EXPLORING CRITICAL VULNERABILITIES IN SIEM IMPLEMENTATION AND SOC SERVICE PROCUREMENT: AN IN-DEPTH ANALYSIS OF HIGH-RISK SCENARIOS

Ertuğrul AKBAŞ

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

ABSTRACT

This research paper examines the high risks encountered while using a Security Information and Event Management (SIEM) product or acquiring Security Operations Center (SOC) services. The paper focuses on key challenges such as insufficient logging, the importance of live log retentions, scalability concerns, and the critical aspect of correlation within SIEM. It also emphasizes the significance of compliance with various standards and regulations, as well as industry best practices for effective cybersecurity incident detection, response, and management.

KEYWORDS

SIEM, Security, SOC, Cyber Security, Insufficient logging, Live Log, Hot Log, Log Loss, Correlation

1. INTRODUCTION

SIEM solutions and SOC services stand as foundational pillars in the ever-evolving landscape of modern cybersecurity. These components play a pivotal role in protecting organizations from an increasingly sophisticated array of cyber threats. However, the effectiveness of these vital tools can be undermined by an array of challenges that span from log manage- ment intricacies to the complexities of data correlation. This paper delves deeply into the intricacies of these challenges, dissecting the inherent risks they pose and shedding light on how they can potentially erode an organization's overall security posture.

While there exists a wealth of research analyzing SIEM products and SOC services, this paper takes a novel approach to analyze. We depart from traditional methodologies and instead focus on evaluating these security measures in alignment with legal requirements, governmental orders, industry regulations, and best practices.

In this endeavor, we aim to shed light on the crucial intersection of cybersecurity and compliance. By assessing SIEM and SOC effectiveness through the lens of applicable laws, orders, regulations, and industry benchmarks, we seek to provide a comprehensive understanding of how organizations can not only bolster their security posture but also ensure conformity with the ever-evolving landscape of cybersecurity laws, governmental orders, regulations, standards and obligations.

Our analysis is based on White House orders, OWASP, MITRE, and SANS, which makes our evaluation a novel methodology. Our analysis builds upon the foundation laid by these authoritative sources, weaving together insights, methodologies, and best practices into a

DOI: 10.5121/ijnsa.2023.15601

coherent evaluation framework. By doing so, we aim to provide a holistic and rigorous approach to assessing cybersecurity measures, whether within governmental institutions, corporations, or individual systems.

2. CURRENT METHODOLOGIES IN EVALUATING SIEM SOLUTIONS

Many features within the realm of SIEM solutions are commonly available and fulfilled by a significant portion of the offerings.

Fundamentally, all SIEMs have the capacity to collect, store, and correlate events generated by a managed infrastructure [1]. Besides these key capacities, they listed the features as:

- Correlation rules
- Data sources
- Real time processing
- Data volume
- Visualization
- Data analytics
- Performance
- Forensics
- Complexity
- Scalability
- Risk analysis
- Storage
- Price
- Resilience
- Reaction and reporting capabilities
- UEBA
- Security

They also presented a comparison table and this table depicted at table 1.

Table 1. Analysis of different SIEM solutions [2]

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.

Another comparison table depicted by Muhammad Sheeraz et al. [2]. They used a different feature set to compare products. Their features are:

- Real-time monitoring,
- Threat intelligence,
- Behavior profiling,
- data and user monitoring,
- Application monitoring,
- Analytics,
- Log management,
- Updates,
- Reporting,
- Graphical user interface (GUI),
- Detailed system description,
- Database

Table 2. Analysis of different SIEM solutions [1]

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.

The problem here is that there are numerous SIEM comparison reports [3, 4, 5, 6, 7, 8] and research articles [1, 2], but there has been no evaluation in terms of laws, government orders, regulations, and standards. Apart from previous research and reports, we will analyze how SIEM solutions align with the White House order, OWASP, MITRE, and SANS.

3. INSUFFICIENT LOGGING

Hackers leverage gaps in logging and monitoring by relying on the fact that security teams will take time to detect and remediate the attack to try and escalate privileges.

This section explores the threats associated with insufficient logging & monitoring and the business impacts of a successful attack.

A SIEM solution should primarily collect logs without missing any and should ensure complete data capture. Despite the existence of a reference table published by SANS a decade ago [9] and EPS calculation table depicted in Figure 1, you might encounter significant disparities in the EPS values (log collection rates per second) among different SIEM products in the market and in practice, even when using the same network, same log sources, same number of log sources, and the same company.

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 [10], OWASP Top 10 API Security Risks – 2019 [11], OWASP Top 10 Application Security Risks – 2017 [12].

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 [15].

Across the globe, a multitude of standards, laws, and illustrative best-case scenarios concerning the vital role of live logs have been disseminated [16,17,18,19,20]. 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.

- 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.

- 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.

- 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.

- 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 [21].

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) [22].

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 [23,24,25]. 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. Detection, Regulations and 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. In order to detect cyber-attacks, correlation plays a critical role. Correlation can be delayed or real-time based. Real-time correlation is also one of the critical requirements for regulations [23,24,25]. While delayed correlation or detection is useful, real-time correlation is superior not only in detection but also in meeting regulatory requirements.

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 [26, 27, 28, 29].

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 [30].

8. DISCUSSION

SIEM solutions play an irreplaceable and pivotal role in the realm of cybersecurity. In an increasingly digitized landscape, where threats lurk around every corner of the virtual world, these solutions stand as guardians of digital fortresses. The Security Operations Center (SOC) framework, a cornerstone of modern cybersecurity, encompasses the procurement of vital cybersecurity services, with SIEM standing tall among them. This acquisition can take the form of harnessing the expertise of in-house cybersecurity teams or entrusting the task to external experts through outsourcing. Regardless of the chosen path, what remains non-negotiable is a methodical and meticulous approach to certain core areas.

Central to this approach is an unwavering focus on effective log management, which serves as the digital memory bank of an organization's activities. The value of real-time log monitoring cannot be overstated, akin to having a watchful eye on the heartbeat of an organization's network and systems. The art of correlation, weaving together seemingly disparate pieces of information to unveil patterns and anomalies, is the very essence of modern threat detection and prevention.

Within the realm of these practices lie critical aspects that demand special attention. Preventing the loss of logs, or the risk of insufficient logging, is akin to safeguarding an organization's history. Logs, those time-stamped records of events, hold the clues to untangling complex cyber incidents. Ensuring their continuity for at least a year in an active state, followed by an archival period of 1.5 years, is the equivalent of maintaining an extended digital memory—a practice that can be instrumental in forensic investigations and compliance adherence.

Equally important is the journey up the correlation pyramid. This hierarchical structure, discussed within the context of this article, signifies the progressive levels of sophistication in threat detection. Reaching at least level 3 of this pyramid denotes a mature and comprehensive approach to understanding and addressing the intricate relationships between various cybersecurity events.

The implications of overlooking these practices are grave. Notable cyber incidents like the SolarWinds breach, the infamous Stuxnet Worm Attack, the 2017 Verizon Communications Data Breach, and the 2019 Dominion National Data Breach stand as stark reminders of the risks that materialize in the absence of stringent cybersecurity practices.

To further illuminate the importance of these practices, we extended our reach by referencing established risk lists from reputable sources such as OWASP and MITRE. This alignment with industry-recognized risks lends credibility to our approach and emphasizes the universality of the challenges we address.

Moreover, our exploration delved into the legal and regulatory frameworks that encompass global data protection standards. By doing so, we presented a comprehensive picture of how cybersecurity risks are not just technical hurdles, but issues that reverberate throughout the world's legislative and regulatory corridors. Here, we suggest executing an algorithm to select the right solution.

Decision Algorithm:

1. Calculate EPS values according to Figure 1.
2. After obtaining the EPS value, ask, 'What is the required disk size for 1 year hot and 1.5 years archive logs?'
3. Ask if the archive disk will be a cheap disk or not?
4. Test the real-time correlation feature:
    a. Create a login event and check if the related alarm comes immediately.
    b. Test the use case 'User Deleted Within 24hrs of Being Created' and see if the related alarm is triggered immediately.
5. Make a decision based on costs and the required support for log retention and real-time correlation requirements.

At this decisive juncture, when organizations are confronted with selecting products and services to bolster their defenses, our mission was twofold. First, it was to lay bare the vulnerabilities that could potentially expose them to cyber threats. Second, it was to cast a beacon of understanding and insight, illuminating the path for end-users to make informed decisions that would fortify their digital landscapes against the ever-evolving panorama of cybersecurity risks.

9. CONCLUSION

In conclusion, it is evident that the risks associated with the usage of Security Information and Event Management (SIEM) products and the acquisition of Security Operations Center (SOC) services are multifaceted and continually evolving. As organizations strive to enhance their cybersecurity posture, it becomes increasingly critical to address the challenges posed by laws, regulations, standards, and best practices.

This paper has taken a novel approach by not only analyzing SIEM and SOC criteria but also evaluating them through the lenses of respected organizations such as OWASP [1,2,3,4], MITRE [5,6], the White House [7], and SANS [1]. By considering these perspectives, we have provided a comprehensive view of the effectiveness and relevance of SIEM and SOC solutions in the broader context of cybersecurity.

The insights gained from this analysis underscore the need for organizations to continually adapt and align their cybersecurity strategies with the evolving landscape of security standards and regulations. As the threat landscape evolves, so too must our approaches to SIEM and SOC services to effectively mitigate risks and protect critical assets. In this dynamic environment, staying informed and agile is paramount for maintaining robust cybersecurity defenses.

REFERENCES

[1] Gustavo Gonzalez Granadillo, Susana González-Zarzosa, Rodrigo Diaz, Rodrigo.2021.Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. Sensors. vol. 21(14), 4759. http://dx.doi.org/10.3390/s21144759

[2] Muhammad Sheeraz, Muhammad Arsalan Paracha, Mansoor Ul Haque, Muhammad Hanif Durad, Syed Muhammad Mohsin, Shahab S. Band, and Amir Mosavi,2018, Effective Security Monitoring Using Efficient SIEM Architecture, Human-centric Computing and Information Sciences, vol. 8. https://doi.org/10.22967/HCIS.2023.13.017

[3] Gartner.: 7 Macro Factors that will Shape the 2020s. Retrieved May 31, 2023 from https://www.gartner.com/en

[4] TechTarget. TechTarget Search Security.Retrieved May 31, 2023 from http://searchsecurity.techtarget.com/

[5] InfoTech. Info-Tech Research Group. Retrieved May 31, 2023 from http://www.infotech.com/

[6] TechTarget, Search Security. How to Define SIEM Strategy, Management and Success in the Enterprise. Technical Guide. Retrieved Aug 13, 2023 from https://searchsecurity.techtarget.com/essentialguide/How-to-define-SIEM-strategy-management-and-success-in-the-enterprise

[7] Info-Tech Research Group. 2015. Vendor Landscape: Security Information & Event Management. In Optimize IT Security Management and Simplify Compliance with SIEM Tools

[8] Solutions Review. Security Information and Event Management Vendor Map. Retrieved Aug 14, 2023 from https://solutionsreview.com/security-information-event-management/security-information-event-management-vendor-map/

[9] Benchmarking Security Information Event Management (SIEM). Retrieved Aug 14, 2023 from https://apps.es.vt.edu/confluence/download/attachments/460849213/sans%20siem%20benchmarking.pdf

[10] Top 10 Web Application Security Risks. Retrieved Aug 14, 2023 from https://owasp.org/www-project-top-ten/

[11] OWASP Top 10 API Security Risks – 2019.Retrieved Aug 14, 2023 from https://owasp.org/API-Security/editions/2019/en/0x11-t10/

[12] OWASP Top Ten 2017. Retrieved Aug 14, 2023 from https://owasp.org/www-project-top-ten/2017/A10_2017-Insufficient_Logging%2526Monitoring

[13] Common Weakness Enumeration: CWE. Retrieved Aug 14, 2023 from https://cwe.mitre.org/data/definitions/1210.html

[14] Common Weakness Enumeration: CWE. Retrieved Aug 14, 2023 from

https://cwe.mitre.org/data/definitions/778.html
[15] MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES. Retrieved Aug 14, 2023 from 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
[16] Event Logging Guidance from Treasury Board of Canada Secretariat. Retrieved Aug 14, 2023 from https://www.canada.ca/en/government/system/digital-government/online-security-privacy/event-logging-guidance.html
[17] Google. Retaining Logs for A Year: Boring or Useful? Retrieved Aug 14, 2023 from https://chroniclesec.medium.com/retaining-logs-for-a-year-boring-or-useful-9b04c1e55fba
[18] An Evaluator's Guide to NextGen SIEM. Retrieved Aug 14, 2023 from https://www.sans.org/media/vendor/evaluator-039-s-guide-nextgen-siem-38720.pdf
[19] NIST, Assessing Security and Privacy Controls in Information Systems and Organizations. Retrieved Aug 14, 2023 from https://csrc.nist.gov/pubs/sp/800/53/a/r5/final
[20] Vadodara Smart City Development Limited (VSCDL). Retrieved Aug 14, 2023 from http://vadodarasmartcity.in/vscdl/assets/tenders/17.09.2020/2021_499-1.pdf
[21] Ertuğrul Akbaş, Log Investigation: An Indispensable and Crucial Part of Incident Response. Retrieved Aug 14, 2023 from https://medium.com/@drertugrulakbas/log-investigation-an-indispensable-and-crucial-part-of-incident-response-1cff4046ffeb
[22] 11 Strategies of a World-Class Cybersecurity Operations Center. Retrieved Aug 16, 2023 from https://www.mitre.org/sites/default/files/2022-04/11-strategies-of-a-world-class-cybersecurity-operations-center.pdf
[23] Guidelines on Risk Management Practices – Technology Risk. Retrieved Aug 16, 2023 from https://www.mas.gov.sg/regulation/guidelines/technology-risk-management-guidelines
[24] Australian Government Information Security Manual. Retrieved Aug 16, 2023 from https://kmtech.com.au/wp-content/uploads/2021/11/Australian-Government-Information-Security-Manual-September-2021.pdf
[25] NIST Cybersecurity Framework 2.0.Retrieved Aug 21, 2023 from https://www.nist.gov/cyberframework
[26] Splunk Community, Retrieved Aug 21. 2023 from https://community.splunk.com/t5/Splunk-Search/Real-Time-Search-Issues/m-p/423805
[27] Splunk Community, Retrieved Aug 21. 2023 from https://answers.splunk.com/answers/433872/why-are-real-time-searches-not-running-and-getting.html
[28] Splunk Community. Retrieved Aug 21, 2023 from https://docs.splunk.com/Documentation/Splunk/latest/Search/Realtimeperformanceandlimitations
[29] Splunk Community. Retrieved Aug 25, 2023 from https://answers.splunk.com/answers/671819/real-time-alert-1.html
[30] Microsoft Community. Retrieved Aug 25, 2023 from https://docs.microsoft.com/en-us/azure/sentinel/near-real-time-rules

AUTHOR

DR. ERTUĞRUL AKBAŞ. I am an experienced professional in research and development, and I have a career that brings together industry and academia. I hold a doctoral degree in computer engineering, and I also have two master's degrees, one in computer engineering and one in control engineering.

I began my career as a researcher at TÜBİTAK, Turkey's leading R&D institution, and quickly became the youngest project manager in the institution's history. TÜBİTAK is the equivalent governmental agency to the National Science Foundation (NSF) and government research centers in the United States. Since then, I have continued my professional journey successfully by establishing my own companies. Additionally, I am actively engaged in academic work at Istanbul Esenyurt University.

I have implemented numerous successful projects both in Turkey and worldwide. These projects range from research budget-supported projects for major organizations like Türk Telekom to projects that received reference letters from industry leaders such as Honda.

I have furthered my business journey by establishing four different companies. I founded my first company, which executed high-profile projects featured in leading Turkish newspapers. Within this company, I also technically managed R&D projects supported by TÜBİTAK.

Another company I established was acquired by TEI, one of Turkey's leading aviation companies. Subsequently, my third company, named Hakem Bilişim, evolved into ANET. As ANET Software, we have executed cybersecurity projects for hundreds of companies worldwide, including Honda, Hugo Boss, FujiFilm, TÜBİTAK, Türk Telekom, British American Tobacco, Credit Suisse, Boehringer Ingelheim, ETS Tur, and Oyak Yatırım. Our SureLog SIEM product is listed on Gartner Peer Insight.

I have made a significant impact in the academic field as well. My articles have been recognized as references worldwide, from the United States to Finland. They have been used as references in patents, doctoral theses, and academic research. Additionally, I have served as a reviewer for over 20 international academic journals and conferences.