Implementation of Security Information and Event Management (SIEM) for Monitoring IT Assets Using Alienvault OSSIM (Case Study: Udayana University Information Resources Unit)

Fahri Choirul Anam[a1], Gusti Made Arya Sasmita[a2], I Putu Agus Eka Pratama[b3]
[a]Department Information Technology, Faculty of Engineering, Udayana University
Bukit Jimbaran, Bali, Indonesia
e-mail: [1]choirulanam@student.unud.ac.id, [2]aryasasmita@it.unud.ac.id,
[3]eka.pratama@unud.ac.id

Abstract

One way that can be done to analyze cyber security equipment is by monitoring the logs it generates. Meanwhile, to be able to analyze the logs generated from each equipment requires a long time and has a high level of difficulty. When the management of the cyber security system is not going right, it causes the failure of the cyber security system. So a defense mechanism is needed on managing the log called Security Information and Event Management (SIEM) using Alienvault OSSIM tools. Threat Monitoring or monitoring of security threats in the Cyber world, is used to analyze, evaluate, and monitor network threats and as an end point for organizations to provide evidence of security threats, such as network intrusions, data exfiltration, ransomware and other malware attacks. The limitations of the problems carried out in this study were limited to Threat Monitoring using Alienvault OSSIM. There are 6 servers at the Udayana University Information Resources Unit (USDI) that are being monitored. Monitoring was carried out for 3 months. There were 230,622 Events or events that were collected as a whole. IT assets that have the most logs during monitoring are owned by DNS Servers with a total of 200,424 Events. There are 11 Event Names and 34 event logs that are discussed. The log is packaged in the form of a report along with an explanation, of course it can assist administrators in evaluating their IT assets. There is also an email notification feature using Gmail. Overall there are no attacks that are so significant with the low risk category. Alienvault OSSIM is proven to be able to carry out monitoring processes in real time properly and can help USDI to monitor the activities of its IT assets.

Keywords : *Alienvault OSSIM, IT Assets, SIEM, Threat Monitoring, USDI*

1. Introduction

Efforts to improve cyber security or network security are essential. However, due to the large number of network security devices or IT assets being used, more and more equipment is being managed. Assets such as networks, devices and applications must be managed, analyzed and managed with security data to remain safe and function according to their function.

One way to improve cyber security is to analyze IT equipment by monitoring the logs generated from the equipment. Analyzing the logs produced from each piece of equipment takes a long time and is difficult. When the management of the cyber security system does not run well, it causes cyber security system failure. So, a defence mechanism is needed to manage logs called Security Information and Event Management (SIEM). Security Information and Event Management (SIEM) is a technology that correlates logs, events, distributed systems and services with a security baseline (Datacomm Cloud, 2017). The strength of SIEM is its ability to understand logs or events generated by devices, software and hardware, monitor, analyze and correlate them to detect cyber attacks and then provide notifications in the form of alarms or alerts. One of the tools that uses the SIEM mechanism is Alienvault OSSIM (Open Source Security Information and Event Management).

The Udayana University Information Resources Unit (USDI) is an agency that provides computer facilities, broad communications, and Information Technology needs used by Udayana University Lecturers, Staff and Students. Currently, USDI does not have applications or security tools to carry out Threat Monitoring, especially SIEM-based. Additionally, USDI does not yet have an application that can manage logs and provide notifications automatically because USDI is still manual in reading server logs. There was a hack on a server owned by USDI. It is suspected that the cause was due to a backdoor file stored in the USDI directory. So implementing Threat Monitoring using Alienvault OSSIM on USDI is very important so that security or network administrators can get early notification if there are indications of attacks or anomalies occurring on USDI's servers so that they can take precautions. Apart from that, security or network administrators can find out what activities are carried out by monitored IT assets. Therefore, a SIEM-based Threat Monitoring tool, namely Alienvault OSSIM, was implemented at the Information Resources Unit (USDI) at Udayana University.

2. Research Method

In this research, there are several stages that need to be carried out. These stages are carried out sequentially and when one stage is completed, they immediately move on to the next stage. The following is a picture of the flow of the research method used in this research.

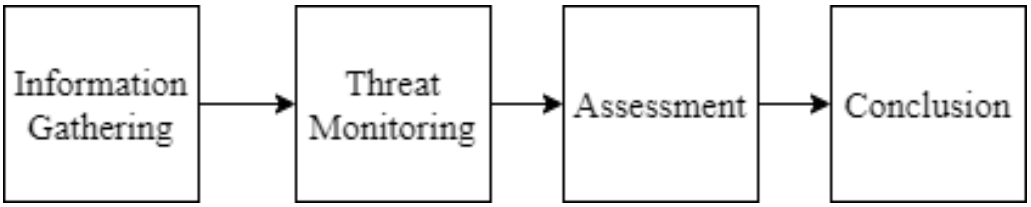

Figure 1 Research Methods

Figure 1 is the process of the research methodology that will be carried out. This research starts from Information Gathering, Threat Monitoring, Assessment, to Conclusion. Research will be carried out from stage one to the next stage. The research begins by conducting an Information Gathering (Information Gathering) with related agencies, collecting information in the form of introducing the environment, network structure, collecting the number of assets that will be monitored, apart from that it can also be in the form of collecting data about problems related to the assets or agencies. Next there will be a Threat Monitoring process, where the Alienvault OSSIM installation and configuration process will be carried out, until the monitoring process lasts for 3 months. Next, an assessment process will be carried out on the results of the monitoring. Assessment of results in the form of events or events related to the assets being monitored. In addition, data processing analysis will be carried out based on these events. Next, the Conclusion process will be carried out, in the form of making conclusions based on the assessment and data processing process from events or monitoring during the 3 months.

3. Literature Study

The literature review discusses theories related to writing research reports.

3. 1 SIEM

Security Information and Event Management or SIEM is a tool used to monitor and analyze network traffic in real time. The data analyzed is in the form of logs generated by the device or application. In addition, SIEM tools function as a means of detecting potential attacks and tracking intrusion paths. SIEM can also be said to be a log management system. The reason is that SIEM collects data or logs from various points, such as databases, firewalls, servers, networks, and so on. SIEM makes it possible to record various events and their correlation from all existing sources.

3. 2 Alienvault OSSIM

Allienvault OSSIM or Open Source Security Information and Event Management is an Open Source System (SIEM) tool, which integrates selected tools designed to help network administrators in Computer Security, Intrusion Detection, and Prevention. OSSIM is intended to

provide security analysis and give Administrators a more complete view of all aspects of their system security, by combining extensible log management with plugins and asset management and discovery with information from specific information security control and detection systems. This information is then correlated together to create context for the information that would not be apparent from any one part alone. Alarm displays and availability views along with reporting capabilities are provided to enhance the tool's capabilities and usability for security and systems engineers. The Allienvault OSSIM tool uses various types of sensors to monitor data, including Snort, Ntop, Openvas, P0f (Passive OS Detection), Pads, Arpwatch (Mac change anomalies), OSSEC (IDS for Host level), Osiris, Nagios and OCS (Inventory), these sensors are used to monitor events originating from remote hosts using the Syslog protocol. This development was carried out with the aim of preventing attacks based on attack patterns aimed at the system.

3. 3 Threat Monitoring

Threat Monitoring or monitoring security threats in the cyber world, is used to analyze, evaluate and monitor network threats and as an end point for organizations to provide evidence of security threats, such as network intrusion, data exfiltration, ransomware and other malware attacks. Once a threat is identified, threat monitoring software issues an alert and stops the threat. Threat Monitoring provides visibility into the network for Security Engineers and provides actions to users who access it. Threat Monitoring can provide stronger data protection and prevent or reduce damage caused by breaches. Companies are now hiring Security Engineers for Threat Monitoring to avoid additional risks to company data and sensitive information, as well as encourage monitoring of security threats in the company.

3. 4 Hardware and Software Requirements

Meanwhile, carrying out this research requires several devices in the form of hardware and software that can be used to carry out the monitoring process. The following are several tools used to conduct Implementation research (SIEM) for IT Asset Monitoring Using Alienvault OSSIM as follows.

3.4.1 Hardware Requirements

Hardware is all types of components in a computer device that have a physical form, can be seen, touched and felt. The main function of hardware is to provide support for the main function of a computer, such as input, processing, output, secondary storage and communication (Napizahni, 2023). The following is some of the hardware used in conducting final assignment research entitled Implementation (SIEM) for IT Asset Monitoring Using Alienvault OSSIM as follows.

a. Alienvault OSSIM Server with specification CPU Intel Xeon 2.8GHz 12 Core, RAM 8Gb, Disk 200Gb.
b. Router
c. Hub
d. Gateway Server
e. Webserver
f. DNS Server
g. Radius Server (WIFI)

3.4.2 Software Requirements

Software is a collection of instructions, code, or programs created to help users interact with a computer and carry out certain tasks. Simply put, software helps computers how they function. Therefore, without computer software it will not be able to function and do anything. For example, without web browser software such as Chrome or others, users cannot access the internet (Anendya, 2023). The following is some of the software used in conducting final assignment research entitled Implementation (SIEM) for Monitoring IT Assets Using Alienvault OSSIM as follows.

a. Alienvault OSSIM

b. Linux
c. OSSEC
d. VMware
e. Putty SSH
f. VPS Linux Ubuntu
g. G-Mail

3.5 List of IT Assets that are Monitored

The following is a list of IT assets that undergo a monitoring process. This determination process is through a discussion process between the researcher and the person in charge of the relevant agency. The monitoring process is carried out on six assets. The following is a list of assets that are monitored using Alienvault OSSIM on USDI.

Table 1 Monitoring List IT Assets

Server Name	Hostname
AGENT SSH GATEWAY SERVER	GDLN 1
SERVER UNIT VM 11	GDLN 2
UNIT WEB 6 VM 12	GDLN 3
WEB 2 VM 12	GDLN 4
SERVER DNS	GDLN 5
SERVER RADIUS (WIFI)	GDLN 6

3.6 Network Topology

Network topology is something that explains the geometric relationships between the basic elements that make up a network, namely nodes, links and stations. The selection of network topology is based on network scale, cost, objectives, and usage. The following is the Network Topology that will be used in Implementation research (SIEM) for Monitoring IT Assets Using Alienvault OSSIM (Case Study: Udayana University Information Resources Unit (USDI).

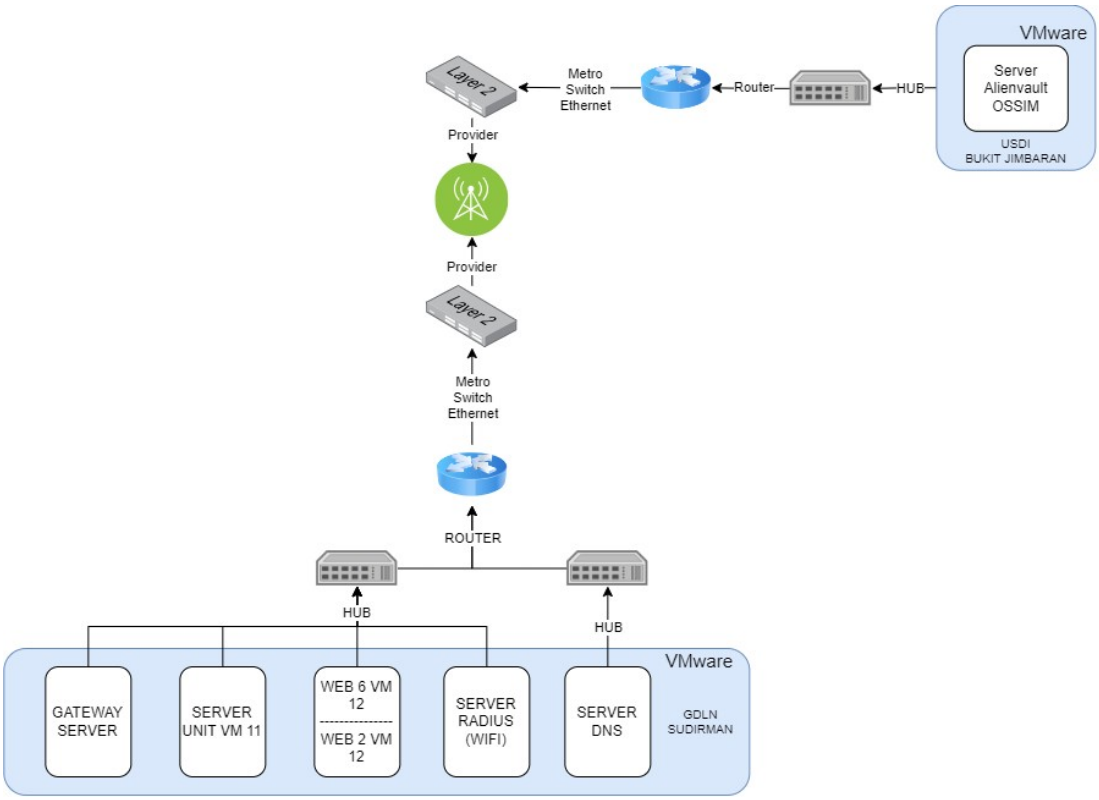

Figure 2 Network Topology

Figure 2 is the Research Network Topology applied to the Information Resources Unit (USDI) at Udayana University. The VMware Server between Alienvault OSSIM and Agent Server is not located in the same location. However, they can be network connected using a local network to each other. The Alienvault OSSIM Server and Agent Server that are monitored are connected using a Metro Switch Ethernet which is also connected to the same provider in each location, namely GDLN Sudirman and USDI Bukit Jimbaran.

3.7 Alienvault OSSIM Architecture

In a good application design, one of the things that must be considered is the information architecture. Information architecture will help users to find the information they need more easily and quickly. An application is said to have good information architecture if the application organizes information well and is structured. In this way, users will not get lost in the application when they need information, and will get the information they need quickly. The following is the architecture of Alienvault OSSIM.

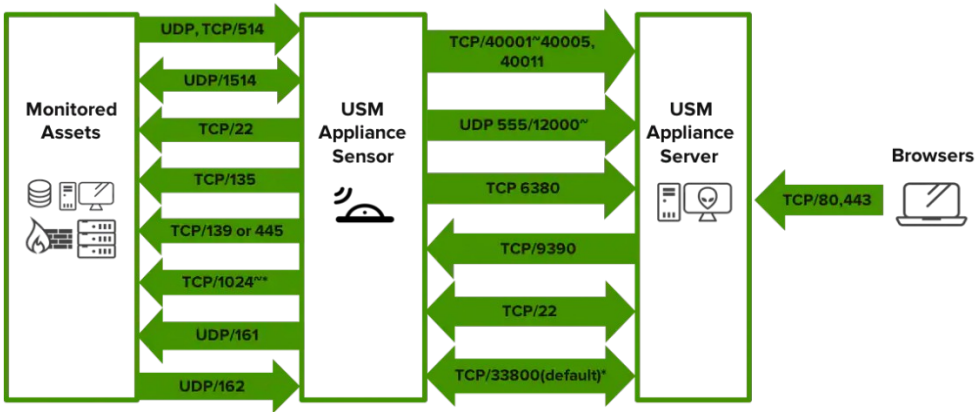

Figure 3 Alienvault OSSIM Architecture

Figure 3 is the architecture implemented in Alienvault OSSIM. Based on this architecture, it is divided into 4 main parts, namely Monitored Assets, Alienvault OSSIM Sensors, Alienvault OSSIM Server, and Browsers. The stages carried out by Alienvault OSSIM are based on this structure, such as monitoring and collection processes for monitored assets or taking events in the form of logs on monitored assets which are carried out by sensors owned by Alienvault OSSIM using a TCP/UDP connection with a certain port. Next, after going through the event retrieval or collection process, the event is given by the sensor to the Alienvault OSSIM Server. This process is also carried out using a TCP/UDP connection with a specific port. After the event arrives at the Alienvault OSSIM Server, a process of checking the correlation of the event with other events, the event with the event originating system, the event with the time of occurrence, and the event with other attributes is carried out. After the event correlation process has been successful, an administrator can access or obtain this information via a browser with a device connected directly to Alienvault OSSIM. This process uses a TCP connection using port 80, namely the HTPP protocol, and port 443, namely the HTTPS protocol. After this process, an administrator can carry out the monitoring process in real time.

4. Result and Discussion

This section contains a discussion of research results and discussion consisting of research variables, data preprocessing results, data processing results, comparative analysis between models, decision tree visualization, rules and test results.

4.1 Installation of Alienvault OSSIM Server

Alienvault OSSIM is an OS with a Debian version of Linux. Alienvault OSSIM can be downloaded as a file with the .ISO extension at the following official Alienvault OSSIM link https://cybersecurity.att.com/products/ossim/download. Next, after successfully downloading the file with the .ISO extension, you can install it on the desired server. The first step in installation is simply booting the server then using the ISO that has been downloaded. After that, the user will immediately be given the Alienvault OSSIM configuration display. The following is what Alienvault OSSIM will look like if the installation has been successful.

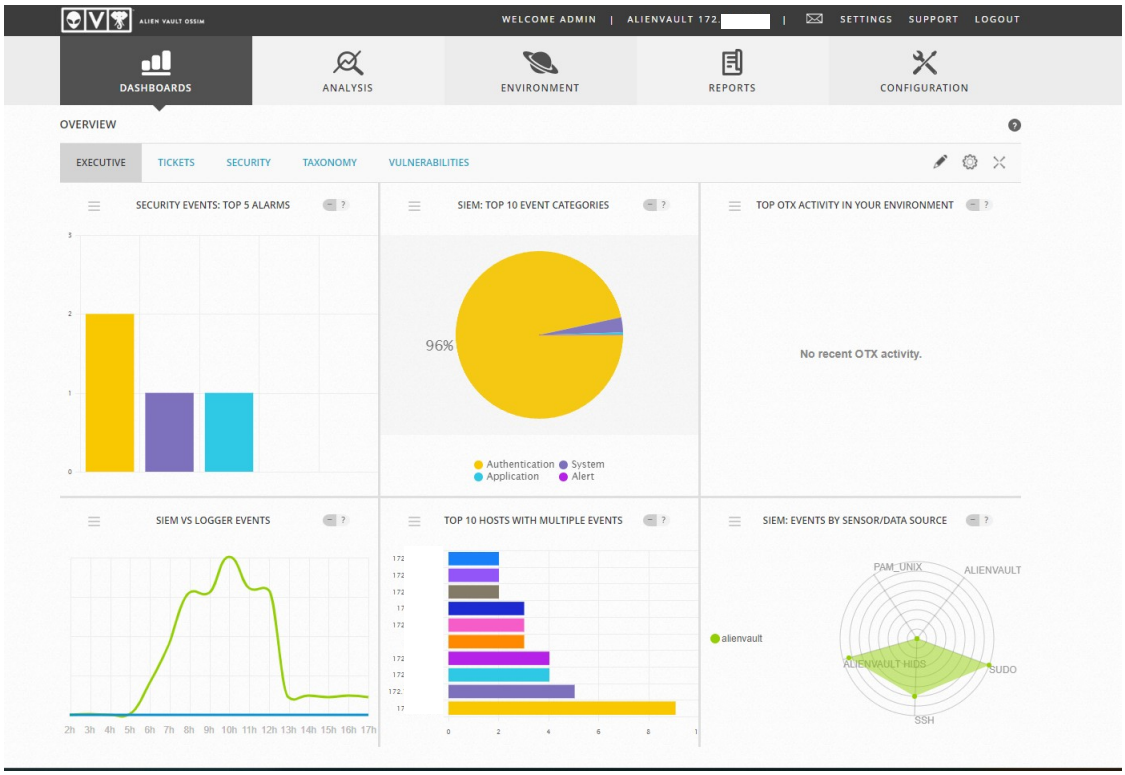

Figure 4 Alienvault OSSIM GUI display in browser

Figure 4 is the initial appearance of the Alienvault OSSIM GUI in the browser. This display shows that Alienvault OSSIM has been successfully installed and is ready to use. Next, users can carry out the configuration process to add hosts or assets to become agents.

4.2 Configure Policy for Gmail Notifications

Policy is a rule that can be applied to Alienvault OSSIM. In this section, users can set what policies will be implemented to assist the process of monitoring IT assets according to the conditions of the organization or institution concerned. The following is an image of the policy applied in this research.

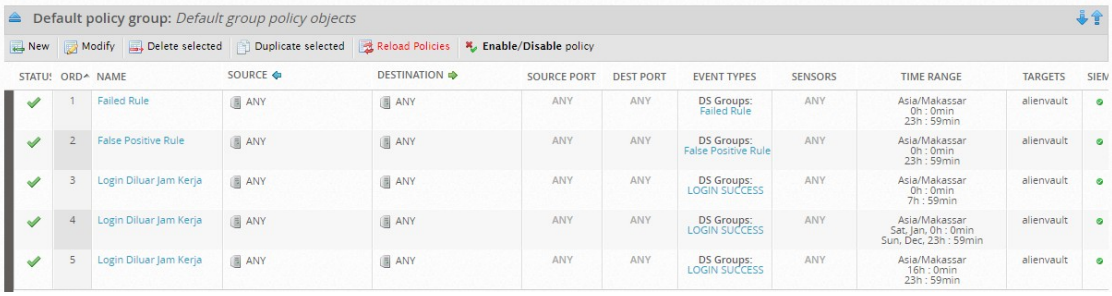

Figure 5 Policy Configuration

Figure 5 is a picture of the policy configuration implemented in Alienvault OSSIM for monitoring IT assets on USDI. In the figure, five types of policies are implemented which aim to assist monitoring in the form of providing notifications if there are appropriate regulatory conditions, both for the type of event selected and at the specified time. To implement this, users can enter the threat intelligence menu and then policy. In the policy section it will look like figure 5, then you can press the new button to create a new policy. After that, users can configure policies according to the conditions of the research location. The following is a table that explains what policies are applied in this research.

Table 2 Event Type Failed Rule

No.	Event Type	Event Name
1.	SSH	SSHd:Failed Password
		SSHd:Failed Publickey
		SSHd:Invalid User
		SSHd:Illegal User
		SSHd:Root login refused
		SSHd:User not Allowed because listed in DenyUsers
2.	Alienvault HIDS - Authentication Failed	User Authentication failure
		User missed the password more than one time
		User missed the password to change UID (user id)
		User missed the password to change UID to root
		User Login Failed
		Attempt to login using a non-existent user
		SSHd Authentication Failed
		Login Session Failed
		User Failed to change UID (user id)
		User authentication failed
		Admin authentication failed
		Web authentication failed
		Database authentication failure
		Bad password attempt
		Authentication failed for user
3.	Alienvault HIDS - Invalid Login	Attempt to login with an invalid user
		Attempt to login using a denied user
		Login session failed (invalid user)
		Possible Registration Hijacking
		Attempt to login using a non-existent user
4.	Alienvault HIDS - SShd	Possible attack on the ssh server (or version gathering)
		Reverse lookup error (bad ISP or Attack)
		Possible breakin attempt (high number of reverse lookup errors)
		Timeout while logging in (sshd)
5.	Alienvault HIDS - Sudo	Failed attempt to run sudo
		First time user executed sudo
		Three failed attempts to run sudo
6.	Alienvault HIDS - rootcheck	Host-based anomaly detection event (rootcheck)
		Windows Malware Detected
		Windows Adware/Spyware application found

Tabel 3 Event Type False Positive Rule

No.	Event Type	Event Name
1.	Alienvault HIDS - syslog	User Changed Password
2.	Alienvault HIDS – Authentication Success	First time user logged in

Tabel 4 Event Type Login Success

No.	Event Type	Event Name
1.	SSh	Login Succesful, Accepted Password
2.	Alienvault HIDS – Authentication Success	SSHd Authentication Success

The previous tables discuss what event types or events have been configured. If an appropriate event or event occurs it will be sent to Gmail notification. Next, the following is the configuration actions that have been implemented.

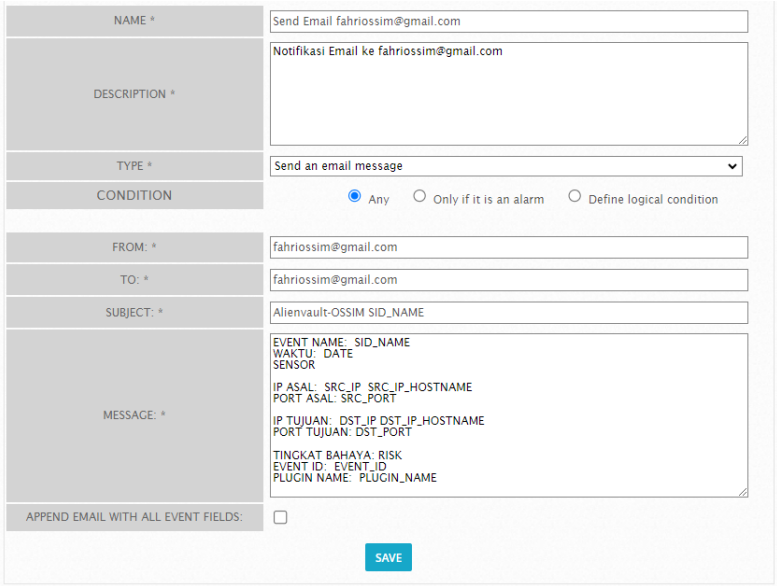

Figure 6 Actions Configuration

Figure 6 shows the display if the user successfully enters the new actions menu and wants to configure the actions. Apart from that, this display is also a display of configuration actions that apply to monitoring IT assets using Alienvault OSSIM. In this display there are columns name, description, type, condition, from, to, subject, message, and save option. Once successful, the following is an example of the results of the notification if an incident or event occurs in accordance with the configuration that has been implemented.

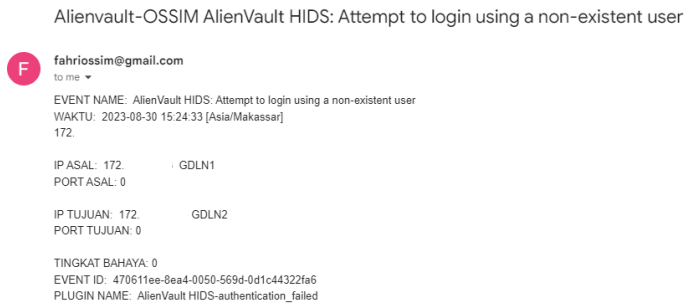

Figure 7 Example of Email Notification Display in Gmail

Figure 7 is an example of an email notification display in Gmail that has been successfully configured. In the email address you can see that the email was sent from "fahriossim@gmail.com" and sent to "fahriossim@gmail.com". This is in accordance with the configuration previously provided. The contents of the email message obtained are in accordance with the configuration previously carried out in Figure 6. In the example of Figure 7, the information obtained is in the form of an Event Name, namely Alienvault HIDS: Attempt to login using a non-existent user, with the time 30 August 2023 at 15:24 :33. This event was detected with the 172.x.x.x sensor in the form of the Alienvault OSSIM IP address. Next, the event originates from the original IP with the hostname, namely GDLN1. The event goes to the destination IP, namely GDLN2. The danger level is 0 (Low). There is also Event ID and Plugin Name information. The Attempt to login event using a non-existent user is an event in the form of an attempted login using a user who has not been registered, or there is no suitable user.

4.3 Results Number of Events

SIEM implementation for monitoring IT assets using Alienvault OSSIM will run from April 22 2023 – July 22 2023. The following are the results of events that have been obtained and grouped based on the IT assets being monitored.

Table 5 Number of Events based on IT Assets

Nama Server	Number of Events
GDLN 1 - AGENT SSH GATEWAY SERVER	150 EVENTS
GDLN 2 - SERVER UNIT VM 11	425 EVENTS
GDLN 3 - UNIT WEB 6 VM 12	29.195 EVENTS
GDLN 4 - WEB 2 VM 12	269 EVENTS
GDLN 5 - SERVER DNS	200.424 EVENTS
GDLN 6 – SERVER RADIUS (WIFI)	159 EVENTS
TOTAL	230.622 EVENTS

Table 5 is a table that discusses the total events for each IT asset. In this table, the total events for all IT assets that were monitored were 230,622 events. Apart from that, it can be concluded that the DNS Server is the busiest IT asset, next, Web Unit 6 VM 12 which is a web server can also be categorized as the busiest.

4.4 Report Event

After completing the monitoring process, you will of course get lots of events. Some of these events can of course become problematic topics and can also be used as references as reports that are worth discussing. The following are several event logs that are used as reports as well as explanations and risks.

Table 6 Report Event

No.	Event Name	Log Event	Explaination
1.	Login Session Opened	LOCATION: "(GDLN4) 172.x.x.x->/var/log/auth.log"; EVENT: "[INIT]May 23 18:50:02 web2-vm12 sshd[8090]: pam_unix(sshd:session): session opened for user usdiadminutbknew by (uid=0)[END]";	There is a login process on GDLN 4 May 23 at 18:50:02. Using user usdiadminutbknew. This activity runs outside office working hours.
2.	New FTP Connection	LOCATION: "(GDLN3) 172.x.x.x ->/var/log/syslog"; EVENT: "[INIT]Apr 28 13:32:58 unit-web6-vm12 pure-ftpd: (?@172.x.x.x) [INFO] New connection from 172.x.x.x [END]";	There was a New FTP Connection process on April 28 which ran on GDLN 3 from IP address 172.x.x.x. This activity carries the risk of file transfers occurring between the server and unknown parties. This happened in 1 trial.

3.	SSHD Authenticati on	LOCATION: "(GDLN4) 172.x.x.x ->/var/log/auth.log"; EVENT: "[INIT]May 23 18:51:00 web2-vm12 sshd[62394]: Accepted password for usdiadminutbknew from 172.x.x.x port 35548 ssh2[END]";	There was an attempt to login authentication via SSH on GDLN 4 on May 23 at 18:51:00. The Authentication process runs using the user usdiadminutbknew. The activity is risky because it occurs outside office working hours, resulting in the possibility of the user login process being carried out by unknown perpetrators.
4.	User Login Failed	LOCATION: "(GDLN4) 172.x.x.x ->/var/log/auth.log"; EVENT: "[INIT]May 7 22:00:21 web2-vm12 sshd[64758]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=172.x.x.x user=soma[END]";	There is activity in the form of login failed. This happened on GDLN 4 on May 7 at 22:00:21 with user soma, this happened in 7 attempts. This activity carries the risk of potentially unwanted login attempts occurring or it could also be a bruteforce attempt if carried out in many attempts.
5.	Host Based Anomaly Detection	LOCATION: "(GDLN2) 172.x.x.x ->rootcheck"; EVENT: "[INIT]Files hidden inside directory '/tmp'. Link count does not match number of files (9,10).[END]";	An anomaly was detected on Host GDLN 2 in the form of hidden files in the '/tmp' directory. This activity carries the risk of files being infiltrated by unknown people into the directory.
6.	SSHD Authenticati on Failed	LOCATION: "(GDLN4) 172.x.x.x ->/var/log/auth.log"; EVENT:"[INIT]May 17 14:26:01 web2-vm12 sshd[51993]: Failed password for soma from 172.x.x.x port 42204 ssh2[END]";	An SSH Authentication Failed attempt was detected on GDLN 4 on May 17 at 14:26:01 with user soma. This experiment occurred 4 times. This activity is at risk of unwanted login attempts or could also be a bruteforce attempt if carried out in many attempts.
7.	Attempt to Login using a non-existent user	LOCATION: "(GDLN4)17k2.x.x.x ->/var/log/auth.log"; EVENT: "[INIT]Jul 1 15:47:34 web2-vm12 sshd[23610]: Invalid user pusat-utbk from 172.x.x.x[END]";	Detected a login attempt on a non-existing user on GDLN 4 on July 1 at 15:47:34. This experiment occurred once with UTBK-center users. This activity carries the risk of possible user guessing or bruteforce attempts if it occurs in many attempts.
8.	First Time User Logged in	LOCATION: "(GDLN4) 172.x.x.x ->/var/log/auth.log"; EVENT: "[INIT]May 16 16:11:59 web2-vm12 sshd[55512]: Accepted password for usdiadminutbknew from 172.x.x.x port 56474 ssh2[END]";	Detected a login process for the first time on GDLN 4 May 16 at 16:11:59. The user is usdiadminutbknew. This activity is at risk if a new user is successfully created and logged in without the administrator's knowledge.

9.	New User Added to the System	LOCATION: "(GDLN3) 172.x.x.x ->/var/log/auth.log"; EVENT: "[INIT]May 21 22:54:01 unit-web6-vm12 useradd[48852]: new user: name=usdiadminicamsac, UID=1065, GID=1004, home=/var/www/clients/client2/web290/ home/usdiadminicamsac, shell=/bin/bash[END]";	Detected the addition of a new user on GDLN 3 on May 21 at 22:54:01. The user is usdiadminicamsac. This activity carries the risk of adding new users without the administrator's knowledge.
10.	User missed the password more than one time	LOCATION: "(GDLN4)172.x.x.x ->/var/log/auth.log"; EVENT: "[INIT]May 17 14:26:09 web2-vm12 sshd[51993]: PAM 2 more authentication failures; logname= uid=0euid=0 tty=ssh ruser= rhost=172.x.x.x user=soma[END]";	An attempt was detected in the form of failed login or incorrect password more than once on May 17 at 14:26:09. The experiment used Soma users. This activity could be at risk of brute force if it occurs repeatedly in many events.
11.	User deleted	LOCATION: "(GDLN3) 172.x.x.x ->/var/log/auth.log"; EVENT: "[INIT]May 21 22:44:02 unit-web6-vm12 userdel[48427]: delete user 'web289'[END]";	Detected deleted user activity on GDLN 3 May 21 at 22:44:02. The user who was deleted was web289. This activity can be at risk of unwanted user deletion and without the administrator's knowledge.

Table 6 is a table containing some activity information on USDI's IT assets after monitoring using Alienvault OSSIM which is used as a report. In the table, the meaning and some of the risks have been explained. These reports can certainly help administrators in evaluating the IT assets they own. Apart from that, the report has been given to the relevant agency, namely USDI. It is hoped that the relevant agencies can pay more attention to the reports provided. Apart from that, overall in the table the risk level or value (Risk Value) is still at a low level (Low).

4.5 Recommendation

After successfully carrying out Threat Monitoring and collecting events which are used as reports. The author provides several recommendations that can be applied to the case study location, namely the Information Resources Unit (USDI), so that it can help improve Information Technology security in the agency as well as the actions taken in handling the event reports obtained. These recommendations are adjusted to the problems in the existing event report. The following is an explanation of several recommendations that can be applied in the following table.

Table 7 Recommendation

No	Event Name	Recommendation
1.	*Login Session Opened*	Carrying out checks on related users and validating whether the user is actually carrying out the login process at a certain time.
2.	*New FTP Connection*	Carrying out checks in the form of identifying the relevant IP that is carrying out the FTP process with the Server
3.	*SSHd Authentication*	Checking the relevant user and validating whether the user is actually logging in via SSH at a certain time.
4.	*User Login Failed*	Apply punishment or penalty if there is Failed Authentication. This can also of course avoid bruteforce experiments.
5.	*Host Based Anomaly Detection*	Examine directories that contain indications of anomalies
6.	*SSHD*	Apply punishment or penalty if there is Failed Authentication

	Authentication Failed	
7.	*Attempt to Login using a non-existent user*	Apply punishment or penalty if there is Failed Authentication
8.	*First Time User Logged in*	Check and validate the names of users who have logged in for the first time
9.	*New User Added to the System*	Check and validate whether a new user has really been added to the system
10.	*User missed the password more than one time*	Apply punishment or penalty if there is Failed Authentication. This can also of course avoid bruteforce experiments.
11.	*User deleted*	Carrying out checks and validation of users undergoing the deletion process
12.	*Port Mirroring*	Implement Port Mirroring with the aim that the Network Intrusion Detection System (NIDS) can be active

Table 7 is a collection of recommendations given to the case study agency, namely the Udayana University Information Resources Unit (USDI). The 10 recommendations given have been implemented during the monitoring process. There is one recommendation that has not been implemented, namely implementing Port Mirroring with the aim of activating NIDS (Network Intrusion Detection System) so that later Alienvault OSSIM can work more optimally in carrying out the threat monitoring process.

5. Conclusion

Based on data processing or previous discussions, the author draws the following conclusions. The implementation was successful by installing Alienvault OSSIM on a server owned by USDI and able to connect to the asset you wanted to monitor. Monitoring was carried out on 6 IT assets, where all Linux-based assets consisted of the SSH Gateway Server Agent, SERVER UNIT VM 11, Web Unit 6 VM 12, Web 2 VM 12, DNS Server, and Radius Server (WIFI). Alienvault OSSIM can work in real time 24/7. So it can minimize negligence and help administrators who cannot monitor the IT assets they own 24 hours a day. There is an email notification feature on Gmail if there is an attack or there are logs that have previously been set in policy. This feature is certainly very helpful for an administrator to monitor the activities of the IT assets he owns. Apart from that, it can also help administrators obtain information about incidents on IT assets that are being monitored so that prevention can be carried out quickly and precisely.

The total number of events collected was 230,622 events. The IT asset that has the most logs during monitoring is owned by the DNS Server with a total of 200,424 Events. Based on this, it can be concluded that the DNS Server is the busiest IT asset during the monitoring process. Apart from that, there are 11 Event Names and 34 event logs which are used as reports with explanations and risks during the monitoring process. There are 12 recommendations that have been given in order to increase USDI's level of security.

The overall final result is based on the logs collected after the monitoring process, there are no attacks, threats, or risks that are very significant or dangerous for the relevant IT assets. No Alert detected. The overall risk category is in the low category.

The impact of implementing Alienvault OSSIM on USDI as a threat monitoring tool is being able to set User Authorization when using the server, being able to help Administrators in reading logs and monitoring servers, Gmail notifications can be integrated on mobile phones so that they can help administrators find out about an incident and can take preventative steps (prevention). Apart from that, Alienvault OSSIM on USDI will continue to be used and continued by USDI.

Daftar Pustaka

[1] Abdullah, B., Budiyono, A., & Widjajarto, A. (2020). ANALISIS KERENTANAN MENGGUNAKAN ALIENVAULT DAN QUALYS PADA SECURITY OPERATION CENTER (SOC) BERDASARKAN FRAMEWORK CYBER KILL ANALYSIS OF VULNERABILITIES USING ALIENVAULT AND QUALYS IN SECURITY OPERATIONS CENTER (SOC) ON CYBER KILL FRAMEWORK menggunakan. 7(2), 6879–6886.

[2] Akmal, M. D., Diah, K., Wardhani, K., Muhammad, D., Fadhly, A., Jurnal, R., Komputer, A., Politeknik, T., Riau, C., Dzul Akmal, M., Arif, D. M., & Ridha, F. (2018). Impelementasi Security Information And Event Management (SIEM) Menggunakan Ossim. Jurnal Aksara Komputer Terapan Politeknik Caltex Riau, 7(2), 1.

[3] Anendya, A. (2023). Mengetahui Pengertian Software, Fungsi, Jenis, dan Contohnya. https://www.dewaweb.com/blog/apa-itu-software/

[4] Arfanudin, C., Sugiantoro, B., & Prayudi, Y. (2019). Analisis Serangan Router Dengan Security Information and Event Management Dan Implikasinya Pada Indeks Keamanan Informasi. CyberSecurity Dan Forensik Digita, 2(1), 1–7.

[5] Bagas, A. (2021). Peran Security Operation Center. Inixindo. https://www.inixindo.id/peran-security-operation-center/

[6] Bambang, W., Handaya, T., & Suteja, B. R. (2019). Laporan Penelitian Pengembangan Manajemen Keamanan Sistem dan Informasi dengan Penerapan Sistem Pendeteksi menggunakan OSSIM alienvault Fakultas Teknologi Informasi Universitas Kristen Maranatha.

[7] Computing, C. (2011). Analisis Performa Network Intrusion Detection System (NIDS) Menggunakan Metode Signature Based Dalam Mendeteksi Serangan Denial of Service (DoS) Berbasis UDP Flooding Muhammad Rien Suryatama Idrus ABSTRAK Analysis Performances of Network Intrusion Det.

[8] Cybersecurity, P. (2022). Security Operation Center. PROTERGO CYBERSECURITY. https://protergo.id/services/x-force-security-operation-center/

[9] Datacomm Cloud. (2017). Mengenal apa itu SIEM. Datacomm Cloud Business. https://datacommcloud.co.id/mengenal-apa-itu-siem/

[10] González-granadillo, G., González-zarzosa, S., & Diaz, R. (2021). Trends , and Usage in Critical Infrastructures.

[11] Hadiansyah, C., & Iskandar, I. (2020). Pembangunan Server Security Information Management Untuk Monitoring Keamanan Di Server Diskominfo Provinsi Jawa Barat. 1–8.

[12] Himawan, B., Hidayat, T., Detection, H. I., & Hids, S. (2007). Perancangan Host-Based Intrusion Detection System Berbasis. 2007(Snati), 69–73.

[13] Huda, N. (2022). SIEM: Pengertian, Cara Kerja, serta Perbedaannya dengan SOAR. https://www.dewaweb.com/blog/pengertian-siem/

[14] Jho. (2023). Apa itu DNS Server: Definisi, Fungsi & Cara Kerja! https://www.jogjahost.co.id/blog/dns-server-adalah/

[15] Kurniawan, B. (2022). Pengertian IDS, Cara Kerja, Jenis, Komponen, dan Contoh IDS.

[16] Lord, N. (2020). What is Threat Monitoring?

[17] Moedasir, A. (2022). Visi dan Misi Adalah: Perbedaan, Tujuan, dan Contoh. https://majoo.id/solusi/detail/visi-dan-misi

[18] Napizahni, M. (2023). Pengertian Hardware, Fungsi, Cara Kerja, Jenis, dan Contohnya. https://www.dewaweb.com/blog/apa-itu-hardware/

[19] Novi, V. (2021). Pengertian Struktur Organisasi: Fungsi, Jenis, dan Contoh. https://www.gramedia.com/literasi/supply-chain-management/

[20] Onno. (2021). OSSEC.

[21] Prasetio, Y. L. (2018). No Title. https://socs.binus.ac.id/2018/12/20/arsitektur-informasi/#:~:text=Arsitektur informasi akan membantu user,informasi dengan baik dan terstruktur.

[22] Rihal, M. (2019). Implementasi Dan Analisa Security Information Management Menggunakan OSSIM Pada Sebuah Perusahaan. Skripsi Fakultas Teknik, Program Studi Teknik Informatika.

[23] Riset, K., Dan, T., Tinggi, P., Tinggi, S., Informatika, M., Komputer, D. A. N., Juansyah, A., Pratama, B., & Dian, I. (2021). Analisis Dan Implementasi Open Source Security Pada Keamanan Jaringan Komputer.

[24] Roestam, I. R., Sc, M., & Ph, D. (2021). Monitoring Jaringan Dengan Memanfaatkan Ossim Alienvault Pada Pt . Metalogix Infolink Persada.

[25] Shinta, A. (2022). Pengertian Port, Jenis, dan Fungsinya pada Jaringan Komputer. https://www.dewaweb.com/blog/apa-itu-port/#Physical_Port

[26] Wikipedia. (2022a). Berkas log.

[27] Wikipedia. (2022b). OSSIM. https://en.wikipedia.org/wiki/OSSIM

[28] Yasin, A., & Mohidin, I. (2019). Monitoring DDOS Pada Openflow Switch Dengan Alienvault Ossim. Jurnal Teknologi Informasi Indonesia (JTII), 3(2), 23. https://doi.org/10.30869/jtii.v3i2.260

[29] Yasin, K. (2019). Apa Itu SSH dan Bagaimana Cara Kerjanya? https://www.niagahoster.co.id/blog/apa-itu-ssh/?gclid=CjwKCAjwo9unBhBTEiwAipC11-y9jIK51iBRUxuSQJZ7zDOujTQkNg4r-yztqAGeg_Pbk-6_COMQMBoCCyAQAvD_BwE