Develop a Monitoring Solution

Reading

30m - 45m

Status | Incomplete

Introduction

In the *Develop a Monitoring Solution* reading, you will be introduced to a case study where you will utilize the knowledge learned in the *Windows and Linux Logs, IoCs and Monitoring* portions as well as the *Network Monitoring* portions of the course in order to help Cat plan and set up a monitoring solution for the organization in the case study.

Case Study: Cat Scan II Big Dog

Case Study Overview

In this case study, you will provide a monitoring solution that covers key components in the client's infrastructure, protecting their key assets. Consider the following points to make sure you address all the needs of the organization:

- You will have to assess the assets and the data the organization has to ensure that you are putting the right emphasis on the right items.
- Make sure you take into account all the information you are given, ensuring that the items you choose to put sensors and alerts on are the ones that will best identify known IoCs.
- Additionally, ensure that you are putting the most sensors as well as the correct sensors on items to which you have assigned the high priorities.
- Use Industry Standard resources like NIST, and MITRE to help you research known vulnerabilities and the IoCs that should be monitored to help protect them. And don't forget to include Industry Best Practices in your considerations.
- Be sure you understand why you are recommending each sensor and alert threshold as you will have to justify your decisions.
- You may also recommend basic monitoring of logs, events, and SNMP for the scenario given in the case study.

Case Study Tasks

In this case study, you will help Cat by recommending PRTG with sensors and alerts thresholds to be set up in her Network Monitoring tool (PRTG); you will identify end-points and research potential vulnerabilities that they may have. To do so, you will start with creating a list of assets in the Big Dog organization, prioritize these assets by importance, and discover the vulnerabilities and risks associated with each asset (eg. SCs and SILs). Then, you will finally create a formal report, which is also your project for the course, outlining your findings for the Big Dog organization, including information, such as prioritized sensors with alert thresholds, IoCs, vulnerabilities, risks, threats, tactics and techniques, monitoring recommendations, etc.

> ⚠ Note, you will work on this case study/ project through this entire unit. As a part of working on this case study/ project, you will complete the following tasks:

- First, read and analyse the case study scenario given in this reading (i.e. *Develop a Monitoring Solution* reading),
- Then, create a list of risks and vulnerabilities in the next activity (i.e. *List of Risks and Vulnerabilties* task), and discuss the same with your peers,
- Document additional findings and insights as you research for the risks and vulnerabilties (during the *Tools Research and Documentation* task),
- Finally create a report as per the provided template (in your final project *Report on Risks & Vulnerabilities*). Creating a report is the last step in the case study/ project.

So, let's take the first step and understand the actual scenario you will be working on in this case study.

Scenario: Cat's New Gig, Big Dog

Thanks to your help, Cat has been given a larger project, Big Dog, and is now in charge of securing a larger network, with more systems. In addition, as she has become more aware that monitoring network traffic is also important, she will be adding some network monitoring to the list of items she will be looking at.

Cat is in charge of securing a business that uses a mix of Windows and Linux-based systems. As she has other duties in the company, she has chosen to use a central monitoring system on the server, PAESSLER's PRTG. The system has been installed, and the systems that need to be monitored have been added to it. Her next step is to make sure that the appropriate sensors have been added to the systems for monitoring key items and that proper thresholds have been set for alerts. As one of the systems is a server, she wants to focus most of her attention there, but also remembering that the Windows Workstation and Linux system are used for development, and the Windows Server system has an SQL database that needs to be watched.

Cat figures that she should have approximately 20 sensors to monitor, with alert thresholds, though she could use more if needed. She does not want to be overwhelmed with information or unneeded alerts. Since she has put a limit on the number of sensors, she feels she should have a rationalization for the use of each.

The Client – Big Dog

The client, Big Dog, has a network that can be generally be broken down like this:

- Windows Server, runs:
    - SQL database
    - IIS webserver
    - PRTG Network Monitor
- Linux:
    - Used by developers to create important proprietary intellectual property (IP) for the company
- Windows workstations:
    - Sales
    - Marketing
    - Management functions
- Kali
    - Test systems
    - IT systems

The heads of the company have stated that all company information falls within the following classifications:

- Privacy (P),
- Proprietary (IP),
- Financial (F),
- Admin (A),

- Security mManagement (SM),
- Systems (S)

They have further ranked the importance of each class of information from most important to least important as follows:

- Privacy (P)
- Proprietary (IP)
- Admin (A)
- Financial/accounting (F)
- Security Management (SM)
- Systems (S)

For Students using Eve

> When completing your vulnerability and risk research and prioritization, you can use the OS/software versions found in your EVE lab environment as those that are found in the Big Dog architecture.

For Students using VirtualBox

> When completing your vulnerability and risk research and prioritization, you can use the OS/software versions found in your VirtualBox lab environment as those that are found in the Big Dog architecture.

Conclusion

Now that you have understood the scenario, let's begin by creating a list of risks and vulnerabilities as our next activity.

✓ Mark Completed

Previous
Case Study: Identify the Attacks

Next
List of Risks and Vulnerabilities

W02D5

Fri Jul 5

› Outline & Notes (1)

› Lectures (1)

⌄ Work (9)

11 hrs

- Assessing Scenarios
- Case Study: Identify the Attacks
- Develop a Monitoring Solution
- List of Risks and Vulnerabilities
- Tools Research and Documentation
- New Project Open
- Project: Report on Risks & Vulnerabilities
- TIs: How to Prepare
- TIs: Study Guide

› Other (1)

W02D5 Schedule »