**National University of Computing and Emerging Sciences - FAST**

**Project Report**

**Group Members:**

**Arman 19K-0263**

**Muhammad Bilal 19K-0297**

**Muhammad Sajjad Aziz 19K-1411**

**Section: 7E**

**Course Code: CS3002**

**Course Name: Information Security**

**Submitted to: Dr. Sufian Hameed**

**Table of Contents**

[**What is SIEM?**](#_70b3bvpde8nh) **4**

[**Why is SIEM important?**](#_ovmzzt7cjmcd) **4**

[**How Does SIEM Work?**](#_edd1r9xgvlr) **4**

[Log Management](#_841m5l3098ve) 5

[Event Correlation and Analytics](#_s3m8axuz6470) 5

[Incident Monitoring and Security Alerts](#_onlaybg1zewm) 5

[Compliance Management and Reporting](#_gmnaolnxbq99) 5

[**The Benefits of SIEM**](#_in15xr8cten8) **6**

[Advanced Real-time Threat Recognition](#_8xsno7p3o6ub) 6

[Regulatory Compliance Auditing](#_tauck9nck6bh) 6

[AI-driven Automation](#_yzp349rgjpcj) 6

[Improved Organizational Efficiency](#_whzw12ixlwzl) 7

[Detecting Advanced and Unknown Threats](#_r6s41l8w9mz1) 7

[Conducting Forensic Investigations](#_rh9ed3k4k44l) 8

[Assessing and Reporting on Compliance](#_bi8wasvsde9f) 8

[Monitoring Users and Applications](#_6bnoyfel6h1r) 8

[**Tools and features involved in a SIEM solution**](#_6chaosw39k6) **8**

[Log Data Management](#_7oju5k29yoz0) 8

[Network Visibility](#_gq1zo12p8gbh) 8

[Threat Intelligence](#_wwfd3cgl2bu4) 9

[Analytics](#_o1a1fd6jy5lp) 9

[Real-time Alerting](#_w1impziet5b) 9

[Dashboards and Reporting](#_uaz3qlutdzqn) 9

[IT Compliance](#_wqzntyas131r) 9

[Security & IT Integrations](#_h4t2s4jijq7m) 10

[**SIEM Implementation**](#_z4ehmfh8smvr) **10**

[**SIEM Solutions in the Market**](#_rlrmkahzwt63) **11**

[ArcSight](#_5ms6oajo7ve0) 11

[IBM QRadar](#_k0zms6g18uje) 11

[Splunk](#_2y671yqfunp8) 11

[**SIEM and PCI DSS compliance**](#_oq9hnausbiuk) **12**

[**Problems with SIEMs**](#_g8jtr5ynyby2) **12**

[SIEMs are Expensive](#_tn4qm0dtt5cj) 13

[Configuration of SIEMs](#_jvrbr4mx8ido) 13

[Specialized Employees](#_6sr323q3ivsj) 14

[Noise Data](#_nzrlgid5l5o) 14

[Context Around Alerts](#_fcziwngeiy3n) 15

[Reporting Problem](#_hdxplapiw7sf) 15

[Summary of Problems](#_90elwcr07t01) 15

[**SIEM Alternatives**](#_fnpuu9a7850a) **15**

[Centralized Log Management platform (CLM)](#_nom0vjg3dhtc) 15

[User Entity and Behavior Analytics (UEBA)](#_y64ytbo6puvy) 16

Security Information and Event Management (SIEM)

# What is SIEM?

Security information and event management or SIEM, is a tool that enables businesses to identify, assess, and respond to security threats before they have a negative impact on business operations.

# Why is SIEM important?

Security information and event management (SIEM), which combines security information management (SIM) and security event management (SEM), is a security tool that aids companies in identifying potential security flaws and threats before they have a chance to interfere with daily operations. For security and compliance management use cases, it surfaces user behavior anomalies and employs artificial intelligence to automate many of the manual operations related to threat identification and incident response. It has become a mainstay in contemporary security operation centers (SOCs).

Over time, SIEM has developed into something more than the log management technologies that came before it. Thanks to the power of AI and machine learning, SIEM now provides advanced user and entity behavior analytics (UEBA). It is a very effective data orchestration solution for handling constantly changing risks as well as reporting and regulatory compliance.

# How Does SIEM Work?

All SIEM solutions perform some level of data aggregation, consolidation, and sorting at the most fundamental level in order to detect threats and meet data compliance standards. While some solutions have a range of capabilities, the majority provide the same fundamental functionality:

## Log Management

SIEM gathers event data from numerous sources throughout the network of a company. IT and security teams can automatically manage their network's event log and network flow data in one centralized location thanks to the real-time collection, storage, and analysis of logs and flow data from users, applications, assets, cloud environments, and networks.

In order to compare their internal security data with known threat signatures and profiles, several SIEM solutions also integrate with third-party threat intelligence feeds. Teams can stop or recognise novel attack signature types through integration with real-time threat sources.

## Event Correlation and Analytics

Any SIEM solution must provide event correlation. Event correlation uses advanced analytics to quickly find and eliminate possible threats to enterprise security by identifying and comprehending complex data patterns. The manual operations associated with the in-depth analysis of security events are offloaded by SIEM systems, which considerably reduce the mean time to detect (MTTD) and mean time to respond (MTTR) for IT security teams.

## Incident Monitoring and Security Alerts

SIEM systems are able to recognise all entities in the IT environment since they provide centralized management of on-premise and cloud-based infrastructure. By categorizing strange activity as it is discovered on the network, SIEM technology is able to monitor for security incidents across all connected users, devices, and applications. Administrators can be quickly warned and take appropriate action to mitigate it using customisable, established correlation criteria before it develops into more serious security risks.

## Compliance Management and Reporting

SIEM solutions are a popular option for businesses that must adhere to various regulatory requirements. SIEM is a useful solution for obtaining and verifying compliance data across the whole corporate infrastructure because of the automated data collection and analysis it offers. The burden of security management can be lessened by SIEM solutions' ability to produce real-time compliance reports for PCI-DSS, GDPR, HIPPA, SOX, and other compliance requirements. These reports can also help identify potential infractions before they become problems. Numerous SIEM solutions provide pre-built add-ons that can automatically produce reports that satisfy compliance standards right out of the box.

# The Benefits of SIEM

No matter how big or small your company is, it's critical to take proactive measures to monitor for and reduce IT security risks. Enterprises can gain from SIEM systems in a number of ways, and they have become a key part of optimizing security procedures. Among the advantages are:

## Advanced Real-time Threat Recognition

As your organization grows, SIEM active monitoring solutions throughout your whole infrastructure help to boost security posture by reducing the amount of time it takes to detect and respond to possible network attacks and vulnerabilities.

## Regulatory Compliance Auditing

Centralized compliance audits and reporting across the whole corporate infrastructure is made possible by SIEM systems. While adhering to stringent compliance reporting rules, advanced automation speeds the gathering and analysis of system logs and security incidents.

## AI-driven Automation

As IT teams manage enterprise security, next-generation SIEM systems interact with potent Security Orchestration, Automation and Response (SOAR) capabilities to save time and resources. These technologies are able to handle sophisticated threat identification and incident response protocols in a substantial amount less time than physical teams because they use deep machine learning that automatically adjusts to network behavior.

## Improved Organizational Efficiency

SIEM can be a key factor in increasing interdepartmental efficiencies because of the enhanced visibility of IT infrastructures it offers. Teams may communicate and work together more effectively when responding to perceived events and security problems when they have a single, unified view of the system data and an integrated SOAR.

Explore further SIEM resources from IBM's security intelligence experts to learn more about the advantages of security information and event management and to determine if it is appropriate for your company.

## Detecting Advanced and Unknown Threats

Organizations must be able to rely on solutions that can identify and respond to both known and unidentified security threats given how quickly the cybersecurity landscape changes. SIEM successfully mitigated using integrated threat intelligence feeds and AI technology against modern security breaches like:

* **Insider Threats -** Assaults or security flaws that result from unauthorized users accessing corporate networks and digital assets Credential compromise may have led to these attacks.
* **Phishing Attacks -** Social engineering attacks that pose as reliable organizations are frequently used to acquire customer information, login passwords, financial information, or other confidential corporate data.
* **SQL Injections -** Malicious code designed to get past security barriers and add, change, or remove records in a SQL database that is executed via a compromised website or application.
* **DDos Attacks -** A DDoS assault that aims to overwhelm networks and systems with excessive traffic, rendering servers and websites useless as a result.
* **Data exfiltration -** Data extrusion or theft is frequently accomplished via a network asset's popular or simple-to-crack credentials or by using an Advanced Persistent Threat, or APT.

## Conducting Forensic Investigations

When a security issue happens, SIEM systems are excellent for performing digital forensic investigations. Organizations can effectively gather and analyze log data from all of their digital assets with SIEM systems. This enables them to reproduce previous occurrences, examine current ones, look into questionable activities, and put in place more efficient security procedures.

## Assessing and Reporting on Compliance

For many firms, compliance auditing and reporting is a crucial yet difficult duty. By offering real-time audits and on-demand reporting of regulatory compliance whenever necessary, SIEM solutions significantly cut the resource expenditures necessary to manage this process.

## Monitoring Users and Applications

Organizations require the amount of visibility required to manage network hazards from outside the conventional network perimeter as remote workforces, SaaS apps, and BYOD (Bring Your Own Device) policies gain popularity. The visibility of the entire infrastructure is greatly improved by SIEM systems, which keep track of all network activity across all users, devices, and apps. These solutions also detect risks regardless of where digital assets and services are accessed.

# Tools and features involved in a SIEM solution

## Log Data Management

The base of security information and event management is log data collection. Productivity and efficiency are increased by real-time data collection, analysis, and correlation.

## Network Visibility

The SIEM analytics engine can gain further insights into assets, IP addresses, and protocols by looking at packet captures for visibility into network flows. This allows it to spot malicious files or the data exfiltration of personally identifiable information (PII) flowing across the network.

## Threat Intelligence

To identify and counteract current vulnerabilities and attack signatures, your SIEM solution must be able to include both proprietary and open-source intelligence streams.

## Analytics

The level of data analysis offered by different SIEM solutions varies. As more sophisticated and complicated attacks occur, solutions incorporating cutting-edge technology like machine learning and artificial intelligence assist in their investigation.

## Real-time Alerting

SIEM systems can be tailored to meet specific business requirements by using pre-defined, tiered alerts and notifications distributed among numerous teams.

## Dashboards and Reporting

Hundreds or even thousands of network events per day may occur in some organizations. It's crucial to comprehend incidents and report them in a customisable view with no lag time.

## IT Compliance

The criteria for complying with regulations differ greatly amongst organizations. Even while not all SIEM products provide comprehensive compliance coverage, businesses in highly regulated sectors give auditing and on-demand reporting priority over other functions.

## Security & IT Integrations

A SIEM that interacts with pre-existing investments in security and IT tools will be beneficial to established enterprises. Organizational visibility starts with integrating the SIEM with a variety of security and non-security log sources.

# SIEM Implementation

Here are some SIEM implementation best practices you have to adhere to, both before and after you invest in your new solution:

1. Start by thoroughly comprehending the implementation's scope. Determine which deployment strategies will help your company the most, and then put up the relevant security use cases.
2. Create and implement your established data correlation rules across all networks and systems, including any cloud deployments.
3. To better understand your risk posture, list all of your company's compliance obligations and make sure your SIEM solution is set up to audit and report on them in real-time.
4. Organize and categorize every digital asset in the IT infrastructure of your company. This will be crucial for controlling log data collection, spotting access abuses, and keeping an eye on network activity.
5. Establish IT setups, limits, and BYOD (Bring Your Own Device) policies that can be tracked when integrating your SIEM system.
6. Tune your SIEM configurations frequently to make sure you're lowering the number of false positives in your security alerts.
7. To ensure that teams can react swiftly to any security issues that call for action, it is important to document and practice all incident response strategies and protocols.
8. Automate where you can by utilizing security orchestration, automation, and response (SOAR) tools and artificial intelligence (AI).
9. Consider whether you should spend money on a managed security service provider (MSSP) to oversee your SIEM deployments. The complexity of your SIEM setup, as well as routine management and upkeep of its continuous performance, may be best handled by MSSPs depending on the particular demands of your business.

# SIEM Solutions in the Market

There are numerous event and security information management solutions available. Among the most well-known are Splunk, IBM QRadar, and Arcsight ESM.

## ArcSight

ArcSight gathers and examines log data from the operating systems, applications, and security tools used by an organization. Security workers are informed by the system when a malicious threat is found.

Additionally, ArcSight can initiate an automatic response to halt the harmful behavior. The capability to include outside threat intelligence feeds for more precise threat detection is another benefit.

## IBM QRadar

IBM QRadar gathers log data from a variety of information system sources within an organization, including network hardware, operating systems, software, and user activity.

Real-time log data analysis provided by the QRadar SIEM enables customers to immediately recognise and stop threats. From cloud-based applications, QRadar can also gather network flow information and log events. Threat intelligence feeds are supported by this SIEM as well.

## Splunk

Splunk Enterprise Security offers real-time threat monitoring, quick analyses using visual correlations, and investigative research to track the dynamic actions linked to sophisticated security threats.

Both a locally installed copy of the software and a cloud service are options for the Splunk SIEM. Third-party app integration of threat intelligence feeds is supported.

# SIEM and PCI DSS compliance

An organization can become PCI DSS compliant with the aid of SIEM tools. Customers are reassured by this security requirement that a corporation will protect their credit card and payment information from loss and unauthorized use.

The following PCI DSS standards can be satisfied by a SIEM:

* Unauthorized network connection detection: Organizations that are PCI DSS compliant must have a system that can identify any unauthorized network connections to or from their IT assets. Such a system might be a SIEM solution.
* Finding insecure protocols - A SIEM has the capacity to record and support the use of an organization's approved services, protocols, and ports as well as to record security measures taken for insecure protocols.
* Examine the flow of traffic across the DMZ. PCI-compliant businesses must set up a DMZ to control connections between web servers and untrusted networks (like the internet). Outgoing traffic involving cardholder information needs to be scrutinized, and inbound internet traffic to IPs in the DMZ needs to be restricted.

By examining traffic that crosses the DMZ to and from internal systems and reporting on security issues, SIEM solutions can satisfy these requirements.

# Problems with SIEMs

Security information and event management (SIEM) platforms can be incredibly effective defensive tools, but their effectiveness is constrained by a long list of issues that frequently make them more of a burden than a help. To be clear, a properly configured SIEM managed by a security department with adequate staffing is a huge help to an organization's capacity to detect and respond to incidents.

In other words, SIEMs are great in an ideal world, but few of us really live in one.

In the real world, SIEMs are intrinsically difficult, and the difficulties are quite simple to list: SIEMs are expensive, operate with highly trained personnel, take a long time to set up, are frequently distracting, and have rigid and frequently complex reporting requirements. In the end, many businesses just lack the time, funds, or resources necessary to support all of the different parts of running a SIEM.

Although there are many ways in which SIEM concerns are integrally linked to one another, we will attempt to discuss them separately below.

## SIEMs are Expensive

SIEMs are costly. quite pricey. Additionally, the costs are not entirely clear. The original purchase of SIEM accounts for 25% of costs, with the rest 75% going for installation, upkeep, and staffing, according to a Ponemon Institute study. More particular, SIEM prices vary and are not uniform. Initial license fees, implementation, continuing maintenance, renewal, integration of data sources, and employee training are all expenses that must be paid before the SIEM can be used. Approximately 78 percent of the firms that responded to Ponemon's survey said they only have one employee who is solely responsible for their SIEM, yet 64 percent said they spend more than $1M yearly on SIEM-related expenses.

To date, in a different survey performed by a business named Netwrix, 69% of respondents stated a desire to lower their SIEM expenses. This issue is worsened by consumption-rate-based pricing methods that are typical among SIEM providers and can result in unforeseen costs in the future.

## Configuration of SIEMs

Almost nothing is done by a SIEM on its own out of the box. Of course, a business can spend extra money on a preconfigured SIEM, but these preconfigured SIEMs are frequently distractingly noisy and contextless. Additionally, it is quite unlikely that a preconfigured SIEM is and truly cannot be tailored to the distinct threat model, maturity, and demands of an organization. As a result, the expense of employing an employee or consultant with the necessary expertise to not only build out your SIEM but also produce the correlation rules for it moving forward is intrinsically built into the already high cost of the SIEM. By the way, the cybersecurity business is now experiencing a rather severe skills shortfall. As an alternative, you might pay for a threat intelligence feed to be used to populate your SIEM, but this is also pricey and noisy, which is a separate issue. It could take weeks or months to feed your various data sources into your SIEM, noise aside (we'll talk about that later). This task becomes more challenging the more dissimilar the data sources are.

Similar to this, the Netwrix survey revealed that finding the requested data in the SIEM can be very difficult, with 65% of respondents saying this. Beyond this, since things can just cease feeding the SIEM, you need to constantly monitor what is and isn't talking with it. Sometimes it's difficult to ignore; other times, it's not immediately obvious that a data source has been disconnected.

The founder of The Ponemon Institute succinctly summarizes SIEM configuration and management issues:

“The root of their dissatisfaction seems to be related to the complexity of the SIEM itself,” explained Dr. Larry Ponemon, chairman and founder of the Ponemon Institute. “In fact, 75 percent of respondents said there is significant, or very significant, effort involved in configuring their SIEM for their organization. Obviously, this complexity can make it very difficult to extract the value they want and need.”

## Specialized Employees

In a survey conducted by 451 Research, 44% of firms said they lacked the staff skills needed to manage a SIEM effectively. According to the Netwrix poll mentioned earlier, 55% of businesses rely on SIEM experts to run their SIEM.

## Noise Data

According to research conducted by Netwrix, 81 percent of respondents stated that their SIEMs produced too much "noise data." In its SIEM survey, Rapid7 discovered that more than half of enterprises can only analyze one to ten alerts every day, whereas nearly three-quarters of respondents' SIEMs produce more than ten alerts per day.

## Context Around Alerts

Since SIEMs only compile system logs and solely notify analysts when something potentially negative has occurred, they frequently lack context and useful information, which might leave analysts unsure of how to react to a SIEM alert. Less than half of those who participated in the Ponemon Institute study said they were happy with the useful information their SIEMs provided.

## Reporting Problem

SIEM reporting is purely rigid. Another statistic from Netwrix: 63% of survey participants reported having trouble understanding the reports generated by their SIEM, and a further 53% indicated they manually adjusted their SIEM reporting to make it more comprehensible for non-tech stakeholders.

## Summary of Problems

Daniel Kennedy, an analyst with 451 Research, nicely encapsulates the problems with SOCs:

“SIEM solutions hold a lot of promise as the centralized solution for unlocking all the secrets held in the logs of enterprise systems and marrying them with the use of threat intelligence”, said Kennedy. ”That promise comes at a cost, SIEM solutions still retain a reputation for being difficult to set up, difficult to add new feeds to, and difficult to tune. That said, their value to the enterprise security manager is increasingly understood, and while many SIEM implementations may have started out as a compliance check mark, they have transcended those roots.”

# SIEM Alternatives

## Centralized Log Management platform (CLM)

Centralized Log Management is a comprehensive approach to network, data, and security management that uses automated tools to collect logs from across an IT infrastructure.

## User Entity and Behavior Analytics (UEBA)

User Entity and Behavior Analytics is the process of gathering insight into the network events that users generate every day. Once collected and analyzed, it can be used to detect the use of compromised credentials, lateral movement, and other malicious behavior.