SOC-IT: Setting up Security Operation Center using full open source tools

PREAMBLE

IT-Security is a medium-sized company has decided to implement a Security Operation Center. It is a dedicated site where the enterprise information systems (web sites, applications, databases, data centers and servers, networks, desktops and other endpoints) are monitored, assessed, and defended.

The SOC enhances significant efficiency to provide detection and reaction services to security incidents as well as cost-saving to the company.

The SOC team is also charged of finding malicious and suspicious activity happening on the networks or systems. The team reviews the alerts, performs a filtering and research process then decides the level of risk the threat represents. The combination of proper tools and the members' experience guarantees the success of the SOC team**.**

The goal of this project is to deploy and integrate open source security solutions for network monitoring and event analysis to detect attacks and anomalies. These solutions are generally based on a central log and event management system combined with tools for collecting and analyzing network traffic and systems.

The project consists of designing a functional and technical architecture, benchmarking open source solutions, installing and testing the solutions chosen to integrate them in the same environment.

You have received this project specification sheet and are asked to study technically the overall physical and virtualized systems from both functional and security point of views. The objective is to emulate the SOC department physical infrastructures and the wide area network used for interconnection. You have to deploy sample services and applications on the top of the virtualized infrastructure. Furthermore, you need to install or develop appropriate security solutions for both physical and virtual infrastructures. Finally, you need to test the robustness of these solutions against attacks and to write a detailed report.

PROJECT OVERVIEW

The objective of this project is to design, implement and integrate open source security solution for network monitoring and event analysis to detect attacks and anomalies. The PoC must include:

i. Infrastructure: A central infrastructure services and software based on SOC.
ii. Different sites (A minimum of 3): Emulating local area networks of each site and their connection to the wide area network.
iii. DMZ Network emulation connect to infrastructure.
iv. Sources of attacks: emulation of attacking machines (attacks against both physical and virtualized infrastructure).

The SOC must ensure the following requirements:

i. Sensor or probe to monitor the traffic coming in and out both private and demilitarized zone.
ii. Incident response mechanism to report alerts.
iii. Visualization platform for analysts.
iv. Threat intelligence platform.
v. Honeynet (Centralized management of Honeypots) to trick attackers and gather information about intruders.
vi. Servers and services monitoring.
vii. Management interface for analysts to control and deploy sensors.

PROJECT DETAILS

This paragraph describes in details the requirements of the aforementioned PoC.

1. Security department networks and their communication with SOC infrastructure

i. Each site hosts its own networking services (e.g., Host configuration, Domain name resolution)
ii. Isolate the internal network infrastructure department from the risks of exogenous traffic and attacks.
iii. Secure and authenticated communication between department and the SOC site.

2. Security of physical infrastructure

i. physical infrastructure must be protected against classical cyber-attacks (intrusions, spoofing, denial of service, etc)
ii. A monitoring of the physical infrastructure must be allowed.

1. What is an operational security center (SOC)?
2. What are the different types of SOC models?
3. Why did organizations choose the SOC?
4. Is the management console configured by the strict access controls and is it locked for specific users?
5. Why are SOC's created?
6. Are controls applied to specific users for the aim of limiting access or read/write
7. capabilities?
8. How to structure a SOC?
9. Are software licenses up-to-date?
10. How monitors for threats?
11. When should you set up a SOC?
12. When your threat landscape requires dedicated security resources?
13. when your monitoring and workflows are ineffective?
14. Are all unused devices disconnected from the virtual machine?
15. How is network traffic on a virtual machine authenticated?
16. Have most recent security patches been applied to guest and host operating systems?
17. Are patches tested before they are installed in a production environment?
18. Are any reports or alerts generated?

4. Deploying department' services and applications on IT-Security

Services and applications of each department must be hosted in virtual machines of the virtualized infrastructure. For each emulated department, at least the following services/software have to be deployed and secured:

i. Web service protected from communes' web attacks
ii. Mail service integrated with antimalware solutions
iii. File transfer service secured
iv. Directory information service
v. Anti virus…...

DELIVERABLES

You are invited in addition to the SOC to furnish the following documents:

1) A presentation of a general approach for carrying out the project. This approach contains:

- ✓ Scope of the project
- ✓ Objectives
- ✓ Resources needed (human and material resources)
- ✓ Constraints and Assumptions
- ✓ Cost and Its Relationship to Price
- ✓ Work Breakdown Structure

2) A technical study that contains the presentation of technical and organizational solutions that can be adopted. This study should contain a detailed architecture with all the products and solutions that will be installed.

3) A Work schedule that contains:

- ✓ Activity definition
- ✓ Activity sequencing
- ✓ Activity duration estimating

Additional information

1. All documents related to this project must be written in English.
2. Tutors have the right to add additional services and change chosen technical choices.