STRATEGIC MANAGEMENT OF SECURITY EVENTS IN ENTERPRISE ENVIRONMENTS

Maria-Mădălina ANDRONACHE [1,*], Alexandru VULPE [2], Corneliu BURILEANU [3]

Considering the current security environment, in which artificial intelligence is becoming an integrated part of systems, the old ways of protecting computer networks have become ineffective. Although innovations in the field of security are visible, malicious attacks are also on the rise, threatening cybersecurity. This research is based on the current state of network systems, proposing the development of protective measures for closed environments. Thus, through various ways of configuring the network infrastructure and by implementing SIEM agent-manager systems, the aim is to record and block attacks that may arise from ineffective protective measures or malicious intentions of its users.

Keywords: cybersecurity, SIEM, cyberattack, network information security, security measures

1. Introduction

In the era of digitalization of all types of services, in which the technological field has grown exponentially, the number of attacks on the infrastructures that maintain these services has also increased. Thus, if some of these services (which include various online games or various actions carried out for the purpose of relaxation) do not have an enormous impact if they are interrupted (except for financial losses), for critical infrastructures (such as those in the medical or banking fields), an operation that is interrupted, even for a short period of time, has an extremely pronounced impact. If we also become aware of the current security environment, we find that there are unprecedented threats to network infrastructures because systems are increasingly interconnected, requiring robust solutions to prevent attacks. Attacks are also an important topic because, with exponential technological advances, the way in which they adapt more easily to various systems, are harder to detect or cause much more significant damage than in the past has also increased. The advancement of artificial intelligence technologies, although not created for this purpose, contributes to the expansion of these attacks

[1] * Research Institute "CAMPUS", National University of Science and Technology POLITEHNICA Bucharest, Romania, Corresponding author, e-mail: maria.andronache@stud.etti.upb.ro
[2] Telecommunication Department, National University of Science and Technology POLITEHNICA Bucharest, Romania, e-mail: alex.vulpe@radio.pub.ro
[3] Speech and Dialogue Research Lab, National University of Science and Technology POLITEHNICA Bucharest, Romania, e-mail: corneliu.burileanu@upb.ro

or their adaptation to various network environments. Thus, traditional methods of protecting an infrastructure, although resilient, become ineffective in the "fight" with current technologies.

Within network infrastructure, there are various types of attacks. Thus, starting from DoS (Denial-of-Service) or Man-in-the-middle attacks, to phishing or social engineering attacks, all these affect network infrastructures both through temporary unavailability of services and through financial losses.

An important tool for protecting network resources is log capture. According to [1], logs are records of network activity or, in a negative case, of a network incident that occurred at a certain time. The main advantage of this activity is the continuous monitoring of resources and, therefore, the early detection of attacks. Also, if these logs reach a system based on machine learning or artificial intelligence, various traffic patterns or various types of alerts can be created, which lead to the possibility of real-time intervention or automatic blocking of malicious attacks or activities. In article [1], security aspects of the year 2023 are highlighted. Having this basis and comparing it with the data in [2], in the year 2024, the focus is no longer on mobile devices or personal devices of employees, but on the fact that, for the second consecutive year, phishing attacks and attacks based on stolen or compromised credentials are the most used types of attacks. An important graph states that malicious attacks, from the external or internal environment, caused data breaches in 55% of cases, while human errors and poor configurations in the IT (Information Technology) area caused the other 45%. These data are extremely worrying for the current security environment, which leads to the need to constantly develop new methods of protection against any types of attacks or blocking them based on many specific rules.

One of the most important tools for achieving these objectives is provided by SIEM (Security Information and Event Management) systems. They record network logs and detect network intrusions. Furthermore, they can display alerts in real time, which helps with early detection and isolation of a certain part of the network. According to [3], the logs specific to a SIEM are divided into three main categories: system logs, application logs, and security logs. The difference between the three is that system logs track the general operation of devices (starts, stops, updates), application logs track various software errors specific to a particular application, and security logs track access permissions, authorized authentications, or even firewall-related issues.

The paper is proposing a network architecture, used in most business environments, that includes both the datacenter area and the network resource monitoring area. Thus, it integrates both resources such as regular employee devices and integrated network parts such as SIEM systems, which monitor the network infrastructure and intrusions on it. The purpose of this work is to test a network

architecture close to real ones and to see the efficiency of a SIEM system in identifying intrusions within the network, if the attack is carried out from within it.

2. Related work

Most network infrastructures use SIEM systems to acquire and centralize logs within a network. As stated in [4], most SIEM systems have two main components: the agent area, which is responsible for collecting logs, and the management area, which is responsible for centralizing these logs and making various decisions based on them. Similar to the aforementioned work, in this paper, an attack detection system is proposed that also integrates a SIEM platform. The major differences between the two works are given by the types of attacks used (DDoS - Distributed Denial-of-Service - in the aforementioned work and several different types of attacks in the current work) and the type of SIEM used (in the aforementioned work using Wazuh [5], and in the current work AlienVault OSSIM – Open Source Security Information Management [6]).

As stated in [7], both network and host logs are important in IDS (Intrusion Detection System) systems. This principle is equally applicable to SIEM systems because they can integrate, by their nature, these types of logs, being a hybrid system. It is essential that all this data reaches an analysis in a centralized manner because attacks within a network can be carried out both on endpoint devices and on the actual network infrastructure. Also, from [7] the idea emerges that IDS systems must have both networking logs and system logs, which must be constantly analyzed. Thus, in the event of a possible attack, the system reacts by generating alerts. The system developed in this work also works in a similar way, with the difference that an IDS is not used to perform these operations, but a SIEM system is used.

A similar idea, regarding the management of network logs, can be found in the paper [8], where an architecture of a system that performs data traffic detection is presented. Thus, three large blocks are presented called data collection and analysis (which includes the acquisition of packets, their analysis and the extraction of the main information), local traffic processing (which handles traffic characteristics and records attack events) and cloud network traffic detection (which has a cloud area as its component, through which it classifies the traffic as a known attack or not). In the present paper, the cloud component is not integrated, the network architecture focusing on the local area, where both the acquisition and centralization of data, but also the detection of attacks from the inside area of the network, are performed.

In the paper [9], a set of experiments is carried out that includes the Wazuh SIEM and its integration with YARA [10] and VirusTotal [11]. The purpose of this integration is to achieve automation of network attack detection. The scenarios presented in the paper are similar to those in this paper because a phishing attack

and a forensic attack are used. The phishing attack is based on the mail system, which has a malicious attachment, and the forensic attack, by stealing private data of some people. The Wazuh SIEM and the integrations with YARA and VirusTotal help to isolate the affected files and network area. In this paper, the experiments do not integrate the VirusTotal area, because the network resources do not have explicit access to internet resources. Thus, although useful, this implementation focuses on local detection of network intrusions, both through the SIEM and the antivirus of endpoint devices. However, this implementation, which includes VirusTotal, will be taken into account in future work. An important feature of SIEM systems is that they can acquire a huge number of logs. Although their purpose is good, providing a complete overview of the network, often, for security administrators, most of the information is garbage. Therefore, it is often extremely difficult to distinguish between useful information about an attack and additional information. This is also the main reason for what are called false positives and false negatives in the detection and analysis of an attack within a network architecture. In the paper [12] this topic is addressed from the need to reduce the number of false positive or false negative alerts. The main ideas of the study focus on key aspects of alert testing by checking the effectiveness of alerts (to see if real threats have associated alerts), by checking the priority of the alarm (if the impact of its triggering leads to adverse consequences), by checking the cause of the alarm (it is possible that a system is under maintenance) or by classifying it (depending on importance: critical, high, medium or low). This way of implementing alerts is essential within IDS or SIEM-based systems because it greatly facilitates the work of security teams. Their implementation is possible within various SIEM-type systems, but at least the one based on classification will be found in this work.

Considering all these resources and using a virtual environment to create a network similar to real ones (through the Eve-ng [13] tool), this work will develop a system that will include both carrying out attacks, documenting the alerts made, and finding methods to prevent their spread throughout the entire network.

3. The proposed architecture

The main goal of this work is to create network architecture, which models real architecture of a structure in the business area, that includes both network equipment and the end-device area. In addition, a SIEM type system is integrated, which analyzes network logs, providing network protection against insider attacks. During the implementation of the solution, generic aspects of network equipment configuration were considered, and the attacks carried out were implemented considering various operating scenarios. By separating the architecture into two different modules, a possible isolation of traffic in one of the areas is also provided, if this measure is necessary. This aspect also leads to the prevention of the expansion of an attack into other network areas that need to be protected in a more

efficient way. The system is developed in the Eve-ng virtualization environment. Through it, both network equipment and end-devices and even the SIEM system are implemented. The SIEM agent tool is run on all devices, and the equipment activity is recorded at the manager's level. The operating systems are diverse, including Windows Server and Desktop, Linux Server and Desktop, Kali Linux, Cisco and Aruba network equipment and Fortinet firewalls. The resources needed to maintain the entire infrastructure functional reach almost 50GB RAM and 500GB disk, on a normal server, and with end-devices with minimal operating capacity. The steps to carry out an attack, which will be modeled throughout the experiments, can be found on Fig.1.

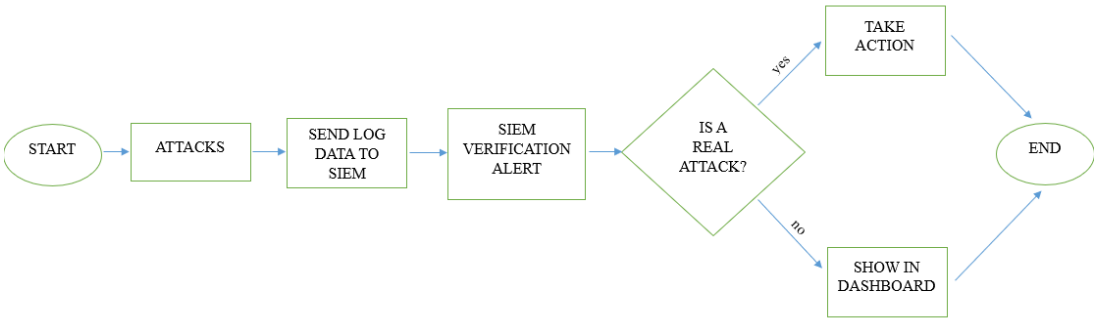


Fig. 1. Flowchart System

Thus, after recording an attack by one of the SIEM agents, it will transmit the data to the manager. Within the attack manager, if the alert is preset, automatic action will be taken to block or isolate the traffic. If, on the other hand, the alert is not configured, it requires the intervention of the security administrator. If it proves to be a viable alert, the necessary measures are taken to isolate or remedy the problem.

If the alert is of the false positive type, it is displayed on the dashboard and no additional measures are taken. Fig. 2 presents the network architecture proposed for the work scenario. Basically, the figure presents the two essential modules of network architecture, which include both the resource provisioning part, in the datacenter area, and the client side, represented, in this case, by the monitoring part in the NOC (Network Operations Center) area.

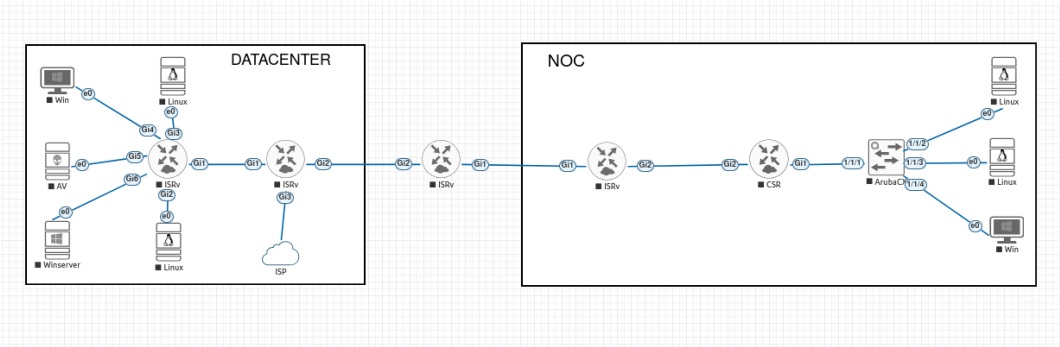


Fig. 2. The proposed network architecture

Practically, within the datacenter area, there are equipment that have Linux and Windows (Win) operating system, Windows Server operating system and the OSSIM SIEM system called AV respecting the name of the manufacturer AlienVault, highlighting the multitude of different equipment that make up such a network. Also, within this block, there is the ISP (Internet Service Provider) area, which ensures internet connection, which is connected to an ISR (Integrated Services Routers) router. In the NOC area, ISR and CSR (Cloud Services Router) routers are presented, along with an Aruba switch, which ensures services to customers, with Linux and Windows (Win) operating systems.

The datacenter area is the most important element and requires special attention because it is the module that provides the operating resources for the entire network infrastructure. The NOC area does not require as much attention, modeling the client side of the network resources, but it will also be necessary to ensure security measures to it. All endpoint devices and all network devices send logs to the SIEM system in the datacenter zone, and the communication part between the three network zones is based on dynamic routing, through the EIGRP (Enhanced Interior Gateway Routing Protocol) routing protocol. At the networking level, it is mentioned that all network devices are part of different networks. In the datacenter area, the network range is from 192.168.165.0/24 to 192.168.170.0/24, in the NOC area, the network range is from 192.168.155.0/24 to 192.168.157.0/24, and in the dynamic routing area, the range is between 10.0.10.0/24 - 10.0.15.0/24.

The novelty brought by the network architecture presented in Fig. 2 is given by the segmented implementation of resources, which indicates a clear separation between the two parts of the network. Another advantage is that, thanks to this segmentation, resources can be managed much more simply, with the possibility of implementing intelligent routing and extended network visibility modes. Also, in this way, there could be a physical delimitation between the two parts of the network, without the need for them to be located at the same location. Also, another advantage, from a security point of view, is the fact that such an implementation can prevent the spread of security incidents to the entire network. A final aspect,

and perhaps the most relevant of all, is the possibility of performing a local analysis, in the event of a security incident or in the event of anomalies at the NOC location, reducing latency and permanent dependence on the datacenter area for analyzing data or processes in the network. In addition, although this architecture cannot be considered new, being a classic architecture of a real business environment, however, comprising elements of various operating systems, routers from several vendors, a SIEM type system, it has the advantages of carrying out experiments similar to those encountered in the real environment.

Practically, based on the data obtained, at an experimental level, in the eveng virtualization environment, certain conclusions can be made, which can also be implemented in the real environment. Of course, being a simulated environment, the conclusions will not be identical to those found in the real case, because the way the equipment is made and the way the data is provided are experimental and created to provide simulation data, but the attacks used throughout this work and the way in which the SIEM system will record the alerts will work in a simulated way in the real environment. The major difference is in what it provides for the volume of data because, in a complex network (specific to a production environment of a real organization), the logs captured by the SIEM system are much more numerous and more complex and, often, become difficult to track. Thus, if sequential testing of key aspects is performed and policies are implemented step by step, the final network architecture can be extremely secure and robust. Within the attack scenario, several different types of attacks will be considered. These will be generated from the NOC area, modeling the behavior of an employee for the monitoring area, who has malicious intentions. Thus, at all client stations, the SIEM agent being already installed, the malicious activity will be recorded, and the data will be sent to the SIEM manager. The actual test is for how many of these attacks, the data will be recorded in the manager and in how long the attack will be detected. It is mentioned that, for some of the attacks, it will be necessary to deactivate the antivirus in the respective station, an aspect that also needs to be monitored through the SIEM, being an element that can indicate the intention of running a malware program. The initial attacks will be focused on a Linux station (with an operating system modified by the employee in Kali Linux). Subsequently, a similar operating scenario will be executed for attacks within a Windows client station. All attacks will focus on the category of network infrastructure attacks.

4. Experimental results

In this section, various results obtained during the experiments within the presented network architecture will be discussed.

4.1 Experimental setup

Since a clear idea is needed on the efficiency of detecting network intrusions through the infrastructure presented in the previous section, some attack

infrastructure scenarios will be implemented, which will work in a similar way to the test conditions. Basically, through Linux (Kali Linux) machine, certain network attacks will be carried out, which will be effective or not, depending on the type of attack. These attacks will be carried out both at the infrastructure level and for access to the resources of other client stations within the network.

In the first part of the test scenario, attacks will be carried out on the device area within the network infrastructure. Thus, the focus will be on resources such as port scans, credential attacks, etc. In the second part of the scenario, various attacks directed at the network infrastructure will be implemented, such as methods of copying the configuration, methods of obtaining privileged access to configurations and resources, finding various network addresses of important resources, etc.

4.2. First attack

The first attack that was considered is necessary to find out the devices on the network and the available ports. This type of attack is called in the literature as Reconnaissance (Information Gathering). The reconnaissance attack is, according to [14], the first stage of any attack, through which various information about the intended target is collected. The information thus obtained is used in the attack plan, to maximize its efficiency.

Basically, the main goal of this type of attack is to find out as much useful information as possible in order to plan the next steps of a more complex attack. This type of attack does not depend on the different categories of devices, applying both to client stations and to network equipment. The experiments carried out in this stage included netdiscover and nmap attacks, which were run multiple times, to observe as many details of the network as possible: **netdiscover -r 192.168.0.0/16 -p -f -P** and **nmap -v -A -PN 192.168.0.0/16.**

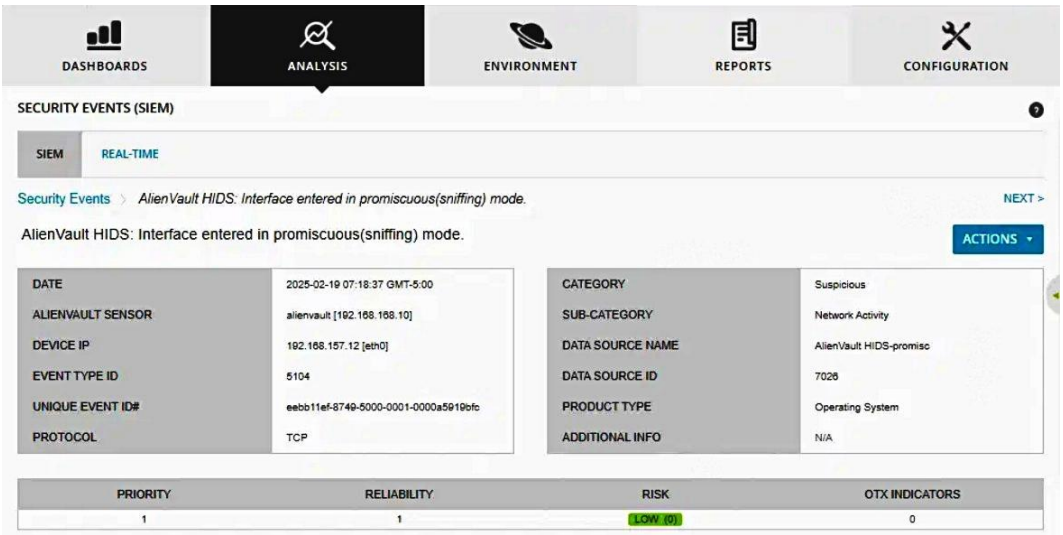


Fig. 3. The alert display in the SIEM dashboard following the nmap attack

In the case of the first attack, the following information is found in the netdiscover command:

- -r: specify the range of IP (Internet Protocol) addresses that should be scanned.
- -p: activates passive mode, which means it "listens" to network traffic and detects devices on the network based on their responses.
- -f: allows quick scanning to get an overview of the network, with the accepted minus in fewer additional details.
- -P: disables promiscuous mode (where all traffic on the local network is listened to), scanning focusing only on traffic related to it.

The first step in identifying the efficiency of the SIEM system used in the project is to verify whether these attacks are recorded or not in the security logs. Fortunately, in this case, the attacks are identified and displayed as alerts within seconds and, therefore, it is concluded that, at this stage, the system has functioned efficiently. It is also mentioned that, in both cases (with netdiscover or nmap), the alert that appears in the display area is: "*Interface entered in promiscuous (sniffing) mode*", as can be seen in Fig. 3.

The next step in the attack plan would be to assess and exploit vulnerabilities found through this type of attack. During this stage, several other attack modes will be used.

4.3. Second attack

In the case of the second attack, the command line is used to perform an aggressive scan on the target IP (or network range), including important information like OS (Operating System) detection, version scanning and traceroute, all of them being displayed in a very detailed output. Also, through these commands, the attacker host will not ping the target before scanning, assuming the target is online and proceeding with the scan directly.

These attacks include an additional scan of network services and finding associated vulnerabilities (old and outdated services, operating systems with known vulnerabilities, open ports that do not have associated services, etc.). Also, during this stage, it is essential to attempt to access network equipment or devices through brute-force attacks, with known passwords, default passwords or password dictionaries. Within this stage of attack, there are small differences in the case of attacks on client devices and on network devices. Thus, in order to correctly measure the effectiveness of the attack, specific attacks on the target devices, found through the previous stage, will be used. These are CAT, copy-router-config.pl or medusa, ncrack or, in a simpler way, brute-force attacks through actual attempts with the SSH (Secure Shell) IP command, etc.

- **CAT -h 192.168.157.1 -p 22 -a /usr/share/wordlists/nmap.lst**;

- **./copy-router-config.pl 192.168.157.1 192.168.157.12 public;**
- **medusa -h 192.168.168.10 -u admin -P /usr/share/wordlists/passwords.txt -M ssh -t 5,**
- **ncrack -u admin -P passadmin.txt -p 3389 192.168.165.11**

In this case of the attacks, the following information is found in the previously used commands:

- -h: specify the hostname (or IP) of the hosts that should be scanned.
- -p: specifies the port on which the scan should be made.
- -a or -P: specifies the path where the file with the passwords that the attack should try can be found.
- public: is the read-only community string for Cisco network devices.
- -u: specifies the username that is used during the attack.
- -M: specifies the protocol that should be attacked.
- -t: sets the number of threads used in the attack.

Considering the effect of brute-force attacks, alerts appearing on SIEM dashboards were of the type "SSHd: Did not receive identification string", "SSH insecure connection attempt (scan)" or "User missed the password more than one time", as shown in Fig. 4. These alerts appear within a reasonable time, within the system, the first data about the attack being recorded a few seconds after the first brute-force attempt. Following the evolution of the attack, certain policies were also taken into account to block access to the station declared to be potentially malicious. Thus, a deny policy was implemented for the IP of the respective station, which made it impossible for it to open the SSH connection to the SIEM system. And the next time the Linux workstation attempts to connect to SIEM via port 22, the terminal prompt displays the message "Connection refused".

The next stage that needs to be in the attention of this article is given by obtaining access to the target system. Its main purpose is given by exploiting identified resources, copying files or maintaining access to explore various types of additional resources. Also, in the case of network equipment, an important aspect is attempts to escalate privileges, in order to be able to configure certain aspects of interest, which would further endanger the network. Also, within this stage, data exfiltration will be attempted, through access to passwords or even system logs.

Although, for the passwords used within the network, a successful attack was not carried out using the passwords from the dictionary password files, in order to carry out experiments that also capture a successful attack, for one of the Cisco routers and for one of the devices in the datacenter area, the default credentials of type cisco/cisco and admin/admin were used. These indicate a clear human error, but the purpose of the experiment is to visualize the aspects recorded by SIEM and how it identifies and classifies these attacks.

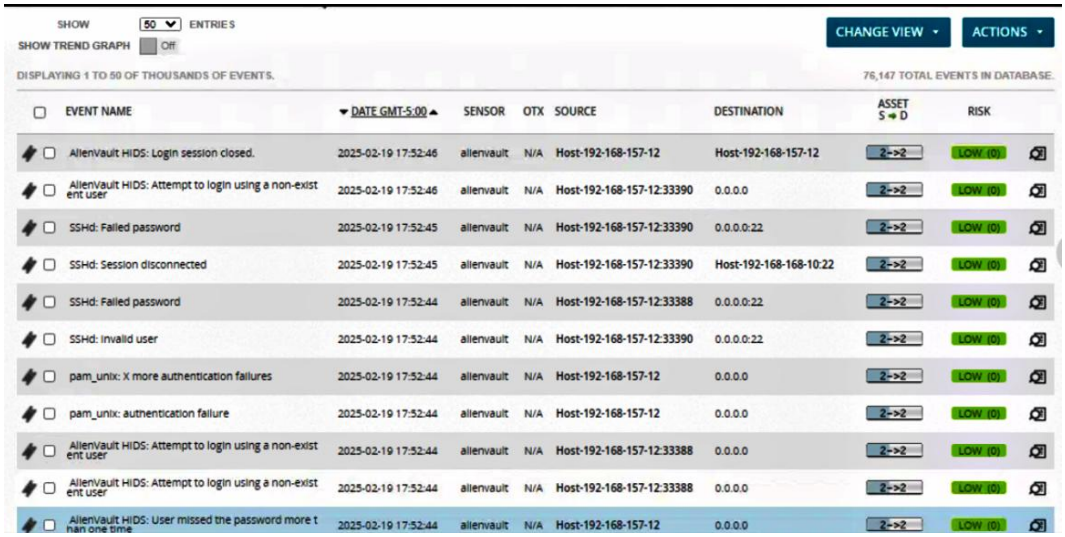
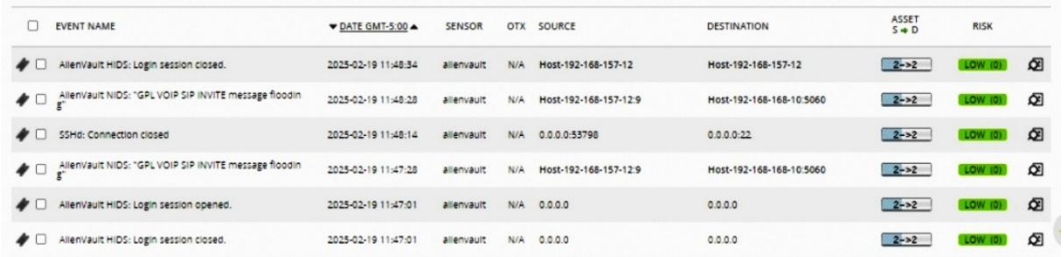


Fig. 4. The alerts displayed in the SIEM dashboard following the SSH brute-force attack with medusa

Following the experiments carried out using the medusa and ncrack tools, the alerts at the SIEM system level are quite explicit and quickly displayed. Thus, in the case of the Cisco equipment, the event is recorded with the alert type "Successful sudo to ROOT executed" and on the client station, in the datacenter area, the alerts at the SIEM dashboard level are of the type "Windows machine logon" and "Special privileges assigned to new logon". However, it is worth noting the common behavior of the SIEM system in relation to attacks based on multiple threads, such that it tends to display a repeated number of logs based on the same event. However, this aspect can also be an advantage for teams monitoring such events because, even if an alert is not triggered and displayed, multiple logs based on the same topic, with the same source and destination, can indicate malicious behavior. To test the way alerts are displayed during an attack directed at the SIEM system, an experiment was also considered in which a DDoS attack is centered from the NOC area directly to the SIEM IP address. For this scenario, the inviteflood tool from Kali Linux was used: **inviteflood eth1 5000 SIEM.local 192.168.168.10 1000**.

Basically, through that command, the type of attack is identified, the interface used to carry it out (the one leading to the target traffic), the user who will carry out the attack (5000 is the default user), the targeted domain (SIEM.local), the targeted IP and the number of packets used. This was run repeatedly, with the number of packets increasing to 5000000. In spite of the fact that there were several simpler tools that performed a DoS attack, the inviteflood tool was chosen because it uses a more atypical protocol, based on SIP/SDP (Session Initiation Protocol/ Session Description Protocol).

Thus, the aim was to test the effectiveness of the SIEM tool with less common traffic or protocols. Although, during the experiments, there were short interruptions of the https connection or short delays in display, the SIEM system repeatedly displayed the alert corresponding to the attack to its source with the message "GPL VOIP SIP INVITE message flooding", also indicating the source IP of the attack, as in Fig.5.



EVENT NAME	DATE GMT-5:00	SENSOR	OTX	SOURCE	DESTINATION	ASSET S→D	RISK
AlienVault HIDS: Login session closed.	2025-02-19 11:48:34	alienvault	N/A	Host-192-168-157-12	Host-192-168-157-12	2->2	LOW (0)
AlienVault NIDS: "GPL VOIP SIP INVITE message floodin g"	2025-02-19 11:48:28	alienvault	N/A	Host-192-168-157-12:9	Host-192-168-168-10:5060	2->2	LOW (0)
SSHd: Connection closed	2025-02-19 11:48:14	alienvault	N/A	0.0.0.0:53798	0.0.0.0:22	2->2	LOW (0)
AlienVault NIDS: "GPL VOIP SIP INVITE message floodin g"	2025-02-19 11:47:28	alienvault	N/A	Host-192-168-157-12:9	Host-192-168-168-10:5060	2->2	LOW (0)
AlienVault HIDS: Login session opened.	2025-02-19 11:47:01	alienvault	N/A	0.0.0.0	0.0.0.0	2->2	LOW (0)
AlienVault HIDS: Login session closed.	2025-02-19 11:47:01	alienvault	N/A	0.0.0.0	0.0.0.0	2->2	LOW (0)

Fig. 5. The alerts displayed in the SIEM dashboard following the inviteflood attack

4.4. Discussion

The purpose of the experiments carried out in this chapter was to test the effectiveness of the way the SIEM works in the network. It can be concluded, taking into account the results obtained through both the first attack, the resource discovery attack, and the combined multiple attack, from the second part of the scenario, that the SIEM system recorded the alerts in an appropriate and efficient manner.

In addition, during experiments, similar to the work [15], combining type 1 and 2 attacks was also considered and carried out. Basically, during the network scanning with the nmap tool, a brute force directed at the SIEM system was attempted, to see how the alerts are displayed and what is prioritized at the dashboard level. Thus, it was found that the emphasis is placed on the brute-force attack, the alert appearing before the network scanning one.

Considering other ways of detecting the efficiency of an analyzed system, the article [16] is also considered, which presents the essential characteristics of a hybrid IDS system. Thus, given that the SIEM used in this work also works similarly to a hybrid IDS, the presented characteristics can also be applied in this case.

Flexibility is the first key element that must be considered and, taking into account the way in which the SIEM effectively displayed attack alerts from different categories, it can be considered a flexible system.

Adaptability is another important element that the SIEM must cover. However, this is not applicable to the current system, because it has a limited number of analyzed devices. However, in the following experiments, the experimental scheme will be much more comprehensive and the adaptability to new traffic conditions and new network dimensions will be an intensively tested element.

Optimization is the third key element and, taking into account that the resources consumed are not very extensive (being an integrated environment in eveng), it is considered that the SIEM ticks this category as well. Also, considering that the nmap or inviteflood attacks recorded even at their level do not prevent the dashboard from functioning and the recording of attacks that are carried out in parallel, it makes it an extremely efficient system.

Self-Modifying is the last parameter analyzed in the paper [16], but it cannot be applied to current systems because the SIEM system used has not altered its own parameters or methods to identify network threats.

Although the previous sections have demonstrated the feasibility of implementing a segmented enterprise network monitored by OSSIM for detecting insider threats, a comprehensive assessment of effectiveness requires a more structured evaluation.

Threat modeling is formalized by explicitly defining internal capabilities, initial access conditions, and operational constraints. Each attack scenario is treated individually, allowing for precise verification of detection effectiveness. However, this approach ensures, at the same time, that the logs of other network equipment and concurrent events are evaluated. Thus, it can be demonstrated that the SIEM system ensures prompt response to incidents. Success criteria were operationalized in measurable terms: an attack was detected when the SIEM generated an alert corresponding to the specific signature within the established latency threshold. However, it is also necessary to consider the potential of the system to generate false positives. This aspect will be addressed in experiments that will be found in the following papers.

Scalability and robustness should also be considered by expanding the experiments to incorporate common background traffic, increasing the number of simulated endpoints, and testing the performance under SIEM stress loads. To assess external validity, background traffic (from other equipment) was introduced, simulating normal enterprise network activity. Detection rates remained consistent, demonstrating that the SIEM correlation rules effectively distinguished between legitimate traffic and malicious events.

However, it is recognized that current experiments focus on a controlled virtualized environment, which makes the conclusions less applicable to real environments. However, the testbed can indicate whether a SIEM system can be applied in a network, without the need to introduce it directly into the production environment. Thus, conclusions can be drawn about the working mode and efficiency of the SIEM system, just by taking the production environment into a test environment. However, if the production environment is much too large, this becomes cumbersome. However, for the chosen work scenario, the demonstration is flexible and, moreover, it also becomes a controlled test environment for newer employees, having the opportunity to get to know the production environment and

test various aspects, without affecting anything real. However, future work will seek to generalize the findings to larger and more heterogeneous enterprise networks. Therefore, this approach transforms the demonstration of applicability of the experiments into a replicable and methodologically robust study. The result is not only a reproducible framework for testing SIEM implementation in segmented architectures, but also solid empirical evidence of its effectiveness in detecting and managing insider threats in enterprise environments. Considering all these parameters and the applied method of evaluating the characteristics of the SIEM used, it is found that this is an efficient system.

6. Conclusions

In this paper, a solution for detecting intrusions at the level of network architecture applicable to a common business system, was presented. This solution was implemented within the network resource emulation system called eve-ng, being a complete solution, both in the networking area, with routing between various parts of the network, but also with client systems, which access resources within the network. At the network level, it is divided into two main categories, the datacenter part, which provides data resources and the NOC part, which monitors network activity. These parts, although integrated into one, for smaller business areas, are imperative for any network. Their modularity also covers the need to provide access rights to resources, which is different within each one, but also the possibility of isolating the spread of an attack, if this is necessary. The main goal was to verify the efficiency of logging and recording intrusive events at the network level by a SIEM system, which is also in the simulated eve-ng environment. All resources and the entire analysis area operate in an offline mode, which is also one of the main disadvantages of the solution. Another main disadvantage, which derives from the previous one, is the fact that, being an offline system, it cannot benefit from updated signatures or integration with other online tools.

However, considering the experimental part, the SIEM system used proved to be extremely efficient for the generated attacks, functioning correctly, even in work scenarios that targeted attacks on them. Thus, it efficiently detected malicious activities that included port scanning and brute force credential theft, correlating events and displaying effective alerts in an extremely short time. Such a way of working is also ideal in real time because it leads to efficient prioritization of events and a short response time from the intervention team.

One aspect worth mentioning is that the SIEM system could also be integrated into the NOC part, for ease of accessing the interface, but in the datacenter area it can be integrated with many more complementary security solutions such as firewalls, IDS/IPS, etc. Thus, taking into account the initial objectives, it proved to be a viable solution for the network architecture used, under test conditions. Of course, if this architecture were to move into a real and

uncontrolled environment, a series of other dangers or unforeseen aspects would have to be considered, and the attacks would, in most cases, be much more complexly developed. But the usefulness of such a system and, essentially, of the experiments carried out comes from the way it tests the capabilities of the SIEM, in the way it efficiently implements alerts, in the way it implements rapid and automatic response methods in the event of an attack being detected, and in the way it visualizes how it is able to record and display events. Being a network with a limited number of devices, the SIEM type system cannot prove how it will work when their number doubles or even triples. However, this is one of the elements that will be analyzed in subsequent developments. Also, the use of attacks from a more complex and much wider scope is necessary to test the functionality of the SIEM. And this aspect is another element that will be considered in subsequent developments.

In future work, we plan to expand our study by evaluating additional SIEM platforms to compare detection capabilities, scalability, and operational efficiency. Although OSSIM was selected for the current EVE-NG testbed due to its open-source availability and ease of integration, other leading SIEMs such as Splunk or QRadar offer complementary advantages. Splunk offers powerful search and analysis capabilities, with advanced correlation and visualization features. IBM QRadar is recognized for its robust threat intelligence integration and automatic incident prioritization. Incorporating these SIEMs into future experiments will allow for a comparative analysis of detection latency, false positive rates, and event correlation under similar virtualized conditions. However, adapting these platforms to EVE-NG will require careful modeling, as alternative SIEMs have not yet been natively implemented in this environment, but this will provide a broader perspective on the relative strengths and trade-offs of different enterprise-level monitoring solutions.

The current study demonstrates the practical implementation and effectiveness of a segmented enterprise network monitored by OSSIM SIEM in detecting insider threats. By extending the experiments to additional SIEM platforms, threat modeling, and comprehensive performance evaluation, future work will further improve the generalizability and applicability of our findings, providing both reproducible methodologies for testing and useful insights for enterprise security management.

REFERENCES

[1] *Y. Kanaparthi, T. M. Abdellatif, A. A. Seyam and G. B. Satrya*, Identifying Security Threats in the System Using Automated Security Logs, 2024 Third International Conference on Sustainable Mobility Applications, Renewables and Technology (SMART), Dubai, United Arab Emirates, 2024, pp. 1-5, DOI: 10.1109/SMART63170.2024.10815284.

[2] *IBM*, Cost of a Data Breach Report 2024, [online] Available: https://www.ibm.com/reports/data-breach.

[3] *E. J. Tan et al.,* Simulation of Pre-Ransomware Attacks on Active Directory, 2024 17th International Conference on Security of Information and Networks (SIN), Sydney, Australia, 2024, pp. 1-9, DOI: 10.1109/SIN63213.2024.10871611.
[4] *M. A. Maliki, P. Sukarno and A. A. Wardana*, Integration of Heterogeneous IDS with SIEM for DDoS Attack Detection in Computer Networked Multi-Organizational Environments, 2024 5th International Conference on Communications, Information, Electronic and Energy Systems (CIEES), Veliko Tarnovo, Bulgaria, 2024, pp. 1-7, DOI: 10.1109/CIEES62939.2024.10811423.
[5] *Wazuh,* Wazuh, [online] Available: https://wazuh.com/.
[6] *LevelBlue,* LevelBlue OSSIM, [online] Available: https://levelblue.com/products/ossim
[7] *Beatrice-Nicoleta Chiriac, Florin-Daniel Anton, Anca-Daniela Ioniță,* A hybrid IDS architecture, UPB Sci. Bull., Series C, Vol. **85**, Iss. 1, 2023.
[8] *Linzhong Zhang*, Malicious Traffic Detection Algorithm for the Internet of Things Based on Temporal Spatial Feature Fusion, International Journal of Advanced Computer Science and Applications (IJACSA), Vol **15**, Iss. 11, 2024.
[9] *H. T. Zaw, T. Aung, A. H. Maw and M. Thida Mon*, Comparative Analysis of YARA and VirusTotal Integrations with Wazuh for Enhanced Malware Detection, 2024 5th International Conference on Advanced Information Technologies (ICAIT), Yangon, Myanmar, 2024, pp. 1-6, DOI: 10.1109/ICAIT65209.2024.10754931.
[10] *GitHub*, yara, [online] Available: https://yara.readthedocs.io/en/stable/gettingstarted.html
[11] VirusTotal, VIRUSTOTAL, [online] Available: https://www.virustotal.com/gui/home/upload
[12] *S. Alabdulhadi and A. Al-Matouq*, Efficient and Standardized Alarm Rationalization for Cybersecurity Monitoring, in IEEE Access, vol. **12**, pp. 166936-166944, 2024, DOI: 10.1109/ACCESS.2024.3492264.
[13] *eve*, EVE - The Emulated Virtual Environment for Network, Security and DevOps Professionals, [online] Available: https://www.eve-ng.net/
[14] *K. Bhatia and S. S. Ojha*, Federated Learning Framework for Early Detection of Reconnaissance Attacks in Smart Grid Environments, 2024 2nd International Conference on Device Intelligence, Computing and Communication Technologies (DICCT), Dehradun, India, 2024, pp. 1-6, DOI: 10.1109/DICCT61038.2024.10533039.
[15] *Limei Ma, Dongmei Zhao, Yijun Gao, Chen Zhao,* Violence Cracking Technology of SSH Service Based on Kali-Linux, International Journal of Advanced Network, Monitoring and Controls, vol. **4**, pp. 35-39, 2019, DOI: 10.21307/ijanmc-2019-045
[16] *J. V. Barpute and S. Bhargava*, Improving System Security: Machine Learning Algorithm-Based Intrusion Detection System, 2024 4th International Conference on Ubiquitous Computing and Intelligent Information Systems (ICUIS), Gobichettipalayam, India, 2024, pp. 433-444, DOI: 10.1109/ICUIS64676.2024.10866908.