp. 7–16. Crossref, https://doi.org/10.1016/s1353-4858(21)00039-8. (real-time event response)

Majeed, Abdul, et al. "Near-miss Situation Based Visual Analysis of SIEM Rules for Real Time Network Security Monitoring." Journal of Ambient Intelligence and Humanized Computing, vol. 10, no. 4, Springer Science and Business Media LLC, July 2018, pp. 1509–26. Crossref, https://doi.org/10.1007/s12652-018-0936-7. (event correlation and security data analysis)

Makkar, A., Kumar, N.: User behavior analysis-based smart energy management for webpage ranking: Learning automata-based solution. Sustain. Comput. Inf. Syst. 20, 174–191(2018) https://doi.org/10.1016/j.suscom.2018.02.003.ISSN22105379 (UEBA)

Svoboda, Tomas, et al. "Behavioral Analysis of SIEM Solutions for Energy Technology Systems." Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, Springer International Publishing, 2021, pp. 265–76. Crossref, https://doi.org/10.1007/978-3-030-67101-3_21. (UEBA) Internet References

Jeferson Martínez, Javier M. Durán. "Software Supply Chain Attacks, a Threat to Global Cybersecurity: SolarWinds' Case Study", International Journal of Safety and Security Engineering,2021 (intro)

Press releases (no date) Uptime Institute. Available at: https://uptimeinstitute.com/about-ui/press-releases (Accessed: December 31, 2022).

Marija Mladenovska Jan 9 (no date). What is a cloud siem?, AT&T Cybersecurity. Available at: https://cybersecurity.att.com/blogs/security-essentials/ cloud-based-siem (Accessed: January 1, 2023).

What is Security Information and Event Management (SIEM)? (no date) IBM. Available at: https://www.ibm.com/topics/siem (Accessed: January 1, 2023).

Datashield (no date) On-premise vs Cloud Siem - Advantages & Disadvantages, SAAS, Gartner, On-Premise vs Cloud SIEM - Advantages & Disadvantages, SaaS, Gartner. Available at: https://www.datashieldprotect.com/blog/on-premises-vs-cloud-siem (Accessed: January 1, 2023).

Beal, V. (2021) What is siem security incident and event manager?, Webopedia. Available at: https://www.webopedia.com/definitions/siem/ (Accessed: January 1, 2023).

Erko, A. (2022) Key requirements for forensic features in Siem solutions, Apriorit. Available at: https://www.apriorit.com/dev-blog/476-requirements-forensic-features-siem (Accessed: January 1, 2023)

About splunk: What is splunk? (no date) Splunk. Available at: https://www.splunk.com/en_us/about-splunk.html (Accessed: January 1, 2023).

Alienvault Open Threat Exchange (OTX) the world's largest Open Threat Intelligence Community that enables collaborative defense with actionable, community-powered threat data (no date) AlienVault Open Threat Exchange (OTX) | Unified ThreatWorks.com. Available at: https://www.unifiedthreatworks.com/OTX.asp (Accessed: January 1, 2023).

Marija Mladenovska Jan 9 (no date) AT&T Cybersecurity Services, AT&T Cybersecurity. Available at: https://cybersecurity.att.com/products/ossim (Accessed: January 2, 2023).

IBM Qradar (no date) IBM QRadar SIEM for Security Intelligence - ScienceSoft. Available at: https://www.scnsoft.com/services/security/siem/ibm-qradar (Accessed: January 2, 2023).

IBM Qradar SIEM product and solutions (2020) IBM Products. Available at: https://www.ibm.com/products (Accessed: January 2, 2023).

Siem: Security Information and Event Management (2022) LogRhythm. Available at: https://logrhythm.com/solutions/security/siem/ (Accessed: January 2, 2023).

Solar winds Infrastructure solutions (no date) SolarWinds. Available at: https://www.solarwinds.com/solutions/infrastructure-solutions#:~:text=SolarWinds%20can%20help%20you%3A%201%20Monitor%20physical%20and,who%20and%20what%20is%20connected%20to%20your%20network (Accessed: January 2, 2023).