# Study of challenges faced by Enterprises using Security Information and Event Management (SIEM)

Mukesh Yadav[1*], Dhirendra S Mishra[2]
[1]Research Scholar, [2]Professor
Department of Computer Engineering
SVKM's NMIMS Deemed to be University,
Mukesh Patel School Of Technology Management & Engineering, Mumbai
[1]yadav92mukesh@gmail.com, [2]dhirendra.mishra@nmims.edu

***Abstract*:** The field of information security plays an important role in education, IT, health domain, etc. Much research has been carried out in order to secure data in hardware, on the cloud, and during transmission over the network. A secure data transmission and securing the stored data is still taken as one of the concerned areas. Cloud-based SIEM is used nowadays, which is the art and science to secure the information of the organization. SIEM is Security Information and Event Management, which means securing the organization containing network devices and devices holding critical and sensitive information. In this paper, a survey is carried out to determine the gap in current security providers and areas that need attention. We take logs as input and send them to SIEM for analysis. Whether a SIEM is capable enough to determine the unknown threats and user behavior to identify insider threats. Also, terms such as EPS, False positive Rate, Mean Time to Resolution are used as compassion and aim to keep False positive rate and mean time resolution value low and EPS no restriction.

***Keywords:*** Cyber Security, SIEM, SIM, SEM, UEBA, SOAR, SOC, EPS, MTTR, Big Data Analytics, Cloud Storage, On-prem, Threat Detection, Event Management, Security Information, Outlier Detection, Information Management, Advanced Threats, Incident, Anomaly Behaviour.

## 1. INTRODUCTION

Security Information and Event Management (SIEM) systems have become today an essential component of all enterprise networks. SIEM's are capable of real-time monitoring of the network at all times to detect and alert in case it identifies an incident and a critical security issue. The main roles of the SIEM solution in an organization's network are to monitor the log data, collect and store it in a central console. The next step involves analyzing the log data, filtering alerts, and building correlation rules. [21] A flow diagram of data flow in SIEM is given in Figure. 1.

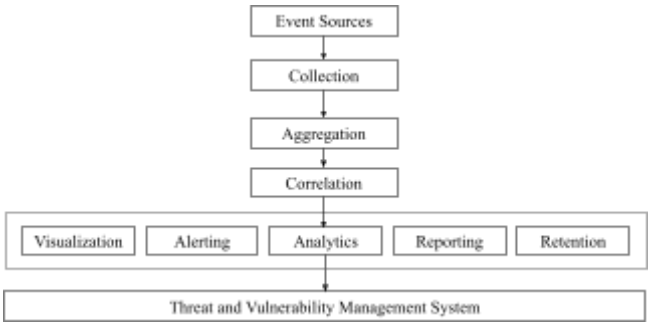


**Figure 1. SIEM data pipeline [22]**

Figure 1 describes the data flow pipeline through various blocks. The first block, event sources, are the devices that generate logs. The second block, data collection, takes place at the SIEM's specific listener port number and the IP address. The third block, data aggregation, segregates all the logs collected and stores them in a properly structured format. The fourth block, data correlation, where the comparison between the different device logs takes place and inference is obtained, which decides what security action needs to be taken. The fifth block, where visualization of logs in the form of monitoring graphs takes place, analytics to find out the threats in the network, alerting the security team, documenting the threats in the form of reports, and keeping the logs for a specific duration called as retention period of the logs, takes place in this section. The last block, threat and vulnerability management system, is used to perform all the management activities like, manage the resources, manage users, manage configurations, and response actions on a specific incident.

Confidentiality ensures that the information can be accessed by the authorized users; integrity provides the accuracy and complete information, and availability provides access to authorized users when required. A threat is a circumstance or event with the potential to adversely impact organizational operations (e.g., mission, functions, reputation), as well as organizational assets, individuals, other organizations, or even the Nation through unauthorized access, destruction, disclosure, modification of information, and/or denial of service. A vulnerability is a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source. A risk is the level of impact on organizational operations, assets, or individuals resulting from tampering with the operation of the information system. The notion of risk covers two aspects: the potential impact of a threat and the likelihood of such a threat occurring. [23]

An attack is an instance or the realization of a potential threat. An attack is denied as the attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise the integrity of a system. The Attack Surface refers to the subset of resources used to attack a system (i.e. methods such as Read, Write, Print, etc.; channels such as TCP, UDP, etc. The Attack Surface Area refers to the system's total surface exposed to a given attack. This surface includes tangible assets (e.g. desktop, mobile phones, network devices, etc.), other assets like confidential information, business reputation, etc. [24]

To mitigate the effects of a given attack, one needs to implement security measures. Countermeasures are security actions required to oppose an attack, either by eliminating or preventing it, by minimizing the harm it can cause or by discovering and reporting it so that corrective action can be taken. Combined countermeasures result from the simultaneous implementation of two or more countermeasures to mitigate a given attack. A combined countermeasure is therefore analyzed as a single solution with a combined cost and combined effectiveness. [25]

In this research, we assume that the implementation of a countermeasure always results in a security policy. A Security Policy defines and constrains the activities of components processing data to maintain security properties for systems and data. Security policies are enforced by Policy Enforcement Points (PEP) which is a logical entity or place on a server that enforces policies for admission control and decisions in response to a request from a user wanting to access a resource or a service on a computer or network server.[24]

A SIEM detects all log sources like application logs, system logs, device logs, Vulnerability scanning tool logs, Deception technology logs, Intrusion detection, and prevention system logs in a network. SIEM collects the log data in a secured channel. To have a secure chain of custody, the logging data process must be automated, consistent,

and apparent. For example, to collect log data from sources over UDP, the collection device preferably has to be located near the source to mitigate the risk of data being lost. This can be possible by reducing the number of packet hops to zero that need travel before reaching their destination. Often, SIEM systems collect large volumes of log data. Thus, the system should be capable of collecting this data without getting overwhelmed. A common construction approach for a SIEM system is the hierarchical approach that enables the system to collect log data at multiple levels. In other words, the system is designed in a way that an agent is deployed in different location levels. These agents communicate back to the SIEMs central management console in charge of data storage and analysis. The process generally does not affect the network performance. Traditionally, the SIEM system focused more on collecting device or structure-related log data and events. For instance, the traditional SIEM implementation required that the operating systems running on both the servers and end-user devices send log data such as log-in events, antivirus application alerts, and communication subsystem information. Logs from the operating system can be successful or unsuccessful logins, admin login, IAM events, and other events. Logs can be from antivirus events like scan results, and infected file details. Network logs like blocked, successful port connections, port connections requests, and network IP details from network devices such as routers, intrusion detection, and prevention systems, firewalls, etc.

The log data collected from different sources is stored in their raw and enriched format in CSV, TXT, a JSON format for a long period. Storing the log data in its raw format optimizes the time taken to access the data in the future. Ultimately, the most critical function of a SIEM application is the analysis of the log data. The SIEM system is required to look into the different logs stored and notify the user about the network environment based on the information insights deducted from the log data. An ideal SIEM solution can correlate both the new data and data that is similar to another set of logs that the system had collected previously.

These SIEMs are implemented in a variety of contexts – from large-scale enterprises with multiple security domains to administering industrial control systems for critical infrastructure – however one context of particular interest is that of the small and medium-sized enterprise (SMEs).[26]

When attackers compromise the perimeter or are operating from within, you need to know. Evidence of intruders and insider threats lies within network communications. Need for detecting network, host and web based threats with real-time network monitoring is very crucial nowadays using big data analytics. As per the observation, many organizations spend a lot of money buying a SIEM product.

### 1.1 Security Operation Center (SOC)

A Security Operations Center (SOC) is a department within an organization that performs configuration management, change management of security devices like Firewalls, IDS/IPS, VPN, SIEM, AV, etc. They also perform Security Incident Response and Monitor near real-time logs with the help of SIEM tools. There may be dedicated teams within a SOC with different reporting hierarchies for Device Management and Monitoring to avoid conflict of interest depending upon contract/ legal requirement etc.

A Security Information & Event Management (SIEM) tool is simply a correlation tool through which SOC monitors the near real-time logs. It logs (if working properly) qualified events and alerts whenever there is an incident. It may also create tickets in the local ticketing tool and send email/ SMS alerts when integrated with other tools. You can tweak the tool as per your requirement.

Security Information and Event Management (SIEM) is about looking at your network through a larger lens than can be provided by a single security control or information source.

### 1.2 What is required in Traditional SIEM?

Current SIEM systems select and deploy security measures without performing a comprehensive impact analysis of attacks and response scenarios.[27]

The selection of countermeasures to mitigate the effects of a given attack requires the use of cost-sensitive metrics. Denying a quantitative model that maximizes the cost-effectiveness ratio of countermeasures contributes to the selection of the appropriate alternative. There is a need for the evaluation of combined countermeasures in a scenario of multiple attacks.

The paper is organized in the following order. Section I introduces SIEM, its usages, and its importance. Section II focuses on a detailed literature survey carried out. Section III discusses the research questions, gaps, and observations. Section IV explains possible solutions for the research questions or gaps from different studies conducted. Section V concludes the findings of the study.

## 2. LITERATURE SURVEY

The current correlation capabilities of Security Information and Event Management (SIEM) are proven to be sufficient to process huge volumes of log events and store them based on the requirements of the organization. The new generation of SIEM technology named NextGen SIEM is much better and more effective as compared to the older version.

The literature review is divided among various categories of research carried out by the authors. First, about Security Information and Event Management (SIEM) tools, their importance, awareness, about big data, types of data. Second, a literature review was carried out on the live project environment at the organization's research labs. Third, the authors discussed getting logs from a specific device like an android operating system. Fourth, some authors proposed some techniques, created some models to improve the existing tools. Fifth, comparison of different SIEM systems, evaluation of a particular SIEM tool. The views, study, experiment, and thoughts on the security tool are given below.

Oskars Podzins et. al [9] discussed the topic "Why is SIEM Irreplaceable in a Secure IT Environment?" It's a very good question as apart from the endpoint security devices which make the end device like your laptop or desktop, why is there a need for a SIEM system. If looking in the domain of cybersecurity wherein IT industries an antivirus is just the smallest device to make the network secure. SIEM overcomes that biggest limitation because SIEM, coined by Gartner, is a solution that analyzes events or logs from each of the security solutions. For example, a traffic flow of a specific IP address might not mean a lot to the firewall (if this IP has not been listed in global threat exchange databases), but SIEM could combine this flaw with the fact that Active Directory Domain Controller security logs indicate this IP was used to brute force a password for several accounts. Using this information, SIEM could launch an automated remediation action of sending an instruction to the Firewall through an API to block connections from this specific IP address. The author worked with 370 windows security events using agent software. The author concluded that SIEM is one of the best investments a company can make. Even if a company has limited resources and limited staff who are talented and experienced in

cybersecurity including SIEM systems, the company should reconsider in-house SOC and instead look for an MSSP.

Similar thoughts were shared by Natalia G. Miloslavskaya et al. [10] which talked about processing huge volumes of data that come from various locations like domain controllers, proxy servers, DNS servers, information protection tools (IPTs), etc. The data and its metadata are stored in the cloud. The author explained how big data and data lake are applied in the security sector. Instead of storing the data in a traditional database like SQL, which has various limitations like getting more in-depth insight about the data. The author also mentioned how to identify the interrelation between the 3 concepts: big data, fast data, data lake, data. These huge volumes can only be handled by SIEM tools.

Sornalakshmi et al. [7] proposed a set of rules for detecting a DoS attack and mentioned that it is a SIEM tool to detect one of the most dangerous network attacks using Denial of Service (DoS) by using only log monitoring from an Apache2 web server and victim Windows OS machine logs from applications, system and security logs. Their module will monitor the change in the web server parameters and accordingly generate alerts based on the specified rules. For detecting DoS attacks the author used process to 1) Check for the number of requests coming to the server 2) Check for the Size of response packet 3) Check for the browser agent 4) Check for Source IP Address 5) Check for the amount of time connection is open 6) Monitoring Registry Value Modification 7) Check for unknown connection to the foreign network 8) Monitoring applications being created automatically 9) Monitor user privilege escalation. Although considering only one network device and labeling that SIEM is not a secure process to provide security. Also, this is only a single tactic labeled under tactic Impact whose technique falls under technique as endpoint denial of service or either network denial of service.

Similarly, Airull Azizi et. al.[8] created a framework for detecting lateral movement in the network using the score in SIEM. The author mentions that this framework can be integrated into the existing network security devices such as next-generation firewall, Advanced Persistent Threat (APT), or (SIEM) to improve lateral movement detection. IF the packet access on prohibited resources is more, then they increase the packet score. If the packet violated the traveling pattern, then increase the packet score. When the overall score is high, quarantine the packet else monitor the outgoing packet from the network. It was an unimplemented framework that was derived based on the packet pattern, behavior, and signature-less detection. This is a tactic Lateral Movement and technique that falls under this category can be remote services, exploitation of remote services, lateral tool transfer, and software deployment options.

Bilal et. al. [11] proposes a framework for a SIEM that focuses more on security administrators. They used OSSIM SIEM and proposed a risk factor calculation formula to identify risk levels from 1 to 10.

Imane Bachane et. al. [2] also talked about SIEM and its importance. The author mentioned challenges that can be faced when a digital forensic investigation is required in a cloud context. The research aimed to provide a proposed approach to integrating a SIEM in cloud computing. The author tried a small experiment where a SIEM server was implemented at the client-side, and then configured the applications and devices to send their logs to the SIEM server. Once the logs were received, they were examined, correlated, and then stored. Once an incident needs a digital forensic investigation, the logs will be restored and verified to solve the incident.

Authors Beatriz Gallego-Nicasio Crespo et. al. [1] and Kai-Oliver Detken et. al. [3] worked on the live projects. These project names were ACDC and CLEARER. In the former live project, new generation SIEM which means 20th-century SIEM was used in the cyber-security context, as part of the work conducted in the ACDC project. Botnets were addressed as security concerns in business risk analysis. Experimenting with DDoS attacks, different types of botnets, malicious websites were conducted. The author

concluded that Botnets are considered among the major security concerns which need to be tackled. In the later live project, the authors aimed at developing a security system, which extends existing NAC systems with SIEM functionality, also analyzing methods and dynamical compliance support by using Open Source Software (OSS). The expected result, a common security platform for attack prevention, will be affordable for small and medium-sized enterprises (SME) in contrast to other vendor-based SIEM systems.

As there are various network devices, databases, servers, etc which can be orchestrated in a cloud setup or on the data lake according to the organization architecture. Authors tried to experiment to provide security to handheld devices i.e. mobile phones. Here, Android operating system logs were collected to analyze and check if any vulnerability is there or not. Markus Scholzel et. al [12] carried out a similar study. Mobile devices such as smartphones and tablet PCs are increasingly used for business purposes. However, the trustworthiness of operating systems and apps is controversial. They can constitute a threat to corporate networks and infrastructures if they are not audited or monitored. Android device logs are sent to the SIEM tool and threats are identified while the device is being used so that audit and user monitoring can be done of who is entering or leaving a network with handheld devices. This is done using IF-Map to control access and restrict access for untrusted devices. The author created a prototype to run on the android device, named DECOmap, which provides features to monitor mobile devices and detect incidents in architecture based in Nagios with and without IF-MAP.

Security information and event management (SIEM) is a tool that is used to analyze security event data in real-time for internal and external threat management, and to collect, store, analyze and report on log data for incident response, forensics, and regulatory compliance. In cybersecurity, botnets need to be detected using SIEM. Beatriz et. al. [1] concluded that botnets have come to be considered among the major security concerns in any business risk analysis. The activities conducted in the paper w.r.t. ACDC was carried out which had proven beneficial to test the integration of different tools provided by partners, identify vulnerabilities, technical requirements, and remedies.

Kai-Oliver Detken et. kal [3] worked on the research project CLEARER aimed at developing a security system, which extends existing NAC systems with SIEM functionality, additional analyzing methods, and dynamical compliance support. This goal will only be reached by using Open Source Software (OSS). The expected result, a common security platform for attack prevention, will be affordable for small and medium-sized enterprises (SME) in contrast to other vendor-based SIEM systems. Another aim is to prove the compliance standards to different authorities.

The authors discussed proposed methods or techniques to make the existing tools better.

Igor Kotenko et. al. [13] aimed at providing a technique for countermeasure selection in SIEM which will be based on the suggested complex of security metrics and countermeasure effectiveness metrics. The author provided solutions on the countermeasure implementation at any time based on the current security state and security events. The author experimented with different attack profiles, different attacker skills, attack paths, attack goals, and different security events to compare. While Amir Azodi et. al. [14] worked on the Syslog format of log data, where a large list of tokenizers was created in order to find an answer to the above-posted question. The tokenizers were run against the log lines until a match was found. The appropriate log line was then passed on to the correct extraction module for further processing. This process is currently the standard procedure of most IDS and SIEM systems. These experiments were carried out on the Splunk SIEM tool. Muhammad Afzaal et. al. [15] used OSSIM SIEM to estimate the performance of the proposed system in terms of signatures generation time. The author proposed architecture for storing forensic data, working with a threshold value of the RSA algorithm which outperforms existing SIEM solutions concerning intrusion detection and fault tolerance. These proposed methods were found to be quite useful for

organizations. Most of which have already been implemented by the current date and time.

While working with SIEM-based systems it is very important to have comparison or evaluation between existing SIEM tools and its research is quite very important. Arshad Khan et. al. [4] studied the evaluation of the performance of LogRhythm SIEM within a network to evaluate its efficiency and the frequency as well as types of threats it can handle. Using LogRhythm SIEM, various external vulnerability tests were performed, 894 alarms were generated out of which 48.7% alarms were categorized as critical condition alarms, 9.84% alarms were confirmed intrusion detection systems, 12.64% alarms were suspicious endpoint authentication activities.

Similarly, Moukafih Nabil et. al [5] studied 3 SIEM tools i.e. OSSIM, ELK, LogPoint, and proposed SIEM selection criteria. Selection criteria applied to OSSIM, ELK and LogPoint contain Data collection, Normalization, Correlation, and Reporting stages, documentation, Evolution of the solution, deployment, and level of integration steps. The selection criteria are through calculation of EPS of the network, and strong and weak points for facilitating the decision-making process in choosing the best solution.

Sandeep Sekharan et. al. [6] studied 4 SIEM tools i.e. IBM QRadar, HP ArcSight, Splunk, and LogRhythm. To study event correlation engine, technical comparative study, also they were focused on open source rule-based correlation engine. Limitation includes false positive alerts. Based on the study it was observed that based on similarity-based, knowledge-based, and statistical-based points, the characteristics of a SIEM are identified. So capabilities of a SIEM must be looked upon while making selection decisions.

Based on the above study it is observed that the authors have done analysis but have not worked on the SIEM. It is important to deploy the free version of the SIEM in the working environment and test the false positives and false negative alerts along with factors mentioned by the Gartner for SIEM tools. Advanced Persistence Techniques (APTs), Advanced Evasion Techniques (AETs) used in sophisticated attacks harm the business and make them vulnerable. SIEMs are expected to tackle the latest and emerging security breaches and challenges with advanced analysis. Along with that, enterprises need to comply with the regulatory standards like PCI DSS, FERPA, HIPAA, ISO, DISA, FISMA, SOX, etc. that leverage multiple types of Use Cases.

## 3. RESEARCH QUESTIONS, GAPS IDENTIFIED AND OBSERVATIONS

### 3.1 Research Questions

SIEM must support virtualization, VMware, Hyper-V, Storage, Networking challenges, Types of known attacks, How to identify unknown attacks, detect the threat, mitigate that threat, alert about the threat. Based on this the questions that need to be answered are:

What sub-areas/process or part of the process SIEM will focus on? Identify and address the features required in a SIEM selection for network security in an organization.

**Q. Which factors affect SIEM study?**

The major factors affecting the research in SIEM are improving the selection of SIEM, technologies supported, integrations available, minimum hardware requirements, and any limitations in achieving network security.

**Q. What makes it more useful or more error-prone or more variable?**

Network security to safeguard critical assets, open networks, devices left unprotected, human errors, hacker attacks, existing network, and hardware vulnerabilities.

**Q. Who do you want to observe carrying out this sub-process?**

Organization SOC team engineers and experts need to check all the features, support plans available, any out-of-the-box services, process workflow, list of attacks the organization can sustain.

**Q. What kind of changes do you think will happen? How will the sub-process, or its outcome be different?**

Changes like organizations will not struggle in selecting which SIEM to choose so that the resources are utilized effectively. The sub-process or its outcome will be different because change is required to protect the data from getting stolen or corrupted.

**Q. Why bother studying this? Why is this problem important? Who should care about this problem and why?**

No best tool compares various SIEM and gives specific information that which SIEM is best for the organization. This problem is important as this is the digital era and the use of digital devices is going to increase more in the coming 20 years. It would help to make the network more secure.

Automated security is what everyone is looking for. But a SIEM is designed semi-automatic to date, SOC team expert expertise is still required in between.

Overworked analysts, alert fatigue, and industry researchers who don't have full visibility to understand, handle and respond to the security alerts need to be reduced.

Before using SIEM and after SIEM is purchased, all the factors must be looked at.

### 3.2 Gaps Identified

Selection of which SIEM tool is suitable for different network environments.

Unavailability of comparison of various SIEM tools, Architectures, Analytics, Use cases.

The unavailability of SIEM tool features makes the network more secure and not available directly. Survey [26] shows that many SIEM are not rated by the standard body.

The available list of known attack techniques and tactics but unavailability of techniques to find out unknown attacks which are still out of radar.

### 3.3 Top 10 SIEM Challenges Faced Today

1. Open source and paid TI available but they still lack ways to identify unknown threats and active threats
2. Deployment of the SIEM as is a long process of fulfilling the prerequisites first and adjust with the network architecture
3. Too many alerts cause system performance degradation
4. Surprise attack alert to the security teams
5. Data Storage at cloud, premises not provided proper account security configurations

6. Low coverage of all devices in the network leads to undiscovered devices
7. Insider threats lead to undiscovered
8. Abnormal system and user behaviors
9. Correlation of logs challenges
10. Huge log management on the deployed systems

## 4. Proposed Idea

The detailed survey shows that the problems need strategic solutions for them to provide security in the area where the focus has never been done or least done. These include

1. **Architecture scalability**: It contains how and where a solution must be deployed, Horizontal and vertical scaling must be evaluated by the solution architect. Horizontal scaling means adding more machines to the pool of resources, also called scale-out whereas the latter means adding more power such as CPU, RAM, disk space to an existing machine, also called scale-up.
2. **Deployment** options available like cloud, on-premises, remote location, and their operation process must be properly shared before deployment.
3. **Log and Data Management** provides maximum compression ratio, easy collection of security event logs, and data from security and non security technologies to conduct threat detection.
4. **Real-time log and device Monitoring** must be available.
5. **Analytics**: It must be available on the live log events received and other offline data sources to detect malicious activity and harmful resources. Machine learning models on real-time data must be available, with the facility of creating custom ones.
6. **Data application monitoring**: It should be capable of providing visualization of data so that monitoring becomes easy over endpoint devices, data sources, applications, network activity, cloud apps, and instance activity.
7. **Threat and environmental context**: It should contain contextual information on the logs through enrichment, audit of SIEM users to detect any anomalous activity of users, network audits for compliance and abnormal behavior of devices, as well as facility to possibly detect external threats like zero-day attacks must be available.
8. **User context and monitoring**: user and data context needed for threat detection must be available for detecting internal threats and lateral movement.
9. **Incident Management and case management**: This must be available to define workflows and automated actions when any incident takes place. Incident handlers solve the threat case by doing log and alert investigations.
10. **Threat detection tools**: must be available by default for threat detection that may be native to the solution or can be sourced from the vendor.
11. **Compliance** with industry standards must be available. Along with the use cases for audit purposes.
12. **A free version** must be available for doing active research for a longer duration with support services.
13. **The total cost of ownership** of the product deployment to be reduced by using data compression, reduced human efforts in analysis with easy user interface, easy deployment of software, deployment on the existing hardware.

## 5. Applications

This research work would help all types of business sectors in the world. This would help in securing global finance, critical assets, information in these industry areas, Aerospace, Transport, Computer, telecommunications, Agriculture, Construction, Education,

Medicine, Food, Health care, Hospitality, Entertainment, Media, Energy, Manufacturing, Music, Mining, and Electronics.

## 6. Conclusion

The new art of using SIEM in information security has been adopted by organizations for the last decade. This type of detailed study by people in the security domain is very crucial. SOC is composed of various expertise of people at different positions, L1, L2, Advanced and systems which provide advanced analytics. Systems find it challenging to figure out how the threat occurred, when it happened, what was the reason behind the attack, which systems were compromised, and the source of process execution. This process takes days and even months to solve.

This study will bring down the workloads and shorten the time to action at the SOC with the latest research on the terms SOAR and UEBA.

At least reduce the percentage of workload on handling threats and reducing the response time automatically without a SOC analyst getting involved.

At least reduce the time of detection, the average overall time between detection and resolution of an attack.

At least reduce the percentage of threats auto-responded which were found to be false positives.

The research would not need any policymaking for the region or the country as the freely available resources will be utilized in the initial to final stages. The importance of SIEM in various fields is crucial in this era where everything is digital. This can be only achieved by using the right SIEM tools and technologies involved. Further approval to use the paid version of the SIEM would be required to enhance research analysis.

In the future, we would compare various SIEM tools and show the proposed flow for a SIEM or the features that a SIEM provider must have for better security. A framework of the solution that is actually used or tested by the product development organizations.

## Acknowledgements

I am using this opportunity to express my gratitude to thank all the people who contributed in some way to the work described in this paper. I express my thanks to the college Mukesh Patel School Of Technology Management & Engineering, Mumbai for extending their support.

## References

[1] Beatriz Gallego-Nicasio Crespo, Alan Garwood, “Fighting Botnets with Cyber-Security Analytics”, 2014 Ninth International Conference on Availability, Reliability and Security, IEEE Access, DOI: 10.1109/ARES.2014.33, 11 December 2014, pp. 192-198

[2] Imane Bachane, Youness Idrissi Khamlichi Adsi, Habiba Chaoui Adsi, “Real time monitoring of security events for forensic purposes in Cloud environments using SIEM”, 2016 Third International Conference on Systems of Collaboration (SysCo), IEEE Access, DOI: 10.1109/SYSCO.2016.7831327, 26 January 2017

[3] Kai-Oliver Detken, Marcel Jahnke, Carsten Kleiner, Marius Rohde, “Combining Network Access Control (NAC) and SIEM Functionality based on Open Source”, 2017 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), IEEE Access, DOI: 10.1109/IDAACS.2017.8095094, 07 November 2017, pp. 300-305

[4] Arshad Khan, Rabia Khan, Farhan Nisar, “Novice Threat Model using SIEM System for Threat Assessment”, 2017 International Conference on Communication Technologies (ComTech), IEEE Access, DOI: 10.1109/COMTECH.2017.8065753, 12 October 20I7, pp. 72-77

[5] Moukafih Nabil, Sabir Soukaina, Abdelmajid Lakbabi and Orhanou Ghizlane, "SIEM Selection Criteria for an efficient contextual security", IEEE Access, DOI: 10.1109/ISNCC.2017.8072035, 19 October 2017, pp. 1-6

[6] S. Sandeep Sekharan and Kamalanathan Kandasamy, "Profiling SIEM Tools and Correlation Engines for Security Analytics", 2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), IEEE Access, DOI: 10.1109/WiSPNET.2017.8299855, 22 February 2018, pp. 717-721

[7] Sornalakshmi. K, "Detection of DoS attack and Zero Day Threat with SIEM", 2017 International Conference on Intelligent Computing and Control Systems (ICICCS), IEEE Access, DOI: 10.1109/ICCONS.2017.8250515, 11 January 2017, pp. 1-7

[8] Airull Azizi Awang Lah, Rudzidatul Akmam Dziyauddin, Marwan Hadri Azmi, "Proposed Framework for Network Lateral Movement Detection Based On User Risk Scoring in SIEM", 2018 2nd International Conference on Telematics and Future Generation Networks (TAFGEN), IEEE Access, DOI: 10.1109/TAFGEN.2018.8580484, 20 December 2018, pp. 149-154

[9] Oskars Podzins, Andrejs Romanovs, "Why SIEM is Irreplaceable in a Secure IT Environment?", 2019 Open Conference of Electrical, Electronic and Information Sciences (eStream), IEEE Access, DOI: 10.1109/eStream.2019.8732173, 06 June 2019

[10] Natalia G. Miloslavskaya, Alexander Tolstoy, "Application of Big Data, Fast Data and Data Lake Concepts to Information Security Issues", 2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), IEEE Access, DOI: 10.1109/W-FiCloud.2016.41, 18 October 2016

[11] Bilal AlSabbagh, Stewart Kowalski, "A Framework and Prototype for A Socio-Technical Security Information and Event Management System (ST-SIEM)", IEEE Access, DOI 10.1109/EISIC.2016.51, 06 March 2017, pp. 192-195

[12] Markus Scholzel, Evren Eren, Kai-Oliver Detken, "A viable SIEM approach for Android", 2015 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), IEEE Access, DOI: 10.1109/IDAACS.2015.7341414, 03 December 2016, pp. 803-807

[13] Igor Kotenko, Elena Doynikova, "Countermeasure selection in SIEM systems based on the integrated complex of security metrics",2015 23rd Euromicro International Conference on Parallel, Distributed, and Network-Based Processing, IEEE Access, DOI 10.1109/PDP.2015.34, 23 April 2015, pp. 567-574

[14] Amir Azodi, David Jaeger, Feng Cheng, Christoph Meinel, "A New Approach to Building a Multi-Tier Direct Access Knowledgebase For IDS/SIEM Systems", 2013 11th International Conference on Dependable, Autonomic and Secure Computing, DOI 10.1109/DASC.2013.48, 26 June 2014, pp. 118-123

[15] Muhammad Afzaal, Cesario Di Sarno, Salvatore D'Antonio, Luigi Romano, "An Intrusion and Fault Tolerant Forensic Storage for a SIEM System", 2012 Eighth International Conference on Signal Image Technology and Internet Based Systems, IEEE Access, DOI 10.1109/SITIS.2012.89, 11 January 2013, pp. 579-586

[16] Vladimir Vasilyev, Rinat Shamsutdinov, "Security Analysis of Wireless Sensor Networks Using SIEM and Multi-agent Approach", 2020 Global Smart Industry Conference (GloSIC), IEEE Access, DOI: 10.1109/GloSIC50886.2020.9267830, 30 November 2020, pp. 291-296

[17] Thi Quynh Nguyen, Romain Laborde, Abdelmalek Benzekri, Bruno Qu'hen, "Detecting abnormal DNS traffic using unsupervised machine learning", 2020 4th Cyber Security in Networking Conference (CSNet), IEEE Access, DOI: 10.1109/CSNet50428.2020.9265466, 26 November 2020

[18] Mohammad Ashiqur Rahaman, Cedric Hebert, Jurgen Frank, "An Attack Pattern Framework for Monitoring Enterprise Information Systems", 25th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises, IEEE Access, DOI: 10.1109/WETICE.2016.46, 11 August 2016, pp. 173-178

[19] Tebogo Mokoena, Tranos Zuva, "Malware Analysis and Detection in Enterprise Systems", 2017 International Symposium on Parallel and Distributed Processing with Applications and 2017 IEEE International Conference on Ubiquitous Computing and Communications (ISPA/IUCC), IEEE Access, DOI: 10.1109/ISPA/IUCC.2017.00199, 28 May 2018, pp. 1304-1310

[20] Safeguarding Your Technology: Practical Guidelines for Electronic Education Information Security, Book by Tom Szuba, September 1988, Chapter 3: Security Policy: Development and Implementation, pp. 27-34

[21] Website, https://www.varonis.com/blog/what-is-siem/

[22] Website, https://www.exabeam.com/siem-guide/siem-architecture/

[23] Website, https://www.nap.edu/read/1581/chapter/4

[24] Website, https://niccs.cisa.gov/about-niccs/cybersecurity-glossary

[25] Website, https://searchsecurity.techtarget.com/definition/attack-vector

[26] Website,https://silo.tips/download/masters-thesis-security-information-and-event-management-for-small-and-medium-si

[27] Website, Security Information and Event Management (SIEM): Analysis, https://www.mdpi.com

Mukesh Yadav received her B.E. (Bachelors) degree in Computer Engineering from Pillai College of Engineering, New Panvel, University of Mumbai, Maharashtra, India in 2013 and M.E. (Masters) degree in Computer Engineering from Pillai College of Engineering, New Panvel, University of Mumbai, Maharashtra, India in 2016. She is currently pursuing her Ph.D. degree from MPSTME, Mumbai of SVKM's NMIMS University, Mumbai, Maharashtra, India. Her research interests include Cybersecurity, Security Information and Event Management, Machine Learning and Big data analytics.

Dr. Dhirendra Mishra received the B.E. degree in Computer Engineering from RAIT, Mumbai, Maharashtra, India in 2002, M.E. in Computer Engineering from TSEC, Mumbai, Maharashtra, India in 2008 and Ph.D. in Computer Engineering from NMIMS, Mumbai, Maharashtra, India in 2012. He is currently working as a Professor in the Department of Computer Engineering with MPSTME, NMIMS University, Mumbai, Maharashtra, India. His research interests include Image Processing - Image Database, Pattern matching, Image/Data Mining, Biometrics, Storage Technologies, Data Analytics.