Evaluating SIEM RADAR: A New Metric for Enhancing Regulatory and Compliance Efficiency

Ertuğrul Akbaş
Computer Engineering, Istanbul Esenyurt University, SureLog SIEM İstanbul, Turkey,

eakbas@gmail.com

Abstract: This research paper explores the modern cybersecurity landscape, particularly focusing on the risks associated with SIEM products and SOC services. It underscores the critical issue of insufficient logging practices that compromise an organization's threat detection and response capabilities, thereby increasing the risk of security breaches. The importance of real-time log retention to address evolving digital threats is highlighted, with recommended retention periods from authoritative sources such as the White House, OWASP, MITRE, and SANS. The paper also addresses scalability challenges due to the exponential growth of log data, the necessity for effective correlation within SIEM systems for timely threat detection, and the importance of compliance with various standards and regulations to enhance security. This comprehensive analysis provides valuable insights for cybersecurity professionals, organizations, and policymakers. Categories and Subject Descriptors: C.2.0 [**Computer-Communication Networks**]: General—Security and Protection; D.4.6 [**Operating Systems**]: Security and Protection; H.5.3 [**Information Interfaces and Presentation**]: Group and Organization Interfaces. **General Terms:** Design, SIEM, Security

Keywords: Security Information and Event Management, Log, SIEM, SOC, Cyber Security, Insufficient logging, Live Log, Hot Log, Log Loss, Correlation

1. Introduction

SIEM solutions and SOC services are foundational elements in modern cybersecurity, crucial for protecting organizations against sophisticated cyber threats. However, their effectiveness can be significantly undermined by challenges ranging from log management intricacies to data correlation complexities. This paper takes a unique approach by evaluating these security measures in alignment with legal requirements, governmental orders, industry regulations, and best practices.

The significant issue of insufficient logging is highlighted with real-world statistics demonstrating its impact on security. For instance, scenarios like the Stuxnet Worm Attack and the 2017 Verizon Communications Data Breach reveal the dangers of inadequate logging and monitoring, which allowed severe breaches and data exposures.

The objective of this paper is to explore these vulnerabilities in-depth, providing a comprehensive understanding of how they can erode an organization's security posture and what can be done to mitigate these risks effectively.

This paper is structured as follows: After this introduction, we delve into the current methodologies for evaluating SIEM solutions, followed by a detailed discussion on the importance of log retention, the challenges of log scalability, and the critical role of effective correlation within SIEM systems. We then examine compliance requirements and conclude with strategic recommendations for strengthening security postures in the face of evolving cyber threats. This comprehensive framework aims to equip cybersecurity professionals, organizations, and policymakers with the necessary insights to enhance their security strategies effectively.

2. Current Methodologies in Evaluating SIEM Solutions

In evaluating SIEM solutions, this paper identifies several limitations that are often overlooked in traditional analyses. The comparison of SIEM features across various products, as depicted in Table 1 and Table 2, provides a foundation for discussing these limitations. However, instead of listing features, a more nuanced approach is taken to discuss the underlying issues and gaps in SIEM functionalities.

Table 1. Analysis of different SIEM solutions (Sheeraz,M. et al 2018.)

Functionality	ArcSight	QRadar	McAfee	LogRhythm	USM-OSSIM	RSA	Splunk	SolarWinds
Correlation rules	○	○	●	●	●	○	–	●
Data sources	●	●	●	○	○	●	●	○
Real time processing	●	●	●	●	●	●	●	●
Data volume	●	○	●	○	○	○	●	○
Visualization	–	○	○	○	○	○	●	○
Data analytics	○	●	○	●	○	○	●	○
Performance	○	○	●	○	○	●	○	●
Forensics	–	●	●	○	●	●	○	○
Complexity	●	○	○	○	○	●	●	●
Scalability	●	●	●	●	–	●	●	●
Risk analysis	–	○	○	○	–	○	–	○
Storage	○	○	●	○	○	○	○	●
Price	●	●	●	○	○	●	●	○
Resilience	○	●	●	○	○	●	○	○
Reaction and reporting	–	–	●	●	–	○	○	○
UEBA	●	●	–	●	–	●	●	–
Security	●	●	–	–	○	○	○	–

– Low/Basic ○ Average ● High/Advanced.

The common features across SIEM systems, including correlation rules, real-time processing, data analytics, and user and entity behavior analytics (UEBA), are critical for effective security monitoring. However, despite their presence, significant gaps remain in the practical application of these features. For instance, real-time processing is often constrained by the scalability of the system as log volumes increase, which can lead to delays in threat detection and response. Similarly, while correlation rules are fundamental to identifying security threats, they require continuous updates and tuning to remain effective against evolving attack vectors.

Furthermore, the integration of threat intelligence is another area where SIEM systems often fall short. Although many SIEM solutions claim to incorporate threat intelligence, the effectiveness of this integration varies significantly. The ability to dynamically adapt to new threats based on reliable intelligence feeds is crucial, yet many systems struggle to update their operational parameters swiftly enough to counteract new threats effectively.

These limitations highlight the need for ongoing research and development in SIEM technology to address these critical gaps. By understanding the deficiencies in current methodologies, organizations can better prepare for and respond to cybersecurity threats. This analysis sets the stage for exploring advanced solutions and adaptations in SIEM technologies to enhance their efficacy in the ever-changing cybersecurity landscape.

Table 2. Analysis of different SIEM solutions (Granadillo,G. and González-Zarzosa,S. and Diaz,R. 2021)

Feature	Open-Source SIEM					Proprietary SIEM					Proposed
	OSSIM	ELK	Wazuh	MozDef	SIEMonster	QRadar	Splunk	Securonix	Exabeam	LogRhythm	SIEM
Real-time monitoring	✓	✓	✓	×	✓	✓	✓	✓	✓	✓	✓
Threat intelligence	×	✓	✓	×	✓	✓	✓	✓	✓	✓	✓
Behavior profiling	✓	✓	×	✓	×	✓	✓	✓	✓	✓	✓
Data monitoring	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
User monitoring	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Application monitoring	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Analytics	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Log management	×	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Updates	✓	✓	✓	✓	×	✓	✓	✓	✓	✓	✓
Reporting	×	✓	✓	×	✓	✓	✓	✓	✓	✓	✓
GUI	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Detailed system description	×	×	×	×	×	×	×	×	×	×	✓
Database	MySQL	ES	MySQL	ES	ES	Ariel	GZip-files	A.Hadoop	ES	SQL-server	MySQL

ES=Elasticsearch.

3. Insufficient Logging

In the realm of cybersecurity, sufficient logging practices are indispensable for effective threat detection and incident response. However, a pervasive issue among various organizations is insufficient logging, which significantly impedes their ability to manage security threats efficiently. This section introduces the Event Volume Score (EVS), a novel metric designed to quantitatively assess and compare the logging practices of organizations, informed by standards such as those set by MITRE and SANS.

The EVS is a comprehensive metric that evaluates the adequacy of logging based on three primary criteria:

- Frequency of Log Generation: Measures how often logs are recorded, capturing the timeliness of log entries in response to security events.
- Variety of Log Sources: Assesses the diversity of sources from which logs are collected, reflecting the breadth of monitoring across the network and systems.
- Detail Level of Logs: Analyzes the granularity and relevance of the information captured in the logs, crucial for detailed forensic investigations and effective threat detection.

A higher EVS indicates robust logging practices that enhance an organization's capability to detect and respond to cyber threats promptly and accurately.

Companies should calculate EPS values according to this table, and if it is different, then it means inadequate logging, a concern highlighted in the OWASP Top 10 Web Application Security Risks – 2021 (OWASP. “Top 10 Web Application Security Risks”, 2021), OWASP Top 10 API Security Risks – 2019 (OWASP. “OWASP Top 10 API Security Risks – 2019”, 2019), OWASP Top 10 Application Security Risks – 2017 (OWASP. “OWASP Top Ten 2017”, 2017.)

Insufficient logging is also listed as a vulnerability in the MITRE CWE database [13,14]. Common Weakness Enumeration (CWE) is a cybersecurity standard developed by MITRE. CWE provides a list of software and hardware weaknesses and vulnerabilities. This listing is developed to enhance the security of computer systems and software and to strengthen defense against cyber-attacks. It is a database that assigns a number and includes a description to identify a type of error or vulnerability. This enables security experts and software developers to identify and address potential vulnerabilities with guidance.

Another challenge of log loss or unsuccessful log filtering is the potential reflection in the need for log access as required by standards like GDPR, PCI. Failing to access the necessary proof or logs in such contexts can lead to legal consequences.

Table 1: Baseline Network Device EPS Averages

Qty	Type	Description	Avg EPS	Total Peak EPS	Average Peak EPS
750	Employees/Endpoints (Windows XP)	Desktops & laptops at 5 locations	Included at domain servers	Included at domain servers	Included at domain servers
7	Cisco Catalyst Switches	One at each location, one in DMZ and one in the Trusted network	5.09	51.88	26.35
7	Cisco Gateway/Routers	One at each location	0.60	380.50	154.20
5	Windows 2003 Domain Servers	One at each location	40.00	404.38	121.75
3	Windows 2003 Application Servers	In high availability cluster at data center	1.38	460.14	230.07
3	MS SQL Database Servers running on Windows 2003 Server	High availability cluster at data center	1.83	654.90	327.45
6	Microsoft Exchange Servers	One at each location with two (cluster) at the data center	3.24	1,121.50	448.60
3	MS IIS Web Servers on Windows 2003	High availability cluster at data center	1.17	2,235.10	1,117.55
2	Windows DNS Servers	At data center – failover	0.72	110.80	110.80
2	Linux Legacy Application Servers	At data center	0.12	43.60	21.80
1	Linux MySQL Database Server	One in Trusted network for legacy application	0.12	21.80	21.80
7	NitroGuard IPS	One at each location, one in DMZ and one in the Trusted network	40.53	5,627.82	1,607.95
1	Netscreen Firewall	Netscreen facing the Internet	0.58	2,414.00	2,414.00
3	Cisco Pix Firewalls	Between the data center and the other four sites, in front of Trusted network, between Trusted and the DMZ	39.00	1,734.00	1,178.00
1	Cisco VPN Concentrator	Located at data center Facing the Internet	0.83	69.45	69.45
1	Squid Proxy	Located at data center	14.58	269.03	269.03
		Totals:	**149.79**	**15,598.90**	**8,118.80**

Figure 1. SANS EPS calculation table

3.1 Examples of Insufficient Logging and Monitoring Attacks

Without proper monitoring and logging of network traffic, businesses fail to prevent attackers from installing malware and accessing crucial data. In recent history, the following are some of the well-known examples of security incidents arising from insufficient logging and monitoring:

The Stuxnet Worm Attack on Iran's Nuclear Program. The Stuxnet worm is a masterfully crafted Malware that attacks Supervisory Control and Data Acquisition (SCADA) systems. In 2010, the security team at the Iranian nuclear program discovered that the bug had been used to access critical weapons control systems.

On deeper analysis, the bug was active since 2005 and spread using infected USB drives. The hackers took advantage of poor logging and monitoring mechanisms to gain elevated access discreetly.

The 2017 Verizon Communications Data Breach. While no data was stolen, Verizon admits that at least 14 million customer records were exposed to the internet in a data breach discovered in 2017. These records included such data as phone numbers and account PINs. This data was not password-protected, and attackers could have easily downloaded and exploited it. However, the records were stored in a cloud-based data repository and were discovered by a cybersecurity researcher before any attackers could take advantage of the loophole.

The 2019 Dominion National Data Breach. In 2019, Insurer Dominion National discovered that members of its health plans could have been exposed to a data breach that lasted more than nine years. The breach, which was determined to have affected over 2 million individuals, exposed sensitive customer data, including:

- Bank account numbers Routing numbers
- Taxpayer identification information social security numbers
- Names and Dates of Birth among others

After an exhaustive investigation, it was determined that this information was not accessed or used by unauthorized persons. Dominion National was, however, ordered to cover any claims for monetary losses reasonably traceable to the breach.

4. Hot, Live, Online, Immediately Available Log Retentions

It is now understood that archiving logs is insufficient from various practical aspects, including legal and cybersecurity concerns. Keeping logs live, meaning being able to go back years for evidence and logs when needed, has been proven essential in numerous studies and literature reviews about incident response against advanced attacks. Moreover, this has become a requirement through laws and standards, surpassing research and development. For instance, there's a presidential memorandum in the United States specifying that logs should be kept live for at least 1 year, and there's an order for at least 1.5 years of archiving. The "Memorandum for the Heads of Executive Departments and Agencies," published by the Executive Office of the President, Office of Management and Budget (**2021."MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES")**

Across the globe, a multitude of standards, laws, and illustrative best-case scenarios concerning the vital role of live logs have been disseminated (2021."Event Logging Guidance from Treasury Board of Canada Secretariat", Google."Retaining Logs for A Year: Boring or Useful?", 2019, SANS. "An Evaluator's Guide to NextGen SIEM", 2018, NIST. "Assessing Security and Privacy Controls in Information Systems and Organizations" 2022, "Vadodara Smart City Development Limited (VSCDL)" 2021). This burgeoning body of knowledge underscores the paramount importance of real-time, dynamic log data in the realm of cybersecurity. As the digital landscape continues to evolve, the significance of live logs has become more pronounced, serving as a beacon for organizations striving to fortify their security postures.

In this evolving landscape, a paradigm shift has occurred. The conventional reliance on archived logs for incident response has been debunked, as the shortcomings of such an approach have become glaringly apparent. Timely incident response demands the immediacy and accuracy that only live logs can provide. These logs, capturing events as they unfold, offer a real-time perspective that is invaluable in identifying and mitigating security breaches promptly.

In light of this realization, a clarion call echoes across the industry: companies and organizations must reevaluate their approach to log management. The static nature of archived logs falls short in meeting the demands of modern cybersecurity, where threats can materialize in moments. Acknowledging this, proactive measures are

indispensable. Organizations should not only embrace the usage of live logs but also elevate their status as a vital risk parameter.

The heart of this transformation lies in the realm of SIEM solutions and the acquisition of SOC services. These pivotal tools stand as the vanguard of an organization's defence against the ever-evolving landscape of cyber threats. However, their efficacy hinges on the quality and timeliness of the data they process. Live logs, as an integral component of this data, assume an outsized role in bolstering an organization's resilience. Therefore, the imperative is clear: companies and organizations must regard live logs as a linchpin in their cybersecurity strategy. The integration of live logs into the fabric of SIEM solutions and SOC services enhances the accuracy of threat detection, facilitates rapid incident response, and bolsters post-incident analysis. By recognizing live logs as a formidable risk parameter, organizations set the stage for a proactive stance against potential breaches. To this end, taking measures to optimize the collection, aggregation, and analysis of live logs is paramount. Automation, advanced analytics, and real-time monitoring must be harnessed to ensure the efficacy of these logs in a dynamic threat landscape. Compliance with industry standards and regulations further underscores the significance of live logs, as their utilization aligns with the best practices advocated by these frameworks.

In conclusion, the era of static, archived logs as the cornerstone of incident response has passed. The ascendancy of live logs in the cybersecurity narrative is undeniable. With a shift in perspective, organizations can embrace the agility and accuracy that live logs offer. This paradigm shift beckons companies and organizations to leverage live logs as a vital component in their cybersecurity arsenal, navigating the complexities of modern threats with vigilance and confidence.

4.1 Challenges

The exponential growth of log data poses challenges in managing and retaining large volumes of logs. There are different technologies in the market. For example, Apache Lucene's indexed (hot, live) log growth formula:

disk space used(original) = 1/3 original for each indexed field + 1 * original for stored + 2 * original per field with term vectors

There are other technologies utilized by some SIEM vendors that compress both the indexes and raw logs. Organizations must contend with scalability issues and invest in robust log storage and management solutions to accommodate the influx of log data. Log volume increases can be unmanageable both in terms of price and disk size.

5. Log Investigation: an Indispensable and Crucial Part of Incident Response

Log investigation is indeed a crucial and indispensable part of incident response. Logs serve as a valuable source of information, providing insights into the activities that transpire within an information system. They encompass a wide range of data, including network traffic, system events, user actions, and application activities. By thoroughly analyzing logs, security analysts can unlock various benefits and effectively respond to security incidents.

1. Detection of Indicators of Compromise (IOCs): Logs play a pivotal role in identifying IOCs, which are signs or evidence of a security breach or compromise. Security analysts can examine logs for patterns, anomalies, or specific events that indicate unauthorized access, malicious activities, or potential vulnerabilities. These IOCs might include IP addresses, file modifications, failed login attempts, or abnormal behavior.
2. Tracing the Steps of an Attacker: Through log investigation, analysts can retrace the steps of an attacker, reconstructing the sequence of events that led to a security incident. By analyzing network logs, system logs, and other relevant logs, analysts can determine the attack vectors, techniques employed, and the extent of damage caused. This information is crucial for understanding the attack landscape and devising effective countermeasures.
3. Assessing the Scope of a Breach: Logs provide critical insights into the scope and impact of a security breach. By examining logs from different systems or devices, analysts can identify the systems compromised, data accessed or exfiltrated, and the duration of the breach. This helps in assessing the severity of the incident, prioritizing response efforts, and containing further damage.
4. Gathering Evidence for Investigation and Legal Proceedings: Logs serve as a valuable source of evidence during investigations and legal proceedings. They provide a chronological record of events and actions taken within the information system, enabling analysts to reconstruct the incident timeline and identify

key actors. Log analysis can assist in building a case, supporting legal actions, and facilitating compliance with regulatory requirements.

6. SOC

SOC stands for Security Operations Center. It is a centralized unit within an organization responsible for monitoring, detecting, analyzing, and responding to security incidents and threats. A SOC is designed to provide continuous monitoring and protection of an organization's information systems, networks, applications, and data. It typically employs a combination of technologies, processes, and skilled cybersecurity professionals to ensure the organization's security posture is maintained and threats are promptly addressed. The SOC's primary goal is to enhance an organization's ability to identify, mitigate, and recover from security breaches and incidents.

There are standards related to live logs for SOCs. For instance, in the book '11 Strategies of a World-Class Cybersecurity Operations Center' published by MITRE, it is stated that logs should be retained for a period ranging from 6 months to 2 years depending on the type of logs (such as Firewall logs, for example) (MITRE. “11 Strategies of a World-Class Cybersecurity Operations Center”, 2022).

7. Correlation

Effective correlation is a crucial aspect of SIEM solutions. Numerous regulations worldwide emphasize real-time correlation as a means of identifying and responding to security threats promptly (The Monetary Authority of Singapore (MAS). 2021, Australian Cyber Security Center. 2021, NIST. “NIST Cybersecurity Framework 2.0” 2023). Correlation capabilities enable the identification of patterns and anomalies across diverse data sources, enhancing an organization's ability to detect and mitigate potential security breaches.

The future of SIEM and SOC services lies in the integration of artificial intelligence (AI) and automation. AI-driven anomaly detection and predictive analytics enable the identification of sophisticated threats that evade traditional security measures. Machine learning models can learn from historical data and adapt to evolving threat landscapes. Additionally, integrating threat intelligence feeds and collaborating with external cybersecurity communities strengthen an organization's ability to identify emerging threats quickly.

Moreover, the process of correlating data across diverse sources poses an enigmatic challenge. SIEM solutions rely on the accurate correlation of events to identify patterns and indicators of potential breaches. Yet, as logs pour in from different devices, platforms, and applications, deciphering meaningful connections becomes a complex puzzle. Incorrect or incomplete correlations can lead to missed threats or false alarms, both of which can significantly impact an organization's ability to respond effectively.

7.1 Real Time Correlation

In today’s complex and ever-evolving cybersecurity landscape, organizations face a myriad of sophisticated threats that can cause significant damage if left undetected. Real time correlation is the critical requirements for regulations (The Monetary Authority of Singapore (MAS). 2021, Australian Cyber Security Center. 2021, NIST. “NIST Cybersecurity Framework 2.0” 2023).

In this context, real-time correlation is of paramount importance for several reasons:

- Timely Threat Identification: The speed at which security incidents are identified and responded to is crucial in mitigating potential damage. Real-time detection in SIEM/UEBA solutions allows security teams to receive alerts as soon as suspicious activities are detected. This rapid identification gives organizations a crucial advantage in thwarting attacks before they can escalate and cause harm.
- Reduced Dwell Time: Dwell time, the period between a security breach and its discovery, is a critical metric in cybersecurity. Real-time detection helps reduce dwell time by quickly spotting malicious activities, preventing attackers from establishing a persistent presence within the network. Minimizing dwell time limits the damage attackers can inflict and shortens the window of opportunity for exfiltrating sensitive data.
- Automated Response: Integrating real-time detection with automated response capabilities enables organizations to respond rapidly to security incidents. Automated actions, such as blocking malicious IPs, quarantining compromised systems, and initiating predefined incident response playbooks, ensure that threats are contained promptly, even when security teams are not immediately available.

- Correlation of Events: The true value of SIEM/UEBA solutions lies in their ability to correlate seemingly unrelated security events in real-time. This correlation identifies patterns, trends, and relationships between different activities that could indicate a coordinated attack or unusual user behavior. By connecting the dots, security analysts gain valuable insights into the attack's nature and can respond more effectively.
- Advanced Threat Detection: Advanced threats, including APTs (Advanced Persistent Threats), often involve multiple stages and tactics spread across the network. Real-time detection and correlation can piece together disparate events, even those occurring in different parts of the network, to uncover these sophisticated attack campaigns. This holistic view is essential for understanding the full scope of the threat.
- Insider Threat Detection: Insider threats, whether malicious or unintentional, pose significant risks to organizations. UEBA solutions play a vital role in detecting anomalous user behavior that might indicate insider threats. Real-time analysis of user actions, such as accessing sensitive data outside regular working hours or attempting unauthorized activities, allows organizations to respond swiftly and prevent data breaches.
- Compliance and Reporting: Meeting regulatory compliance requirements demands timely detection and response to security incidents. Real-time detection and correlation ensure that organizations can demonstrate their adherence to compliance standards by promptly reporting incidents and maintaining accurate audit trails.
- Proactive Incident Response: Real-time detection allows organizations to adopt a proactive approach to incident response. By identifying potential threats early, organizations can take preemptive actions to prevent attacks, strengthen security controls, and bolster their overall security posture.
- Adaptive Security Measures: Real-time detection and correlation enable organizations to dynamically adjust their security measures based on emerging threats and attack vectors. This adaptability ensures that security protocols remain effective and relevant in an ever-changing threat landscape.

Real-time correlation is not supported or is limited in some cases. When Splunk is deployed in cloud environments, it disables real-time searching and correlation. In on-premises installations, it also dedicates a core for each real-time monitoring task, which translates into substantial CPU costs (Splunk. Splunk Community, 2019, Splunk. Splunk Community, 2016, Splunk. Splunk Community, 2021, Splunk. Splunk Community, 2018).

Even Microsoft Sentinel, a powerful player in the security information and event management arena, has its own set of constraints. It imposes a limit of 50 rules for a tenant when it comes to real-time correlation (Microsoft. Microsoft Community, 2023).

8. Discussion

SIEM solutions are essential in the realm of cybersecurity, serving as robust guardians in an increasingly digital landscape where threats are omnipresent. The Security Operations Center (SOC) framework, fundamental to modern cybersecurity, involves procuring vital services with SIEM systems at the forefront. Whether through in-house teams or external outsourcing, the commitment to rigorous and detailed cybersecurity practices is essential.

Central to these practices is effective log management, which acts as the digital memory of an organization's activities. The criticality of real-time log monitoring is akin to monitoring the vital signs of an organization's network and systems, providing essential visibility and control.

A crucial element in enhancing these practices is the introduction of the Event Volume Score (EVS), a new metric developed to quantitatively assess and improve logging practices. EVS focuses on evaluating the frequency, variety, and detail of log entries, thereby ensuring that logging practices are robust enough to handle complex security demands. This metric is pivotal in maintaining the integrity and continuity of logs, which should be active for at least a year and archived for an additional 1.5 years to support forensic investigations and compliance.

The journey up the correlation pyramid is also vital, with each level representing a deeper and more sophisticated understanding of threat detection through the integration of disparate data points. Achieving higher levels of this pyramid indicates a mature capability to decipher and address the complex relationships between varied cybersecurity events.

Ignoring these enhanced practices can have severe implications, as demonstrated by significant breaches like the SolarWinds and Stuxnet incidents. These events underscore the risks of inadequate cybersecurity measures and highlight the necessity of stringent log management and effective correlation practices.

Our discussion extends to include recognized risk lists from sources such as OWASP and MITRE, aligning our practices with industry standards to underscore the universality of these challenges. Furthermore, we delve into the legal and regulatory frameworks governing global data protection, illustrating that cybersecurity risks encompass more than just technical challenges; they have broad implications across legislative and regulatory environments.

At this critical juncture, as organizations select products and services to strengthen their defenses, our mission is twofold: to expose potential vulnerabilities that could lead to cyber threats and to provide clarity and insights, guiding end-users to make informed decisions that fortify their digital infrastructures against the dynamic spectrum of cybersecurity risks. This comprehensive approach ensures that organizations not only understand the risks but also have the tools and knowledge to mitigate them effectively.

9. Conclusion

In conclusion, the risks inherent in deploying Security Information and Event Management (SIEM) systems and acquiring Security Operations Center (SOC) services are complex and constantly changing. As organizations work to strengthen their cybersecurity measures, it is crucial to navigate the myriad challenges posed by evolving laws, regulations, standards, and best practices.

This paper introduces a novel approach by not only scrutinizing the criteria for SIEM and SOC systems but also incorporating perspectives from esteemed entities such as OWASP, MITRE, the White House, and SANS, along with introducing the Event Volume Score (EVS) as a new metric to assess these systems. This holistic evaluation provides a detailed view of the effectiveness and relevance of SIEM and SOC solutions within the larger cybersecurity framework.

The findings from this research highlight the importance for organizations to continuously refine and adjust their cybersecurity strategies to keep pace with the dynamic security landscape. As threats evolve, so must the methods and approaches to managing SIEM and SOC systems to effectively safeguard critical assets. In such a rapidly shifting environment, it is imperative for organizations to remain vigilant and proactive, ensuring their cybersecurity defenses are both resilient and adaptive.

References

Australian Cyber Security Center. 2021. “Australian Government Information Security Manual”, [online] https://kmtech.com.au/wp-content/uploads/2021/11/Australian-Government-Information-Security-Manual-September-2021.pdf [Accessed: 18th Aug 2023]

2021.“Event Logging Guidance from Treasury Board of Canada Secretariat”, [online] https://www.canada.ca/en/government/system/digital-government/online-security-privacy/event-logging-guidance.html [Accessed: 1st May 2023]

Gartner. 2023. “6 Macro Factors Reshaping Business This Decade”, [online] https://www.gartner.com/en/articles/6-macro-factors-reshaping-business-this-decade [Accessed: 2nd May 2023]

Granadillo,G. and González-Zarzosa,S. and Diaz,R. 2021 “Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures”, Sensors, vol 21(14), 4759. [online] http://dx.doi.org/10.3390/s21144759 [Accessed: 3rd May 2023]

Google.”Retaining Logs for A Year: Boring or Useful?”, 2019. [online] https://chroniclesec.medium.com/retaining-logs-for-a-year-boring-or-useful-9b04c1e55fba [Accessed: 2nd Aug 2023]

InfoTech. 2021. [online] http://www.infotech.com [Accessed: 6th May 2023]

Info-Tech Research Group. 2015. “Vendor Landscape: Security Information & Event Management. In Optimize IT Security Management and Simplify Compliance with SIEM Tools” [online] https://infotech.report/Resources/Whitepapers/4d60fcda-43d8-410a-bb83-e737f828d078_SIEM%20Tools%20to%20Optimize%20IT%20Security.pdf [Accessed: 8th May 2023]

2021.“MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES”,[online] https://www.whitehouse.gov/wp-content/uploads/2021/08/M-21-31-Improving-the-Federal-Governments-Investigative-and-Remediation-Capabilities-Related-to-Cybersecurity-Incidents.pdf [Accessed: 6th Aug 2023]

Microsoft. Microsoft Community, 2023. [online] https://docs.microsoft.com/en-us/azure/sentinel/near-real-time-rules [Accessed: 7th Aug 2023]

MITRE. “Common Weakness Enumeration: CWE”, 2019. [online] https://cwe.mitre.org/data/definitions/1210.html [Accessed: 9th Aug 2023]
MITRE. “Common Weakness Enumeration: CWE”, 2009. https://cwe.mitre.org/data/definitions/778.html [Accessed: 9th Aug 2023]
MITRE. “11 Strategies of a World-Class Cybersecurity Operations Center”, 2022. [online] https://www.mitre.org/sites/default/files/2022-04/11-strategies-of-a-world-class-cybersecurity-operations-center.pdf [Accessed: 10th Aug 2023]
NIST. “NIST Cybersecurity Framework 2.0” 2023. [online] https://www.nist.gov/cyberframework [Accessed: 12th Aug 2023]
NIST. “Assessing Security and Privacy Controls in Information Systems and Organizations” 2022. [online] https://csrc.nist.gov/pubs/sp/800/53/a/r5/final [Accessed: 14th Aug 2023]
OWASP. “Top 10 Web Application Security Risks”, 2021. [online] https://owasp.org/www-project-top-ten [Accessed: 15th Aug 2023]
OWASP. “OWASP Top 10 API Security Risks – 2019”, 2019. [online] https://owasp.org/API-Security/editions/2019/en/0x11-t10 [Accessed: 16th Aug 2023]
OWASP. “OWASP Top Ten 2017”, 2017. [online] https://owasp.org/www-project-top-ten/2017/A10_2017-Insufficient_Logging%2526Monitoring [Accessed: 17th Aug 2023]
SANS. “An Evaluator's Guide to NextGen SIEM”, 2018. [online] https://www.sans.org/media/vendor/evaluator-039-s-guide-nextgen-siem-38720.pdf [Accessed: 18th Aug 2023]
Sheeraz,M. et al 2018. “Effective Security Monitoring Using Efficient SIEM Architecture”, Human-centric Computing and Information Sciences, vol 8, [online] https://doi.org/10.22967/HCIS.2023.13.017 [Accessed: 18th Aug 2023]
Solutions Review . “Security Information and Event Management Vendor Map”,[online] https://solutionsreview.com/security-information-event-management/security-information-event-management-vendor-map [Accessed: 19th Aug 2023]
Splunk. Splunk Community, 2019. [online] https://community.splunk.com/t5/Splunk-Search/Real-Time-Search-Issues/m-p/423805 [Accessed: 20th Aug 2023]
Splunk. Splunk Community, 2016. [online] https://answers.splunk.com/answers/433872/why-are-real-time-searches-not-running-and-getting.html [Accessed: 21st Aug 2023]
Splunk. Splunk Community, 2021. [online] https://docs.splunk.com/Documentation/Splunk/latest/Search/Realtimeperformanceandlimitations [Accessed: 22nd Aug 2023]
Splunk. Splunk Community, 2018. [online] https://answers.splunk.com/answers/671819/real-time-alert-1.html [Accessed: 23rd Aug 2023]
TechTarget. TechTarget Search Security. [online] http://searchsecurity.techtarget.com [Accessed: 24th Aug 2023]
TechTarget. 2013. “How to Define SIEM Strategy, Management and Success in the Enterprise”, [online] https://searchsecurity.techtarget.com/essentialguide/How-to-define-SIEM-strategy-management-and-success-in-the-enterprise [Accessed: 25th Aug 2023]
The Monetary Authority of Singapore (MAS). 2021. “Guidelines on Risk Management Practices – Technology Risk”, [online] https://www.mas.gov.sg/regulation/guidelines/technology-risk-management-guidelines [Accessed: 26th Aug 2023]
“Vadodara Smart City Development Limited (VSCDL)”,2021. [online] http://vadodarasmartcity.in/vscdl/assets/tenders/17.09.2020/2021_499-1.pdf [Accessed: 2thth Aug 2023]
VirginiTech.“Benchmarking Security Information Event Management (SIEM)”, [online] https://apps.es.vt.edu/confluence/download/attachments/460849213/sans%20siem%20benchmarking.pdf [Accessed: 27th Aug 2023]