Mustansiriyah Journal of Pure and Applied Sciences

www.MJPAS.com

A Survey on Network Security Monitoring: Tools and Functionalities

Z. S. Younus[1]* and M. Alanezi [2]

[1,2]Department of Software, College of Computer Sciences and Mathematics, University of Mosul, Mosul, Iraq,
(zeyad.saffawi@uomosul.edu.iq[1*], mafazmhalanezi@uomosul.edu.iq[2])

A B S T R A C T

Recently, cybersecurity breaches have become more common, with varying levels of impact ranging from simple to major losses of financial resources or data. The network infrastructures are the main goal of the malicious activity to compromise confidentiality, integrity, and availability (CIA) of information security. The network devices produce a large number of logs, making the handling of these logs very important because they serve to record all activities and events that take place on the network's devices and applications to detect and prevent abnormal behaviors. Network security monitoring is a process used to monitor network devices and their traffic to detect security vulnerabilities, threats, and suspicious activities. Organizations are using network security monitoring to quickly detect and respond to cybersecurity threats. Various methods are used to protect network devices, like antivirus, firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS), which typically operate independently. For that reason, attacks cannot be identified unless logs and events from different devices and applications are correlated and managed from a centralized location. Security information and event management (SIEM) addresses this issue by offering the capability to increase the level of information security and data protection through centralized log management for network devices. This paper presents a survey of network security monitoring techniques, encompassing their functionality, contents, and tools. Traditional tools, intrusion detection and prevention systems, and SIEM are some of these tools. In addition, the paper introduces SIEM as the most common and advanced security tool, highlighting its functionalities and capabilities.

Keywords: *Cybersecurity, Network Security Monitoring, SIEM, IDS, IPS.*

1. Introduction

In the last few years, data has become the most important source in the world, which has increased the interest of network hackers and fraudsters for the purpose of stealing, modifying, and destroying data and causing financial losses to the victim. In addition, most specified cyberattacks are detected after a breach, which means the cyberattacks are successful and undetected. When taking this information into account, it must improve the ability to detect cyberattacks [1], [2], [3].

There are some examples of cyberattacks and threats that target network infrastructure, such as ransomware attacks, malware, phishing campaigns directed at

hacking the email in the organization to seize email accounts or impersonate officials, stealing and leaking data, and social engineering attacks to collect sensitive information about the organization from its employees [4], [5], [6].

Malware is software that is used to access computer systems and network resources without being detected to perform a malicious impact on the target system (such as trojan horses, spyware, backdoors, and viruses) for the purpose of disrupting operations, collecting personal information, and stealing data [7], [8].

New attacks are detected, and many techniques like antivirus, spyware, firewall, IDS, and IPS search for anomaly action inside the organization, but these techniques are not able to discover the unknown and zero-day attacks [1], [2].

Networks are built with a high level of complexity and are organized in different layers to maintain the security of information. An attacker can affect the level of security by exploiting the weaknesses in the networks [9]. Most efforts in network security focus on preventing attacks, but techniques and solutions based on the detection of attacks and threats and their response are of great importance in the field of cybersecurity [10], [11], [12]. Its objective is to monitor the status of devices and applications within the network to detect and manage anomalous events promptly to prevent their impact on the network. This is a big challenge because devices and applications in the network generate a huge number of logs, which follows the definition of a big data problem [13].

With the great development in information and communication technology (ICT), companies and organizations have become highly dependent on ICT, which puts their assets vulnerable to the risks of cyber threats, and therefore security countermeasures must be taken to remain under control and for the purpose of generating confidence through the use of these assets [14], [15]. For example, companies need to protect employees and customers inside and outside the organization [16], [17].

Information security is one of the major concerns of executives who lead organizations around the world, with increasing visibility among key decision-makers with each passing year [18]. Numerous studies and reports have proven that current strategies to detect and prevent intrusions are insufficient due to reliance on statistical models or attack signatures that attackers know how to avoid. In addition, endpoint solutions are not able to provide the data required to verify malicious activities and intrusions due to the inability to monitor all events and activities that occur over the network and that affect computer systems [18], [19]. Multiple audit systems must be used to analyze data in multiple locations of the network to detect attacks. This is because the process of collecting data from various resources exhibits a number of challenges, like managing a large number of logs that are generated from different devices, which affects the ability of security teams to identify security breaches or

implement the correct procedures to discover, prevent, or reduce harm that occurs through attacks [20].

Network devices generate a large number of logs, and dealing with these logs is very important. To improve security and protect data, it requires a centralized log management system and, therefore, the use of a high classification tool for the purpose of managing events and information. The Log Management System (LMS) is a central location for the purpose of collecting logs from various resources and storing them in a single location [21]. Security Information and Event Management (SIEM) is an important tool that offers a centralized location for the purpose of collecting logs and analyzing security and provides a comprehensive and centralized view of network status. SIEM tools collect, analyze, normalize, correlate all events, and analyze data coming from several devices and give a centralized view of events [22], [23]. SIEM products are used for processing logs, normalizing their format, conducting analysis, and generating alerts in case of detecting abnormal behavior [24], [25].

In this paper, a survey for network security monitoring and its tools was produced. The structure of this paper is as follows: Section one represents the introduction to this paper. Subsequently, Section two introduces the backgrounds. Section three provides an explanation of advanced security systems and their functionality and capabilities. Section four produced some related works. In Section Five the conclusion of this paper is presented

Backgrounds In this section, network security systems and their tools, requirements, and functionality are introduced. In addition, an explanation of the most important security tools that are used in the field of network security.

2.1 Network Security Systems

Network security is an important part of information technology, as organizations face difficulty achieving security requirements [26], [27]. Network security monitoring is used to provide the ability to track activities and processes in the monitored network. To achieve this goal, the network consists of various software and devices that are distributed within the network [28]. These components send information about network events to a central location for logging and analysis. There are several functions that systems perform for the purpose of information monitoring [29].

The collection phase is performed by a software agent that collects events generated by the network devices for the purpose of creating logs and sends them to a central location for analysis [5], [29].

The normalization | parsing phase is the process of identifying and extracting important information from logs for the purpose of obtaining a logical and organized data structure and converting logs into a common format by normalizing them for the

purpose of simplifying the analysis of logs. One of the main problems in the log collection process is that the manufacturers, when designing hardware and software, do not follow a unified format [5], [29], [30].

The correlation phase combines several sources of data into a single event. The existence of redundant logs when collecting logs from different sources is one of the most prominent problems that can be solved through the process of correlating events [5], [29].

The action phase, which includes: detection, which detects irregular events in traffic; monitoring, which allows information exploration; and incident response, which performs automatic actions on the network configuration [29].

2.1.1 Network Traffic:

There are diverse types of log collection according to the source and type of data, which are: Network Traffic, where the information of traffic can be gathered immediately from the network in various formats such as packets, traffic, and statistics, where there are various tools used for collecting it like Wireshark, NetFlow, and Simple Network Management Packet (SNMP) [31], [32].

Logs, which are used to gather information generated from different resources like applications or operating systems, define an event as an activity or process that occurs within a device or application, which means what a single event can describe depends on many logs. The incident represents a malicious event that happened within the network infrastructure, like data loss, security rule violation, disruption, etc. The most common log format is syslog [33]. Syslog is a protocol used to create logs related to the activities and events that are performed on the system, as it records events such as logins to the system for the purpose of triggering alerts about activities or errors that occur within the system. Also, applications such as web browsers and email have special formats for the purpose of recording logs. The e-mail logging information is useful for the purpose of verifying whether the compromised device has exchanged information with other devices before being hacked. Application log collectors allow for anomaly detection and recording of system accesses (failed and successful). This information is useful in investigations after a security event is detected [34].

2.1.2 Network Security Methods

This section presents some tools that are used to provide valuable security information, which are:

1. **Traditional Security Tools:**

In the past, malware was used as a starting point for cyberattacks against computer systems, such as viruses, trojans, and worms. Attacks are identified and detected through the use of antivirus, antispyware, and so on.

1. Antivirus

It is used for detecting and removing malicious files from computer systems depending on signatures or rules; for that reason, it is only used to detect external attacks. It is performed for the purpose of analyzing computer systems and finding compromised files and programs. It can be configured to produce logs, which can be useful for a security system, for example, Kaspersky or Windows Defender [35].

2. Antispyware

It is a kind of malicious software that is used for the purpose of collecting sensitive information about individuals and is installed on the computer without the user's knowledge. Anti-spyware is used for the purpose of detecting and removing spyware [36].

3. Vulnerability Assessment

It is used to disclose vulnerabilities and security holes that may allow illegal access to the system. These tools operate on the network and devices. Network Mapper (Nmap) is a familiar tool used for port scanning to assess the security of operating systems, permitting the detection of weaknesses and providing useful information about open ports and services [37].

2. Intrusion Detection and Prevention Security Systems

1. Firewalls:

Firewall logs represent a valuable source of security data because they include detailed information about each access to the network. It is used to monitor all inputs and outputs of the traffic, allow normal traffic, and prevent suspicious traffic from accessing the network. For instance, the firewall is provided as a part of Windows Defender in Windows operating systems [38]. Figure 1 shows the firewall security tool on the network.

Figure 1 firewall security tool in the network [38].

2. Intrusion Detection System

It is used for monitoring suspicious actions and traffic inside a network, where, if the suspicious actions are detected, an IDS informs the administrator of the network by triggering an alert in the IDS console. IDS is used to collect the logs from network resources and analyze them to detect threats and anomalous activity within a network [7], [12], [31], [39], [40].

Intrusion detection systems implement a set of technologies for the purpose of detecting threats and suspicious activities by monitoring and analyzing events in the network devices [31], [41]. It consists of two types according to its deployment, which are: host IDS (HIDS) and network IDS (NIDS), depending on the source of the collected data. HIDS is deployed on a single machine and is used for the purpose of monitoring the activities of users and the behavior of processes within the system, such as firewalls and spyware detection, while NIDS is used to collect information from the network and then analyze the data to detect threats and breaches and alert security operators [42], [43], [44], [45], [46].

In addition, IDS can be classified according to their detection into signature-based intrusion detection systems and anomaly-based intrusion detection systems. A signature-based intrusion detection system is based on identifying a signature for an attack pattern, where the attack is detected when the action matches the defined signature, while an anomaly-based intrusion detection system depends on defining a profile for normal activity and detects the attack when there is any deviation from the defined normal activity [12], [41]. IDS is used to detect suspicious threats and attacks based on its known attack signature database and launch alerts, but it cannot prevent them from accessing the system or network [43], [47]. There are some types of IDS tools, such as Snort and Suricata [31]. Figure 2 shows the IDS system on the network.

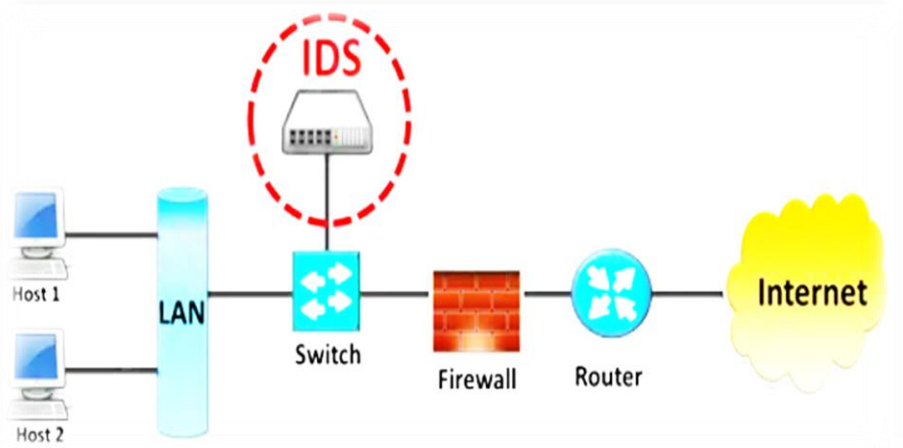

Figure 2 IDS security in the network [38].

3. Intrusion Prevention System

It is a security system that is used for monitoring a network to detect abnormal actions and prevent them from accessing the network infrastructure by taking some defense actions when the threat is occurring, like reporting, blocking, or quarantining it. IPS consists of some types, like network IPS (NIPS) and host IPS (HIPS). HIPS is used to monitor the traffic on the personal computer and check the inputs and outputs of that computer, while, NIPS is used to monitor network traffic and take action to prevent any intrusion or malicious activity against it. Network behavior analysis (NBA), which is used to detect abnormal traffic by analyzing the network traffic, such as distributed denial of service (DDoS) attacks [48], [49], [50]. In addition, IPS can be classified into some methods, including signature-based and anomaly-based [31], [51].

Signature-based, which is used for matching the traffic activity with the signatures of familiar attacks and threats. This method has disadvantages, including the fact that it cannot identify new threats like zero-day attacks. Anomaly-based monitoring is used to monitor suspicious activity in the network by comparing the threshold of normal activity with the actual activity of the network traffic. The drawback of this method is that it can generate false-positive alerts [12]. Figure 3 shows the IPS system on the network.

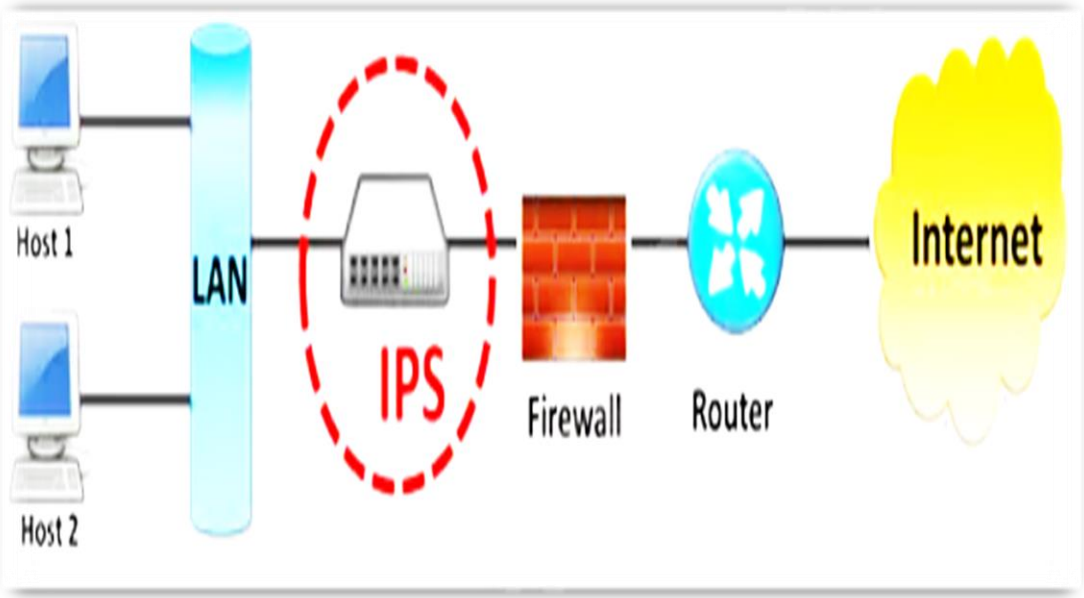

Figure 3 IPS security in the network [38].

The difference between IDS and IPS is that IDS can focus on detecting when an attacker has successfully compromised a system by exploiting a system vulnerability and alerting the administrator about the incidents that occur in the network or system. While IPS focuses on implementing incident response in order to reduce the negative impact of incidents on the system or network, like blocking the source Internet

Protocol (IP) addresses that attempt access to the network [52]. Table 1 explains the main comparison between IDS and IPS [53].

Table 1 A comparison between IDS and IPS [53].

IDS	**IPS**
Detect the suspicious activity and launch alerts	Reduce the negative impact of the Attack
It is not located in the path of traffic	It is located in the path of traffic
NIDS and HIDS: signature-based and abnormal-based	NIPS and HIPS: signature-based and abnormal-based
It is used online or offline	It is used online
It is not reducing the impact of attacks	It is used to reduce the impact of attacks

IDS and IPS Tools:

There are many tools that are used to detect and prevent threats and attacks from having a negative impact. Here, the most common IDS and IPS tools are introduced, as explained below.

- Snort is a common IDS and IPS tool that is used to detect suspicious activities according to the rules and produce alerts to notify the user. The snort is used as a packet sniffer, packet logger, or NIPS [54].
- Suricata is an IDS and IPS tool introduced by the Open Information Security Foundation (OISF) in 2009. It is used to analyze network traffic and threat detection and generate alerts to notify users [55].

3.Advanced Security Tools

1. Cyber Threat Intelligence

It is a process used to collect, process, and analyze information about attacks and threats in cyberspace for the purpose of disseminating information about threats and attacks targeting the organization. It is a mechanism that allows the exchange of information about security threats and attacks for the purpose of improving the detection process between organizations. For example, if a new attack is discovered by the organization, the threat information will be published to the rest of the organizations that use the threat information for the purpose of preventing the attack or dealing with it more effectively. Its aim is to predict security threats and attacks based on previous information, taking into account internal and external threats [56]. Many tools are used in threat intelligence for the purpose of collecting information and creating reports or alerts, and they are combined to work with other security

technologies such as SIEM. There are many tools that are used in threat intelligence, such as the Cyber Threat Alliance [57].

2. Security Information Management (SIM) System

SIM is a tool used to collect and store logs from different resources and provides automated and centralized reporting of the collected data from log files for compliance [58], [59], [60].

3. Security Event Management (SEM) System

SEM is used for the purpose of collecting, analyzing, correlating, and raising alerts and warnings to detect and respond to incidents in real time. The main goal is to create a perception and understanding of the events produced by the network from different sources by collecting events using a single method through which events are analyzed and investigated through forensics, which reduces the time required to conduct investigations [59]. Table 2 demonstrates the differences between SIM and SEM.

Table 2 A comparisons between SIM and SEM [59].

SIM	SEM
Forensics Analysis	Real-time monitoring and alerts
Collect and index logs from different security devices for analysis	Correlation of many events into single incidents
Searching in the logs and alerting the administrator about threats and events	Reporting, alerting, and incident response to mitigate the threat
Long-term storage of logs	Normalization of logs

4. Security Information and Event Management (SIEM) System

Logs are important for information security as they are used for network analysis in order to prevent breaches within an organization or provide incident response in situations where breaches have occurred. Log management and monitoring is a very challenging task, as it is impossible to monitor each log generated from devices and applications and detect the source of an incident in real time. So, the SIEM system can do all the desired actions effectively [16].

In recent years, the need for SIEM systems has increased dramatically in order to provide protection for companies against cyber security threats and enhance their security capabilities. However, one organization's SIEM may not be suitable for another. This is because other factors must be taken into consideration besides the technical aspect when evaluating a SIEM solution [14], [61].

SIEM is a system that performs the process of analyzing events in real time for early detection of threats, intrusions, and attacks targeting the organization. It collects, stores, investigates, and reports on logs for the purposes of incident response, forensics, and regulatory compliance. The main components of SIEM consist of collection logs, normalization, correlation, storage at a central location, and monitoring [62].

In most cases, SIEM can integrate within a security operations center (SOC). SOC is a central unit used for the purpose of monitoring events related to threats and attacks targeting the organization's network [63], [64]. SOC consists of software, operations, and a team of experts and analysts [65], [66].

SIEM can allow SOC analysts to manage and monitor the security of the network infrastructure. The main goal of SIEM is to verify that the concepts of information security, which are confidentiality, integrity, and availability (CIA triad), are included within the organization [9].

Confidentiality is a term used to refer to protecting valuable information from disclosure by an unauthorized person. This information may include sensitive information such as a credit card number, and only the authorized person can access this information. Integrity is a concept that refers to protecting information and data from being tampered with, distracted from, or modified. The common method used in integrity is encryption to protect data and ensure it has not been changed. Availability refers to the fact that the information is available and the authorized person can access and use it when needed. Distributed Denial of Service (DDoS) is a common attack that blocks access to information resources. Redundancy and backup are methods used to maintain the availability of data [9], [63]. The main differences between IDS and SIEM are explained in Table 3 below:

Table 3 A comparisons between IDS and SIEM

IDS	**SIEM**
Used to identify the threats and attacks that target host devices.	Used to collect the logs from different devices, analyze them, and monitor the status of network infrastructure.
Not able to prevent or mitigate attacks or block the attacks from accessing the target.	Used to detect and make incident responses against threats and attacks that target network

	resources.
Passive tool.	Active tool
Collect the network traffic, detect the attacks according to the signature database or abnormal behavior, and generate the logs.	Collect, normalize, and correlate the logs from multiple devices and applications like routers, switches, antivirus, IDS, IPS, and so on to detect and prevent threats and attacks from having an effect on the network.
It can keep logs and alert the administrator if an attack is detected.	Used to store the logs in a central location for the purpose of forensics and compliance and take the necessary actions (monitor, alerts, and reports) and countermeasures against threats and attacks.
High false positive alerts, which means sometimes traffic is normal but IDS produces an alert. In addition, it's time-consuming.	Used to reduce a false positive.

3.1 SIEM Definitions

There are some definitions of SIEM introduced by many researchers, as explained below:

SIEM solutions are used in order to gather logs produced by security devices, network infrastructure, systems, and applications. The event is combined with contextual information about users, assets, threats, and vulnerabilities, and then it is sent to the SIEM server, where it will be normalized and correlated based on correlation rules and then triggered to identify abnormal and suspicious activities [61], [67]. The term SIEM was presented by Gartner in 2005, as illustrated in figure 4 below [33], [58].

SIEM is used to process the logs generated from various resources for analysis and address the complexity of the collection and normalization of logs. [21], [68], [69].

SIEM is a combination of security information management (SIM) and security event management (SEM) functions into one security management system [63], [65], [70].

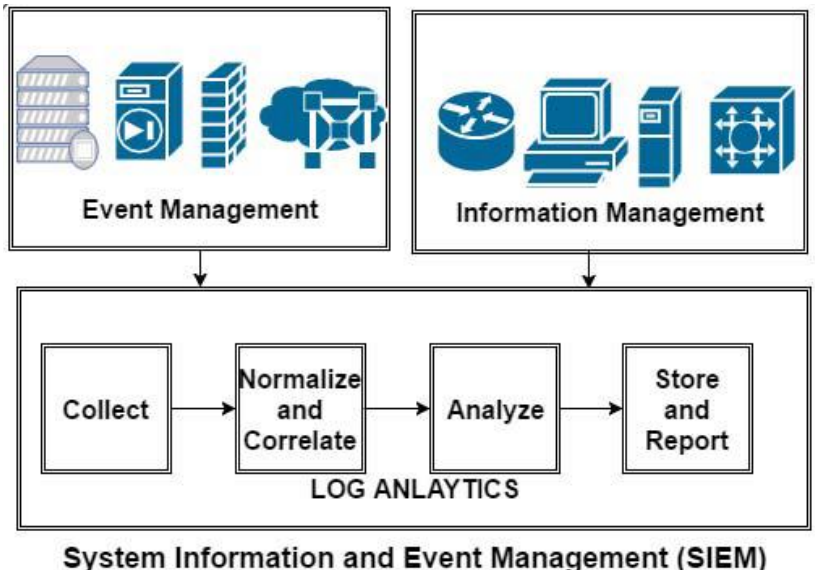

Figure 4 SIEM architecture [70].

SIM is used to collect events in a central repository for analysis and manipulation, and it provides automated and centralized reporting of the collected data from log files for compliance [32], [58]. While SEM focuses on storage management, correlation of events, notifications, and consoles, it also enables real-time monitoring and functionality in a single security management system [20], [22], [71]. For instance, when a problem is detected, SIEM may log it as new information, generate an alert, and instruct other security controls to stop the progress of any activity [61].

SIEM systems are a powerful tool for preventing, detecting, and responding to cyberattacks [24], [72]. It mainly consists of separate processes to assist security staff in detecting threats and abnormal events in order to monitor and analyze network infrastructure. SIEM components include the source device, log collection, log normalization, correlation engine, log storage, and event monitoring that operate independently of each other, but without all of them working together, the SIEM will not function properly [5], [6], [27], [72].

Source devices represent the source that generates the logs, such as network devices like: (routers and switches), security software and appliances like (antivirus, IDS, IPS, and firewalls), applications, systems, and end-user devices [5], [33]. where the logs are gathered and sent to a central location for analysis and storage [27], [73], [74].

Log collection represents the process of collecting logs that are generated by the source devices and forwarding them to the central location, which is SIEM. A collector could be an agents, agentless, or hybrid between them [61], [75]. Log collection consists of push and pull methods [5].

The push method means the source devices, like routers and switches, directly send the logs to the SIEM, which is called the agentless method because it cannot install the agent inside these devices. While the pull method means that SIEM connects to the source devices to extract the logs using agents that are installed on the source devices and send logs to the SIEM, which is called the agent method [5], [33].

Normalizing the collected logs and processing them in their raw form is a difficult process; for that reason, the normalizing and parsing process is used to convert the logs into a unique format. Normalization is the process used to change the various types of log formats generated from different source devices and applications into a

single standard format that is readable by analysts to simplify the rules because each source has its own format [5], [76].

A rule engine is used to trigger alerts on normalized logs inside SIEM according to specified conditions in the logs. Alerts that match a certain rule indicate that a threat is occurring. Rules are written using Boolean logic to identify if specified conditions are matched inside data fields in order to analyze incidents and detect threats in real time [5], [73].

The correlation engine represents the main part of the SIEM system. It is used to match several specified events produced from different resources that were generated by the rules engine and correlate them with a single alert using different methods that can be created by analysts and experts or extracted from another organization in order to monitor the network and detect suspicious actions and unknown threats in real time, like suspicious login attempts [5], [27], [76].

In the log storage process, the logs that are processed within SIEM are stored in various formats (database, text file, and binary file), which can be accessed at any time for historical search and forensics, where a forensic process is performed on logs that are stored within SIEM for historical investigation in order to discover unknown attacks to be presented as legal evidence or regularity compliance. The logs can be stored in an encrypted format for the purpose of increasing security and reliability and ensuring that records are not tampered with during storage [5].

SIEM systems provide real time analysis of events produced by devices and applications in the network and the ability to respond by identifying and deploying countermeasures to threats [6], [77], [78]. In the monitoring process, analysts can interact with and manage the SIEM system to provide a unique perspective on the status of the organization. Also, the analysts can identify the threats and make decisions to determine whether they are false positives or normal traffic. In addition, during the monitoring, the analysts can generate reports to inform the administrator of the organization about the status of network infrastructure, for the purpose of threat intelligence, to exchange information about threats and attacks with other organizations, and for the purpose of regulatory compliance because some countries have rules for reporting information about incidents and attacks that have occurred against the organizations. In addition, SIEM is used to produce reports for regulatory compliance [79], [80]. Also, SIEM can send an alert when incidents occur to the administrator using email or SMS [60], [81]. Figure 5 shows the basic components of SIEM.

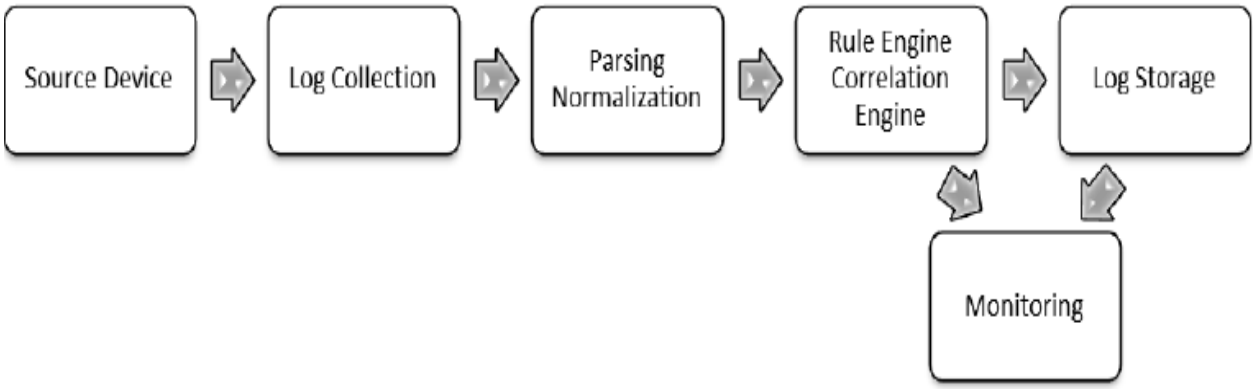

Figure 5 SIEM basic components [5]

Most SIEM systems work by deploying multiple collection agents (collectors) to gather security events from end devices, servers, network equipment, and even specialized security like firewalls, antivirus, IDS, or IPS. The log collectors forward events to a centralized management console, which performs inspections and flags anomalies, while agentless means that the source of the event transmits its logs directly to SIEM. After the process of collecting logs, the data needs to be normalized so that it can be correlated and analyzed. It is also possible to filter the logs associated with the processing center, as a preprocessing mechanism is used in edge collectors, with only certain events allowed to pass over a central management node. In this method, the amount of information being connected and stored can be diminished. The SIEM technique offers real-time correlation of events for the purpose of security monitoring, inquiry, and historical analysis and provides other support for event investigation, compliance reporting, alerting, and alarming as a result of the correlation of multiple alerts [58], [82].

3.2 SIEM Capability

There are different capabilities of SIEM tools, which are [5], [71]:

- Real-time security monitoring includes the storage of logs in a central location, log correlation for the purpose of real time analysis, and generating alerts when suspicious actions or attacks occur to take countermeasures.

- Cyber threat intelligence: provides information and knowledge on unusual threats and attacks that happened on an organization and shares the information with other organizations to reduce the impact of the external threats and attacks that target it.

- Data and user monitoring: monitor the authentication and authorization of the user. After authentication, it will check for any access or alteration to files. It

shouldn't be done, and it generates alerts when any suspicious action occurs. It represents one of the requirements for compliance reporting.

- Application monitoring: attacks are carried out by exploiting weaknesses in an application, such as bugs and vulnerabilities, where the ability to parse activities allows for monitoring applications.

- Analytics: used to detect, analyze, and communicate for the purpose of security analysis, it consists of dashboard views, reports, and query functions. It is used for the investigation of activities to define threats and attacks.

- Regularity compliance represents one of the problems that face building the SIEM system. Regularity compliance depends on the policies and rules of countries and organizations to keep the sensitive information of individuals secure and prevent any unauthorized access to it. Regularity compliance like HIPAA and PCI is used to identify how the logs are stored, what type of logs are needed to be stored, and how many times they are needed to be stored for the purpose of investigation and forensics. For that reason, SIEM is used to provide reports for the purpose of regulatory compliance, where failure to meet these requirements can lead to catastrophic results.

- Log management and reporting: Log management is used for the purpose of simplifying compliance processes when SIEM techniques contain predefined and customizable reports for user action, resource access, and model reports for specific regulations. The functions that facilitate the gathering, indexing, and storage of all log and event data from each source and the capacity to search and report on that data are essential for the massive information store's cost-effective analysis and storage. Predefined reports, the capacity to create custom reports, and the use of third-party reporting tools should all be included in the reporting capabilities.

3.3 SIEM Solutions

SIEM is used for real-time analysis of the events and alerts produced by network devices and applications. Also, it can be applied as software or hardware and produce reports for regulatory compliance [32]. The main goal of the SIEM is to assist organizations in monitoring events, analyzing huge amounts of data, and responding to threats.

3.4 Functionality of SIEM:

SIEM provides the following functionality [5], [32]:

- Event correlation: collect logs, store, normalize, and correlate alerts for incident response and forensics.
- Situation detection: monitoring the network behavior and detection of unwanted and suspicious activities such as anomaly detection methods and configuration management.
- Identity mapping: identify specific information for network users such as IP or MAC addresses.
- Key performance indication: analyze asset details centrally for the purpose of security measurement.
- Compliance reporting: is used to check information technology compliance, such as information integrity, risk management, effectiveness of an organization, and comparison to the real situation.
- Application programming interface (API): is used to provide an interface for the purpose of integration with various systems.
- Role based access control: provide a central view of all events that occurred within the network under consideration of different responsibilities.

3.5 SIEM Vendors

For the purpose of assisting administrators in planning security policies and managing incidents from various resources, SIEM systems have been designed [5], [62]. There are many SIEM systems in the market that have the main capabilities, but there are differences between these systems, as companies have developed special software for SIEMs for the purpose of detecting threats and anomalies in the network infrastructure, such as HP, McAfee, IBM, AlienVault, and Splunk [5], [6], [62]. Some of the commercial and open-source SIEM solutions are explained below:

1. Commercial SIEM

Commercial SIEM is used by organizations to gain powerful capabilities and simplify their use [95].

1. **SPLUNK** is one of the leading commercial SIEM tools introduced by Splunk Enterprise Security, as it includes an easy interface for the purpose of monitoring, researching, understanding, and identifying violations and anomalies within the network, thus facilitating defensive measures and incident response such as alerts to notify the administrator or preventing unauthorized access to the system and helping to protect the network infrastructure. Splunk is used for the purpose of collecting and organizing data in different fields. This

allows for easy search and identification of abnormal behavior and a high level of investigation of the events [83], [84].

2. **QRadar** is a commercial SIEM solution introduced by IBM Security for the purpose of detecting abnormal behaviors and taking incident response actions to mitigate their impact. It is capable of monitoring the high number of applications and devices in the network [85].

3. **McAfee** Enterprise Security Manager is used to detect threats and manage activity related to producing reports in real time and ensuring compliance. It includes a user interface to monitor and deal with incidents. It is used to collect and analyze logs from various resources and generate alerts when incidents occur [86].

4. **LogRhythm** is a commercial SIEM that includes many analysis tools and also uses artificial intelligence and log correlation to enhance detection capabilities, reduce false positive-alerts, and minimize response time [87].

5. **NetWitness** is a commercial SIEM introduced by RSA that uses an open XDR to get the functionality of an artificial intelligent approach for the purpose of detecting and responding to incidents. It is used to collect and analyze logs from various resources and can be used on different platforms, such as physical or virtual [88].

6. **Azure Sentinel** is a SIEM solution from Microsoft releasing in 2019. It is used to collect, detect, investigate, and respond to events, which provide the basic requirements for small and medium organizations [89].

7. **ArcSight** is a SIEM system produced by ArcSight Enterprise Security Manager. It is easy to deploy and maintain and provides essential features like log correlation, action triggers, and log normalization [90].

2. Open Source SIEM

Open source SIEM is used by organizations to minimize the cost of software licenses and assess certain capabilities, which offers essential functionality to small companies that begin to log and analyze security incidents [91].

1. **OSSIM** is an open-source SIEM presented by AlienVault. It is used to detect threats and attacks in real time based on AlienVault's Open Threat Exchange. It is used to merge log storage and correlation features for the purpose of building SIEM. The users faced the problem that they were unable to manage the logs for large enterprises [92].

2. **Wazuh** is an open-source security monitoring system. It is used to collect, correlate, and store the logs. It has important security features such as intrusion and vulnerability detection, incident response, and threat prevention [93].

3. **Prelude** is a SIEM system that is used to collect and analyze logs from various resources. Also, it is used to correlate logs, generate alerts to notify administrators when incidents are occurring, and store logs in a single location [94].

4. **Apache** Metron is a SIEM system released in 2016. It is used to process and store large amounts of data to detect and respond to attacks and threats. It offers essential functionality like log collection, analysis, indexing, and storage [95].

5. **Splunk Free** is a free SIEM version of Splunk Enterprise that is used by users to collect, analyze, and store logs. It is used to store 500 MB per day of data or loss, which is used by Splunk for the purpose of forensics. It has many restrictions, making it not useful for long-term solutions [84].

3.6 Commercial SIEM Classification:

According to Gartner's SIEM Magic Quadrant annual report, SIEM solutions are classified as leaders, challengers, niche players, or visionaries based on the market and major vendors, as explained in Table 4 [6], [83]. Table 4 displays the progress of SIEM solutions for the period 2010 - 2020 [4].

TABLE 4 SIEM vendors Classification [4].

SIEM Vendor	2010	2011	2012	2013	2014	2015	2016	2017	2018	2020
HP/ArcSight/HPE [24]	★	★	★	★	★	★	★	♦		
RSA/EMC [25]	★	★	♦	♦	♦	♦	♦	♦	★	★
SenSage [26]	★	■	▲	▲						
LogLogic [27]	★	★	♦							
Symantec [28]	★	★	♦	♦						
Q1Labs [29]	★	★	★	★						
Novell [30]	★	★	★							
IBM [31]	♦	♦	★	★	★	★	★	★	★	★
Quest Software [32]	♦	♦								
CA [33]	♦									
Tenable [34]	▲	■	▲	▲	▲					
Prism Microsystems [35]	▲	■	▲							
LogMatrix [36]	▲									
NetIQ/Microfocus [37]	■	▲	★	♦	♦	▲	▲	▲	♦	▲
McAfee/Intel [38]	■	★	★	★	★	★	★	★	★	▲
Trustwave [39]	■	■	■	▲	▲	▲	▲	▲		
LogRhythm [40]	■	■	★	★	★	★	★	★	★	★
TriGeo [41]	■	■								
netForensics [42]	■	■								
eIQnetworks [43]	■	■	■	▲						
Splunk [44]		▲	♦	★	★	★	★	★	★	★
Tripwire [45]		▲								
AlienVault/ AT&T		▲	■	■	■	■	■	▲	▲	▲
Cybersecurity [46]										
Correlog [47]		▲	▲							
S21sec [48]		▲	▲							
Tango/04 [49]		▲	▲							
Tier-3 [50]		■	■							
SolarWinds [51]			■	♦	▲	▲	▲	▲	▲	▲
Tibco-LogLogic [52]				■	♦					
EventTracker [53]				▲	▲	▲	▲	▲	▲	
AccelOps/Fortinet [54]					▲	▲	▲	▲	▲	▲
Blackstratus [55]					▲	▲	▲	▲	▲	
Manage Engine [56]							▲	▲	▲	▲
FireEye [57]								▲		▲
Venustech [58]								▲	▲	
Rapid7 [59]								■	■	★
Exabeam [60]								■	★	★
Securonix [61]								■	★	★
LogPoint [62]									▲	■
HanSight [63]										▲

★ Leader ♦ Challenger ▲ Niche Player ■ Visionary.

From Table 4, the symbol (*) refers to the leaders of the market, challengers are specified with a (◊), niche players are specified with a Δ, and visionaries are specified with a (□).

Magic quadrants evaluate products in the market depending on a set of criteria that represent the ability to implement and the completeness of the vision.

The ability to implement refers to the economic strength of a vendor to perform the relevant functions, while completeness of vision is the ability to understand current and future market needs [6], [29], [83].

Leaders mean that the SIEM solution has both high abilities to implement and completeness of vision of the market, while challengers have high abilities to implement but a limited vision of the market's direction. Visionaries mean that the SIEM solution has a good vision of the market but has no competitive ability to implement it, while Niche players focus on a small segment of the market and have limited implementation abilities [83]. Figure 6 represents the Magic Quadrant annual report, which evaluates products on the market during 2022.

Figure 6 Magic quadrants for SIEM classification in the market in 2022 [83].

4. Related Works

In 2014, (Anastasov and Davcev) introduced a method that used the ArcSight ESM SIEM system called the Hierarchical Managers Model using multiple hierarchical SIEM managers. It consists of three layers, which are: The first layer included source devices that generate raw logs. While, the second layer included multiple servers, which means centralized systems that are collecting the original logs from the log sources and are used to merge and store the logs in the log storage. The third layer is

used for the purpose of monitoring and consists of user devices that are used to monitor and review the logs and manage the servers from the second layer. The purpose of this method is to make data management easier to implement by distributing the load, which reduces network overhead [67]. In 2014, (Gao et al) produced a method for IDS that used deep belief networks (DBN) as a classifier with Boltzmann machines for training and back propagation for the KDD Cup 99 dataset [96]. (Anumol) proposed an open-source security information management (OSSIM), to perform the event analysis in 2015. It is used to protect the network through log correlation and management. A support vector machine (SVM) is used for the purpose of processing all normalized data and classification. The main purpose of this method is to decrease the high false positive rate, centralize the event analysis, and produce an effective report through the correlation process [25]. In 2016, (Gharaee and Hosseinvand) introduced IDS that used a genetic algorithm and support vector machine (SVM) for selecting features to improve true positive alerts and reduce false positive alerts [97]. In 2018, (Chakir et al) proposed a method to select NSL-KDD dataset features depending on support vector machine (SVM) with radial-basis kernel function (RBF). In addition, for the purpose of optimizing features selected by SVM, a particle swarm optimization (PSO) algorithm was used [98]. In 2019, (Suhaimi et al) proposed a method using a genetic algorithm to improve feature selection for the purpose of detecting malicious activities within the network. Here, various features were analyzed to produce a ruleset of classification based on the KDD Cup 99 dataset [99]. In 2019, (LEE et al) presented an AI-SIEM based on artificial neural network techniques for the detection of cyber threats. The proposed technique converts a multitude of collected security events into individual event profiles and uses a deep learning-based detection method for improved cyber threat detection. The purpose of this method is to reduce false positive alerts, thus helping security analysts rapidly respond to cyber threats [100]. (Halimaa and Sundarakantham) introduced the IDS method in 2019. In this method, support vector machine (SVM) and naïve bayes are utilized to improve the classification of network traffic, and NSL– KDD dataset is used to assess IDS. The results depict that the SVM is better than Naïve Bayes according to the accuracy of traffic classification [101]. In 2020, (Wang et al) proposed a method for anomaly detection using the k-nearest neighbor (KNN) method to select the good neighbor, which consists of three parts, which are minhash and MVP-tree, which are used to search for neighbors, and after that, k neighbors are used for automatic selection [102]. In 2020, (Moukafih et al) present a SIEM system based on a reliability approach, which is feedforward neural networks, and generate high detection capability with low computation resources. The goal is to improve the detection capability within a SIEM system in order to overcome the increasing number of attacks using sophisticated and complex methods to infiltrate systems [24]. In 2021, (Sulaiman et al) present a way of providing centralized log analysis between network devices. Also, it introduces a method for gathering and displaying all potential threats and alert information on a single dashboard using a deep learning

approach. The purpose of this method is to provide centralized log analysis [27]. In 2022, (Akande et al) suggest an approach for anomaly detection using thresholds to differentiate between normal and malicious traffic, according to the Hadoop Distributed File System (log dataset) [103]. In 2022, (Coppolino et al) presented a method to provide effective protection of critical business processes by applying the SIEM method, based on two techniques for trusted computing, namely: Trusted Execution Environment (TTE) and Homomorphic Encryption (HE) depending on the risk assessment results. The purpose of this method is to effectively protect the critical workflows of hospital business processes from cyberattacks with high impact [104]. In 2022, (Gupta et al) introduced a method using SIEM for digital forensics. The purpose of this paper is to minimize the analysis time during an attack by obtaining only the required data in real-time without affecting the victim's machine during business hours and also transferring only the essential information for analysis, which reduces network overhead and transfer time [105].

5. Conclusion:

Network security systems are an important field in cybersecurity. It is used to detect and prevent threats and attacks that target the network infrastructure by detecting, analyzing, and monitoring the resources of the network and taking countermeasures against the suspicious activity. There are many methods used in network security, such as antivirus, firewalls, intrusion detection systems, and intrusion prevention systems, but these tools work independently and will provide a lot of false positive alerts. For that reason, the SIEM system was introduced to provide a central location for monitoring the network environment. In this paper, an overview of network security systems is introduced. In addition, this paper focuses on explaining the popular security method and its functionality and capabilities. The limitations of this paper are that the topic of network security is too big and it cannot cover all the aspects related to this topic, in addition to consuming a lot of time for the purpose of gathering relevant references and writing this paper.

6. References

[1] Mueller, P. and Yadegari, B., "The Stuxnet Worm," *The university of Arizona* 2012.

[2] Podzins, O. and Romanovs, A., "Why SIEM is Irreplaceable in a Secure IT Environment?,," presented at *the 2019 Open Conference of Electrical, Electronic and Information Sciences (eStream)*, Vilnius, Lithuania, 2019.

[3] Lif, P., Varga, S., Wedlin, M., Lindahl, D., and Persson, M., "Evaluation of Information Elements in a Cyber Incident Report," in *IEEE European S)ymposium on Security and Privacy Workshops (EuroS&PW*, Genoa, Italy, pp. 17-26, 2020.

[4] González-Granadillo, G., González-Zarzosa, S. and Diaz, R., "Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures," *sensor* vol. 21, 2021.

[5] Miller, D., Harris, S., Harper, A., Van Dyke, S. and Blask, C., *Security Information and Event Management (SIEM) Implementation*. 2010: Mc Graw Hill: New York, NY, USA 2010.

[6] Granadillo, G., El-Barbori, M. and Debar, H., "New types of Alert Correlation for Security Information and Event Management Systems," in *8th International Conference on New Technologies, Mobility and Security, NTMS*, Larnaca, Cyprus, 2016.

[7] Muhammad, R., Irawati, I. and Iqbal, M., "Integrated Security System Implementation for Network Intrusion," *Hunan University（Natural Sciences）*, vol. 48, 2021.

[8] Talukder S. and Talukder, Z., "A Survey on Malware Detection and Analysis Tools," *International Journal of Network Security & Its Applications (IJNSA)*, vol. 12, pp. 37-57, 2020.

[9] Kim, J. and Kwon, H., "Threat classification model for security information event management focusing on model efficiency," *Computers and Security*, vol. 120, 2022.

[10] Rapid7.*Prevention vs Detection, Rebalancing YourSecurity Program*. Available: https://www.rapid7.com/resources/prevention-vs-detection/, (2015).

[11] Carklin, N., (2022, 23 Dec 2022). *Network Security Monitoring: A Complete Guide*. Available:https://www.parallels.com/blogs/ras/network-security-monitoring/#:~:text=Network%20security%20monitoring%20is%20an,respond%20to%20cybersecurity%20breaches%20quickly

[12] Ahmad, Z., Khan,A., Shiang, C. and Ahmad, F., "Network intrusion detection system: A systematic study of machine learning and deep learning approaches," *Transactions on Emerging Telecommunications Technologies*, vol. 32, 2022.

[13] Camacho, J., Maciá-Fernández, G., Verdejo, J. and García-Teodoro, P., "Tackling the big data 4 vs for anomaly detection," presented at the IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS), Toronto, ON, Canada, 2014.

[14] Mokalled, H., Catelli, R., Casola, V., Debertol, D., Meda, E. and Zunino, R., "The applicability of a SIEM solution: Requirements and Evaluation," presented at the IEEE 28th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), Napoli, Italy, 2019.

[15] Jeonga, C., TomLeeb, S. and Lim, J., "Information security breaches and IT security investments: Impacts on competitors," *Information and Management*, vol. 56, pp. 681-695, 2019.

[16] Irfan, M., Abbas, H. and Iqbal, W., "Feasibility analysis for incorporating/deploying SIEM for forensics evidence collection in cloud environment," presented at the IEEE/ACIS 14th International Conference on Computer and Information Science (ICIS), Las Vegas, NV, USA, 2015.

[17] Miloslavskaya, N., *Analysis of SIEM Systems and Their Usage inSecurity Operations and Security Intelligence Centers*: Springer, Cham, 2017.

[1] P. Mueller and B. Yadegari, "The Stuxnet Worm," The university of Arizona, The university of Arizona2012.

[2] O. Podzins and A. Romanovs, "Why SIEM is Irreplaceable in a Secure IT Environment?,," presented at the 2019 Open Conference of Electrical, Electronic and Information Sciences (eStream), Vilnius, Lithuania, 2019.

[3] P. Lif, S. Varga, M. Wedlin, D. Lindahl, and M. Persson, "Evaluation of Information Elements in a Cyber Incident Report," in *IEEE European S)ymposium on Security and Privacy Workshops (EuroS&PW*, Genoa, Italy, 2020, pp. 17-26.

[4] G. González-Granadillo, S. González-Zarzosa, and R. Diaz, "Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures," *sensor* vol. 21, 2021.

[5] D. Miller, S. Harris, A. Harper, S. Van Dyke, and C. Blask, *Security Information and Event Management (SIEM) Implementation*. 2010: Mc Graw Hill: New York, NY, USA

2010.

[6] G. Granadillo, M. El-Barbori, and H. Debar, "New types of Alert Correlation for Security Information and Event Management Systems," in *8th International Conference on New Technologies, Mobility and Security, NTMS*, Larnaca, Cyprus, 2016.

[7] R. Muhammad, I. Irawati, and M. Iqbal, "Integrated Security System Implementation for Network Intrusion," *Hunan University（Natural Sciences）*, vol. 48, 2021.

[8] S. Talukder and Z. Talukder, "A Survey on Malware Detection and Analysis Tools," *International Journal of Network Security & Its Applications (IJNSA)*, vol. 12, pp. 37-57, 2020.

[9] J. Kim and H. Kwon, "Threat classification model for security information event management focusing on model efficiency," *Computers and Security*, vol. 120, 2022.

[10] Rapid7. (2015). *Prevention vs Detection, Rebalancing YourSecurity Program*. Available: https://www.rapid7.com/resources/prevention-vs-detection/

[11] N. Carklin. (2022, 23 Dec 2022). *Network Security Monitoring: A Complete Guide*. Available: https://www.parallels.com/blogs/ras/network-security-

monitoring/#:~:text=Network%20security%20monitoring%20is%20an,respond%20to%20cybersecurity%20breaches%20quickly

[12] Z. Ahmad, A. Khan, C. Shiang, and F. Ahmad, "Network intrusion detection system: A systematic study of machine learning and deep learning approaches," *Transactions on Emerging Telecommunications Technologies*, vol. 32, 2022.

[13] J. Camacho, G. Maciá-Fernández, J. Verdejo, and P. García-Teodoro, "Tackling the big data 4 vs for anomaly detection," presented at the IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS), Toronto, ON, Canada, 2014.

[14] H. Mokalled, R. Catelli, V. Casola, D. Debertol, E. Meda, and R. Zunino, "The applicability of a SIEM solution: Requirements and Evaluation," presented at the IEEE 28th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), Napoli, Italy, 2019.

[15] C. Jeonga, S. TomLeeb, and J. Lim, "Information security breaches and IT security investments: Impacts on competitors," *Information and Management*, vol. 56, pp. 681-695, 2019.

[16] M. Irfan, H. Abbas, and W. Iqbal, "Feasibility analysis for incorporating/deploying SIEM for forensics evidence collection in cloud environment," presented at the IEEE/ACIS 14th International Conference on Computer and Information Science (ICIS), Las Vegas, NV, USA, 2015.

[17] N. Miloslavskaya, *Analysis of SIEM Systems and Their Usage inSecurity Operations and Security Intelligence Centers*: Springer, Cham, 2017.

[18] B. Bryant and H. Saiedian, "A novel kill-chain framework for remote security log analysis with SIEM software," *Computers and Security*, vol. 67, pp. 198-210, 2017.

[19] Y. Chen and B. Malin, "Detection of Anomalous Insiders in Collaborative," in *1st ACM conference on Data and application security and privacy, ACM*, 2011, pp. 63-74.

[20] H. Mokalled, C. Pragliola, D. Debertol, E. Meda, and R. Zunino, *A Comprehensive Framework for the Security Risk Management of Cyber-Physical Systems*: Springer, Cham, 2019.

[21] M. Cinque, D. Cotroneo, and A. Pecchia, "Challenges and Directions in Security Information and Event Management (SIEM)," in *International*

Symposium on Software Reliability Engineering Workshops., Memphis, TN, USA, 2018.

[22] S. Sekharan and K. Kandasamy, "Profiling SIEM Tools and Correlation Engines for Security Analytics," in *International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, Chennai, India, 2017.

[23] J. Velásquez, S. Monterrubio, L. Crespo, and D. Rosado, "Systematic review of SIEM technology: SIEM-SC birth," *International Journal of Information Security*, 2023.

[24] N. Moukafih, G. Orhanou, and S. Elhajji, "Neural Network-Based Voting System with High Capacity and Low Computation for Intrusion Detection in SIEM/IDS Systems," *Security and Communication Networks, Hindawi,*, 2020.

[25] E. Anumol, *Use of Machine Learning Algorithms with SIEM for Attack Prediction* vol. 308. Springer, New Delhi, India: Springer, 2015.

[26] A. Khan, R. Khan, and F. Nisar, "Novice threat model using SIEM System for Threat Assessment," in *2th International Conference on Communication Technologies*, Rawalpindi, Pakistan, 2017, pp. 72-77.

[27] M. Sulaiman, M. Ismail, M. Khairuddin, M. Shukran, M. Isa, and A. Sajak, "SIEM Network Behaviour Monitoring Framework using Deep Learning Approach for Campus Network Infrastructure," *International Journal of Electrical and Computer Engineering Systems*, 2021.

[28] I. Ahmed and M. Kashmoola, "Threats on Machine Learning Technique by Data Poisoning Attack: A Survey," presented at the Advances in Cyber Security Communications in Computer and Information Science, Singapore, 2021.

[29] M. Fuentes-García, J. Camacho, and G. Maciá-Fernández, "Present and Future of Network Security Monitoring," in *IEEE Access*, 2021, pp. 112744-112760.

[30] S. Salah, G. Maciá-Fernández, and E. Díaz-Verdejo, "A model-based survey of alert correlation techniques," *Computer Network*, vol. 57, p. 1289_1317, 2013.

[31] M. Collins and O. Media, *Network Security Through Data Analysis: Building Situational Awareness*. CA, USA: O'Reilly, 2014.

[32] K. Detken, T. Rix, C. Kleiner, B. Hellmann, and L. Renners, "SIEM Approach for a Higher Level of IT Security in Enterprise Networks," in *8thIEEE*

International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, Warsaw, Poland., 2015.

[33] M. Vielberth and G. Pernul, "A Security Information and Event Management Pattern," in *12th Latin American Conference on Pattern Languages of Programs*, 2018.

[34] R. Bace, *Intrusion Detection (Technology Series).* New York, NY, USA: Macmillan Technical Publishing, 2000.

[35] J. Jiménez. (2019, 25 Dec 2022). *How to see the information that Windows Defender stores from the analyzes made*. Available: https://bit.ly/2Nwym0r

[36] H. Panwala, "A Methodological Study on Malware Analysis," *International Journal for Research in Applied Science & Engineering Technology (IJRASET)* vol. 9, pp. 450-453, 2021.

[37] G. Lyon. (1997, 17 Dec 2022). *Nmap Network Mapper*. Available: https://nmap.org/

[38] R. Bhardwaj. (2022, 25 Dec 2022). *IDS vs IPS vs Firewall – Know the Difference*. Available: https://ipwithease.com/firewall-vs-ips-vs-ids/

[39] M. Mazinia, B. Shirazib, and I. Mahdavib, "Anomaly network-based intrusion detection system using a reliable hybrid artificial bee colony and AdaBoost algorithms," *Journal of King Saud University - Computer and Information Sciences*, vol. 31, pp. 541-553, 2019.

[40] M. Mahmood, "Hybrid Fuzzy Logic and Artificial Bee Colony Algorithm for Intrusion Detection and Classification," *Iraqi Journal of Science*, vol. 57, pp. 241-252, 2016.

[41] B. Farhan and A. Jasim, "Survey of Intrusion Detection Using Deep Learning in the Internet of Things," *Iraqi Journal for Computer Science and Mathematics*, vol. 3, pp. 83-93, 2022.

[42] M. Mahmod, Z. Alnaish, and I. Al-Hadi, "Hybrid Intrusion Detection System Using Artificial Bee Colony Algorithm and Multi-Layer Perceptron," *International Journal of Computer Science and Information Security,*, vol. 13, 2015.

[43] I. Ahmed, "Enhancement of network attack classification using particle swarm optimization and multi-layer perceptron," *International Journal of Computer Applications*, vol. 137, pp. 18–22, 2016.

[44] T. Lewis. (2022). *IDS and IPS 101: How Each System Works and Why You Need Them*. Available: https://www.lbmc.com/blog/ids-vs-ips/

[45] P. Udas, E. Karim, and K. SankarRoy, "SPIDER: A shallow PCA based network intrusion detection system with enhanced recurrent neural networks," *Journal of King Saud University - Computer and Information Sciences,* vol. 34, pp. 10246-10272, 2022.

[46] W. Liang, K. Li, J. Long, X. Kui, and A. Zomaya, "An Industrial Network Intrusion Detection Algorithm Based on Multifeature Data Clustering Optimization Model," presented at the Transactions on Industrial Informatics, 2020.

[47] T. Sreenivasula reddy and R. Sathya, "Ensemble Machine Learning Techniques for Attack Prediction in NIDS Environment," *Iraqi Journal for Computer Science and Mathematics,* vol. 3, pp. 78-82, 2022.

[48] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Survey of intrusion detection systems: techniques, datasets and challenges," *Cybersecur* vol. 2, 2019.

[49] A. Gaurav, B. Gupta, W. Alhalabi, A. Visvizi, and Y. Asiri, "A comprehensive survey on DDoS attacks on various intelligent systems and it's defense techniques," *International Journal of Intellegint Systems,* vol. 37, pp. 11407- 11431, 2022.

[50] D. Jeon and B. Tak, "BlackEye: automatic IP blacklisting using machine learning from security logs. ," *Wireless Networks, Springer,* vol. 28, pp. 937–948, 2022.

[51] P. Radoglou-Grammatikis and P. Sarigiannidis, "Securing the Smart Grid: A Comprehensive Compilation of Intrusion Detection and Prevention Systems," presented at the IEEE ACCESS, 2019.

[52] F. Zhang, H. Kodituwakku, J. Hines, and J. Coble, "Multilayer Data-Driven Cyber-Attack Detection System for Industrial Control Systems Based on Network, System, and Process Data," presented at the Transactions on Industrial Informatics, 2019.

[53] J. Suroso and C. Prastya, "Cyber Security System With SIEM And Honeypot In Higher Education," in *IOP Conf. Series: Materials Science and Engineering* 2020.

[54] H. Mohamed, L. Adil, T. Saida, and M. Hicham, "A collaborative intrusion detection and Prevention System in Cloud Computing," in *IEEE*, Pointe aux Piments, Mauritius, 2013, pp. 1-5.

[55] (2022). *Snort tool*. Available: https://www.snort.org/products

[56] (2022, 5 Jan 2023). *Suricata tool*. Available: https://suricata.io/

[57] N. Lukova-Chuiko, A. Fesenko, H. Papirna, and S. Gnatyuk, "Threat Hunting as a Method of Protection Against Cyber Threats," in *7th International Conference of Information Technology and Interactions*, 2021.

[58] (2019). *Cyber Threat Alliance.* Available: https://www.cyberthreatalliance.org/

[59] B. Alahmadi, A. L;, and I. Martinovic, "99% False Positives: A Qualitative Study of SOC Analysts' Perspectives on Security Alarms," in *31st USENIX Security Symposium*, Boston, MA, USA, 2022.

[60] J. Stoltzfus. (2022, 5 Jan 2023). *What's the difference between SEM, SIM and SIEM?* Available: https://www.techopedia.com/7/31201/security/whats-the-difference-between-sem-sim-and-siem.

[61] D. Kelley, "Report: Security Management Convergence via SIM (Security Information Management) — A Requirements Perspective," *Journal of Network and Systems Management* vol. 12, 2004.

[62] H. Mokalled, R. Catelli, V. Casola, D. Debertol, E. Meda, and R. Zunino, "The Guidelines to Adopt an Applicable SIEM Solution," *Information Security*, vol. 11, pp. 46-70, 2020.

[63] A. Pecchia, D. Cotroneo, and R. Ganesan, "Filtering security alerts for the analysis of a production saas cloud," in *IEEE/ACM 7th International Conference on Utility and Cloud Computing (UCC)*, 2014, pp. 233-241.

[64] S. Radu, *Comparative Analysis of Security Operations Centre Architectures; Proposals and Architectural Considerations for Frameworks and Operating Models*. Springer International Publishing, Cham, 2016.

[65] A. Serckumecka, I. Medeiros, B. Ferreira, and A. Bessani, "SLICER: Safe Long-Term Cloud Event Archival," in *24th Pacific Rim International Symposium on Dependable Computing (PRDC),*, Kyoto, Japan, 2019.

[66] S. Bhatt, P. Manadhata, and L. Zomlot, "The Operational Role of Security Information and Event Management Systems," in *IEEE Security and Privacy*, 2014, pp. 35–41.

[67] A. Skendžić, B. Kovačić, and B. Balon, "Management and Monitoring Security Events in a Business Organization - SIEM system," in *45th Jubilee International Convention on Information, Communication and Electronic Technology (MIPRO)*, Opatija, Croatia, 2022, pp. 1203-1208.

[68] I. Anastasov and D. Davcev, "SIEM implementation for global and distributed environments," in *World Congress on Computer Applications and Information Systems (WCCAIS)*, 2014, pp. 1-6.

[69] L. Rikhtechi, V. Rafeh, and A. Rezakhani, "Secured Access Control in Security Information and Event Management Systems," pp. 67 - 78, 2021.

[70] V. Sizov and D. Kirov, "Problems of implementing SIEM systems in the practice of managing information security of economic entities," *Open Education*, vol. 24, pp. 69-79, 2020.

[71] K. Sornalakshmi, "Detection of DoS attack and Zero Day Threat with SIEM," presented at the IEEE International Conference on Intelligent Computing and Control Systems ICICCS, 2017.

[72] K. Agrawal and H. Makwana, "A Study on Critical Capabilities for Security Information and Event Management," *International Journal of Science and Research (IJSR)*, vol. 4, 2015.

[73] G. Suarez-Tangil, E. Palomar, A. Ribagorda, and I. Sanz, "Providing SIEM systems with self-adaptation," *Information Fusion*, vol. 21, pp. 145-158, 2015.

[74] T. Laue, T. Klecker, C. Kleiner, and K. Detken, "A SIEM Architecture for Advanced Anomaly Detection," *Open Journal of Big Data (OJBD)* vol. 6, 2022.

[75] A. Zope, A. Vidhate, and N. Harale, "International Journal of Future Computer and Communication," *Data Mining Approach in Security Information and Event Management*, vol. 2, 2013.

[76] A. Gillis. (2022). *Target: Security Information and Event Management (SIEM)* Available: http://searchsecurity.techtarget.com/definition/security-information-and-event-management-SIEM

[77] M. Di Mauro and C. Di Sarno, "Improving SIEM capabilities through an enhanced probe for encrypted Skype traffic detection," *Information Security and Applications*, vol. 38, pp. 85-95, 2018.

[78] V. Vasilyev and R. Shamsutdinov, "Security Analysis of Wireless Sensor Networks Using SIEM and Multi-agent Approach," in *Global Smart Industry Conference (GloSIC)*, Chelyabinsk, Russia, 2020, pp. 291-296.

[79] A. Tariq, J. Manzoor, M. Aziz, Z. Tariq, and A. Masood, "Open source SIEM solutions for an enterprise," *Information and Computer Security*, 2022.

[80] E. Parliament, "DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL," ed, 2016.

[81] S. Eswaran, A. Srinivasan, and P. Honnavalli, "A threshold-based, real-time analysis in early detection of endpoint anomalies using SIEM expertise," *Network Security*, vol. 4, 2021.

[82] M. Alexey, P. Andrey, and P. Andrey, "SIEM-Platform for Research and Educational Tasks on Processing of Security Information Events," presented at the The 15th International Scientific Conference eLearning and Software for Education, Bucharest, 2019.

[83] A. Majeed, R. Rasool, F. Ahmad, M. Alam, and N. Javaid, "Near-miss situation based visual analysis of SIEM rules for real time network security monitoring," *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, pp. 1509–1526, 2019.

[84] Gartner. (2022, 5 Jan. 2023). *Gartner Magic Quadrant*. Available: https://www.gartner.com/en/research/methodologies/magic-quadrants-research

[85] Splunk. (2022, Jan 10, 2023). Available: http://www.splunk.com/

[86] IBMQRADAR. (2022, 25 Dec. 2022). *IBM Security QRadar SIEM*. Available: https://www.ibm.com/qradar/security-qradar-siem

[87] Mcafee. (2022). *Mcafee enterprise security*. Available: https://www.mcafee.com/enterprise/en-us/assets/solution-briefs/sb-enterprise-security-manager.pdf

[88] LogRhythm. (2022, 25 Dec. 2022). *SIEM Solution | Security Information & Event Management | LogRhythm*. Available: https://logrhythm.com/solutions/security/siem/

[89] RSASecurity. (2022, 5 Jan. 2023). *NetWitness Platform – See Everything, Fear Nothing*. Available: https://www.netwitness.com/

[90] Azure. (2022, 5 Jan. 2023). *Microsoft Azure Sentinel* Available: https://azure.microsoft.com/en-us/products/microsoft-sentinel/#overview

[91] arcsight-esm. (2022, 5 Jan. 2023). *arcsight-esm SIEM system*. Available: https://www.microfocus.com/en-us/cyberres/secops/arcsight-esm

[92] SIEM. (2023, 5 Jan. 2023). Available: https://www.coresecurity.com/siem

[93] AT&T/OSSIM. (2022, 5 Jan. 2023). *The Open Source SIEM | AlienVault*. Available: https://cybersecurity.att.com/products/ossim

[94] Wazuh. (2023, 5 Jan. 2023). *The Open Source Security Platform Wazuh* Available: https://wazuh.com/

[95] Prelude. (2022, 5 Jan 2023). *prelude SIEM system*. Available: https://www.prelude-siem.org/

[96] Apache. (2022, 25 Dec. 2022). *Metron Apache SIEM*. Available: https://metron.apache.org/

[97] N. Gao, L. Gao, Q. Gao, and H. Wang, "An Intrusion Detection Model Based on Deep Belief Networks," in *Second International Conference on Advanced Cloud and Big Data*, 2014, pp. 247-252.

[98] H. Gharaee and H. Hosseinvand, "A new feature selection IDS based on genetic algorithm and SVM," in *8th International Symposium on Telecommunications (IST)*, 2016, pp. 139-144.

[99] E. Chakir, M. moughit, and Y. khamlichi, "An effective intrusion detection model based on svm with feature selection and parameters optimization," *Theoretical and Applied Information Technology*, vol. 96, 2018.

[100] H. Suhaimi, S. Suliman, I. Musirin, and A. Harun, " Network intrusion detection system by using genetic algorithm," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 16, pp. 1593-1599, 2019.

[101] J. Lee, J. Kim, I. Kim, and K. Han, "Cyber Threat Detection Based on Artificial Neural Networks Using Event Profiles," in *Artificial Intelligence in Cybersecurity*, 2019.

[102] A. Halimaa and K. Sundarakantham, "Machine Learning Based Intrusion Detection System," in *3rd International Conference on Trends in Electronics and Informatics (ICOEI)*, 2019.

[103] B. Wang, Y. Shi, and Z. Yang, "A Log-Based Anomaly Detection Method with Efficient Neighbor Searching and Automatic K Neighbor Selection " *Sci. Program*, 2020.

[104] T. Akande, B. Kaur, S. Dadkhah, and A. Ghorbani, "Threshold based Technique to Detect Anomalies using Log Files," in *7th International Conference on Machine Learning Technologies (ICMLT'22)* New York, NY, USA, 2022.

[105] L. Coppolino and et al, "Risk Assessment Driven Use of Advanced SIEM Technology for Cyber Protection of Critical e Health Processes," *Springer Nature of Computer Science*, vol. 3, 2022.

[106] R. Gupta and et al, "Automated Data Acquisition in SIEM for Incident Handling Process & Digital Forensics," *Journal of Emerging Technologies and Innovative Research*, vol. 9, 2022.