Group Members :-

Muhammad Izham Bin Norhamadi , B032020039 , S2G1

Ahmad Sha Herizam Bin Tahir, B032020009, S2G1

Muhammad Zahid Bin Saiful Adlan, B032010363, S2G1

Muhammad Haikal Bin Rosli, B032010336, S2G1

4.0 Exercise of ESM Implementation

Student needs to answer questions based on the ESM installation and implementation that student has chosen. The questions are:

a. What did the packet type show in the interface?

- Host data sources
    - System packages
    - Processes
    - Logins
    - System logs

- Network data sources
    - Flows
    - DNS
    - Other protocols

b. What is the packet size (in Mbps)?

- Agent: 1.5Mbps

c. What is the Timestamp for the packet in and packet out?

- YYYY-MM-DD HH:MM:SS

d. Identify some nodes? Yes / no?

-

e. List the protocols that have been implemented on the interface.

- System Logging Protocol
- Network Time Protocol

f. Does the ESM product provide the graph or a dashboard for easy the task of an administrator?

- Yes, SIEM Elastic provides a dashboard that summarizes the detection trends, external alert trends, events, host events, and network events

5.0 Exercise

a. Elaborate the objective of ESM in page 6 of slide chapter 4.

Align business and IT strategies

Every security procedure in ESM must have taken good measure especially to align with the business. The investment made with security in every aspect should support the goal of the business to make sure business and IT go well without problems.

Increase business and IT agility

If we always keep up-to-date with the current trend of ESM and can spread knowledge of the newest software or technique of security protection, automatically business will keep increasing. For example, we will have full trust of our client if the client is fully aware of our security measure in our business. This not only will keep the trust of clients but we might get new clients for our safe and protected business.

Establish and refine future architecture vision

As we know, we don't know what the future will hold for us. That's why ESM is really important to refine the future architecture vision. If we have full knowledge of ESM, the complicated architecture that will become the main priority in the future can be securely overcome.

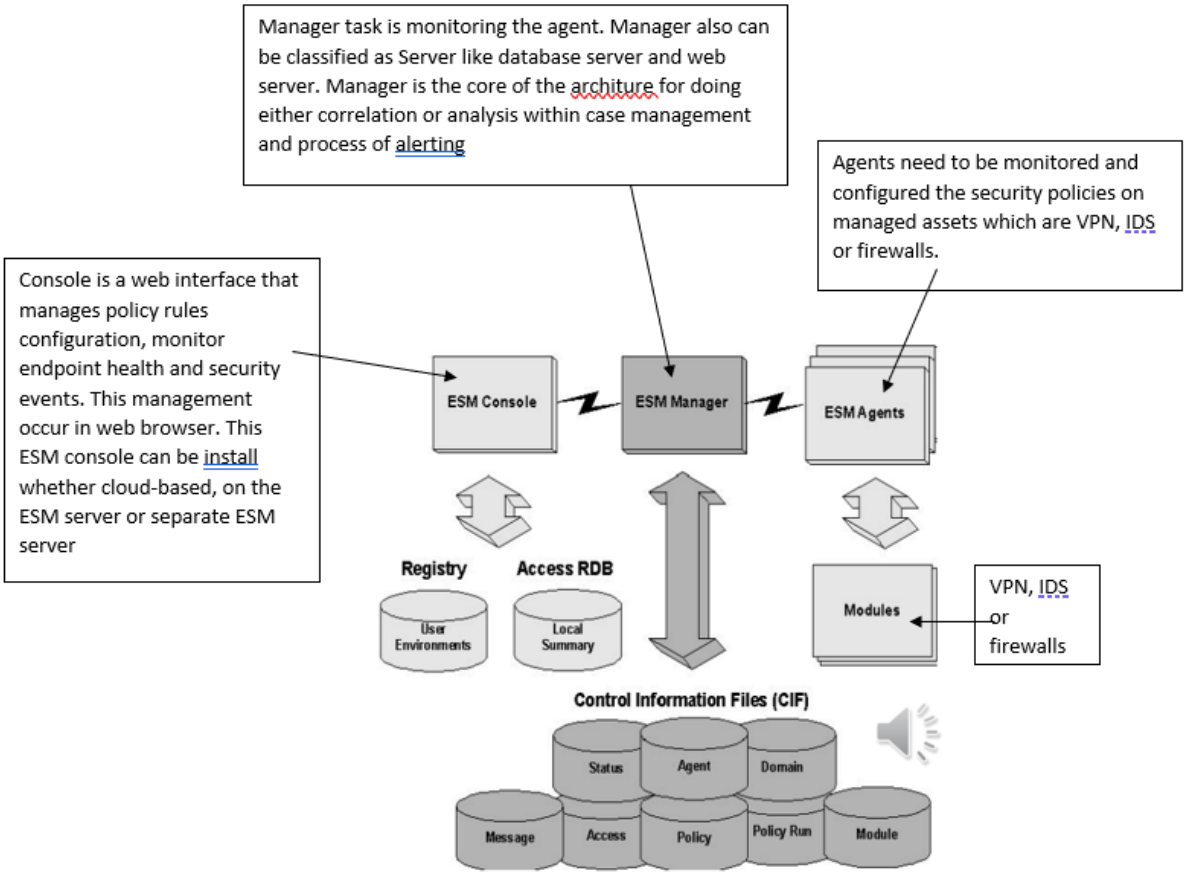
Govern technology decision and direction

In most formal organization, every step to handle any case or problems of security management must have to use reliable and effective procedures. The usage of ESM in this scenario is to make sure every decision made within any formal environment can be easily achieved without any authorized problems occurring.

b. Why does the ESM is important to the enterprise network?

In this modern era, cybersecurity threats keep evolving from time to time and everything related to the internet can face dangerous attacks from any malicious source. This is why ESM is needed to prevent any threats. Other than that, ESM is needed in terms of communication since information flow through the communication might be really important toward an organization. That's why a secure line of communication must be established to make sure there's no leak of information occuring.

c. Explain the ESM architecture and provide an illustration to show the explanation.



d. Explain the component of ESM

EEM- Provide registration to the event in a private access and authentication through a gateway. Password with smartcard or biometrics are used for verification in order to access the system.

SIM- System of management framework facilitating the collection, retention and translation of security control data into relevant risk management information. SIM includes log data generated from antivirus, IDS, IPS file systems, firewalls, routers, switches and servers to discover problems within a system.

SEM- real time monitoring and event management to support IT security operations. SEM notifies network administrators about potential issues.

SIEM- Is a set of tool that combine SIM and SEM. SIEM provides centralize storage, interpretation and analysis of logs, events and other generated logs executed from various of devices.

e. What is SOAR?

SOAR stands for Security Orchestration, Automation and Response. SOAR is a stack of compatible software programs that helps an organization or facilities to gather information of security threats from any security events that occur with the response of the system. This procedure happens without the help of any human assistance. This program is to make sure the efficiency of not only digital security but physical security to the maximum level.

From the name itself, we can see that SOAR can be divided into three main components: Security Orchestration, Security Automation and Security Response.

The first one is Security Orchestration. This component of SOAR by using built-in or even custom integration and application programming interfaces(APIs), it can connect as well as integrate disparate internal and external tools. Some examples that will include in the connected system us firewalls, endpoint protection products and vulnerability scanners.

The second one is Security Automation. All the data and alerts gathered from the Security Orchestration will be analyzed and the data then creates a repeated and automated process as we can see from the name itself. This automated process is to replace the existing manual process. For example, an analyst tasks such as log analysis, auditing capabilities and vulnerability scanning can be executed by SOAR automatically. SOAR automation can make vast responses and recommendations automatically by using AI and machine learning to adapt insights from analysts.

The last one is Security Response. This component is to help the analysts once a threat is successfully detected. Analysts can get a single view into the planning, managing, monitoring and reporting of actions carried out. Post-incident response activities also include in the component.

f. What is COAR?

COAR stands for Cloud Orchestration, Automation and Response. Unlike SOAR which specialize in security, COAR is more leaning towards cloud management. COAR aggregates security intelligence and context from disparate systems. It uses machine intelligence. This is because it reduces the time of the incident detection and response process.

Same as SOAR, COAR also can be divided into three components which are Cloud Orchestration, Cloud Automation and Cloud Response.

Cloud Orchestration is about arrangement and coordination of automated tasks that will give a result of consolidated workflow or process. This component can reduce cost of management and offer a systematic approach that can give full potential of automation benefits. Cloud orchestration also give opportunity for business to accelerate delivery either for new innovation, application or hybrid infrastructure by orchestrating processes across systems, domains and teams.

The second components is Cloud Automation is occur in cloud environment in execution of workflows by using the automated tools and processes otherwise it have to be performed manually. This components give advantage of cloud resources efficiently and avoid any security failures which might happen if teams rely too much on manual workflow.

The last component in the COAR is Cloud Response which is an approach to cloud security in defending cloud infrastructure and application from any kind of threats such as insider threats and access misuse. Cloud Response offers data-driven analytics and visibility to investigate, analyze and mitigate threats in the cloud environment. This component also focuses on providing continuous, consolidated visibility of users, privileges and any event occurring across cloud applications and services.