Report on Risks & Vulnerabilities

Evaluated Project

w02d5 → w03d1

Not Submitted

In this project, you will create a report that gives recommendations on sensors that should be monitored, associating the sensor with well known IoCs for the organization in the case study. The report explains what sensors should be used, prioritizing them and connecting them to IoCs, threats and vulnerabilities. It specifies what alert thresholds need to be set and why.

My Submissions

The status of your previous submissions to this project are displayed here. However, you have not submitted this project.

Submit Project

Description Eval Rubric

Project Description

This is your project activity for this course! In this project, you will create a formal report outlining your findings for the company in the case study Cat Scan II given a set of pre-selected sensors. While working on this report, you will focus on coming up with a rationale of prioritization, based on the sensor used and the IoCs that they assist in monitoring. You will prioritize based on the prioritization of the asset being monitored, vulnerabilities, threats, tactics, techniques, and risk severity to the organization, and prepare monitoring recommendations for the company in the case study.

Instructions

Using the information you have collected on your own and from group & class discussions, as well as using the table given below, complete the case study tasks given here and then write a formal report outlining your findings for the Big Dog organization.

> ℹ On communicating with Cat and reviewing the Big Dog environment, the following table has been started; the column headings of the table have been explained here:

- **Sensor**: Generic sensor name
- **Description**: A short non-technical description of the sensor
- **System**: The endpoint that the sensor will be monitoring
- **IoCs**: The Indicators of Compromise that the sensor is expected to monitor
- **Rationale**: Why this sensor may have been chosen, linked to MITRE or some other framework information
- **Priority**: Based on the nature of Risk/IoC/SIL, etc.

- **Thresholds/ Assumptions**: Based on what is monitored, do we monitor for a high condition, a low condition or both and why? This column can also be used to specify any assumptions made.

> ℹ Sample explanations/ examples are given in the table in the ***bold and italic format***.

Sensor	Description	System	IoCs Associated (May be more than 1)	Rationale	Priority	Thresholds /Assumptions
HTTP Load Time	***Monitors the time it takes for the page to load.***	***Linux***	***May be used to indicate Malicious Redirects, DDoS Attacks or Content Injection***	***Unexpected changes in load time can indicate anomalies or performance-related issues that could be indicative of a security breach or compromise***	***Medium (SIL of high, see assumptions)***	***Changes of 20% over the average load. SIL base on the fact that BIG DOG does NOT have a large Web Presence, the linux web server being internal and this one outward facing(Assumption) There is a relatively low impact on CIA (specifically A) but a higher chance of compromise I have assigned an SIL of high***
HTTP Load Time		Linux				
MySQL Database Query Sensor		Linux				
SSH Sensor		Linux				
Antivirus Status Sensor		All				
File Sensor		Linux				
Windows Event Log Sensor		Windows11				
Windows Event Log Sensor		Windows11				

Bandwidth Usage Sensor		All				

Case Study Tasks

- Cat has provided a list of sensors (in the table given above) she wishes to add. Complete the table!

> Revisit the column headings explanations given above as you try and complete the table.

- Justify your selections, as is recommended by the NIST RMF, by giving Cat a Security Impact Level (SIL) for each item/system monitored.

> You are encouraged to record your justifications/ notes in your PKM; you may need these notes while writing your case study report.

- Make sure you use SILs as part of your priority selection so she can arrange her dashboard to show the most important items.

Case Study Report

> Once you have completed all the tasks, create a formal report; make sure you include the following elements and information in your report:

- Include an executive summary and overall conclusions.
- The completed table.
- List and explain the IoCs as they relate to vulnerabilities and risks/threats covered by the sensors.
- Explain why you have prioritized them the way you have(set SIL) (this includes the risks and the company's associated tolerances, and threats and the associated CIA impacts they may cause).
- Specify what alert thresholds need to be set and why. You do NOT need to specify numbers, just if high, low or both conditions evaluate to a potential compromise.
- Tie your findings and recommendations together with industry standard framework and tool references.

> Follow the template given below to prepare the formal report.

- **Title**: Title of the report should be Cat Scan II Big Dog.
- **Executive Summary**: A short, one or two paragraph summary explaining what you have done. Include information about the top five SILs and the sensors and thresholds you are monitoring or recommending.
- **Table of Sensors**: Complete the table as required; give appropriate explanation wherever required.
- **Discussion Section**: A discussion of each of the connections between the sensors, IoCs and thresholds.
- **Recommendation Section**: A recommendation section where you should recommend how the client might enhance the security of their systems (for example added sensors); you must cite industry best practices as you make your recommendations.

Video Presentation

After you are done creating the report, create a video presentation overviewing the executive summary of your report for the case study Cat Scan II.

> Follow the instructions given below to create your executive summary presentation:

- Create a video (five minutes maximum) of yourself giving a verbal overview of the executive summary for your report you prepared for the case study Cat Scan II.
- Be sure to present your executive summary as if you are talking to executive members of the Big Dog company.
- You can show yourself talking or present a slideshow with you talking about it, the choice is yours, but your peers and instructors must hear you presenting your findings.
- Once done, include the link to the video presentation in the report.

Project Outcomes

By the end of this project, you should have created a report which includes:

- Completed table of sensors, each described, with suggested alert thresholds, and tied to appropriate vulnerabilities/risks and IoC(s) supported by industry standard frameworks and tools
- A prioritized list of sensors and any other recommended monitoring mitigations, with alert threshold suggestions and associated IoCs and risks supported by industry standard frameworks and tools
- Explanations and rationales for the decisions you have made while selecting alert thresholds, and recommending security posture and monitoring improvements
- Link to the video presentation of the executive summary

Submission Guidelines

- For this project, you will need to submit a link to a Google doc that contains your report. This report will be evaluated.
- Remember, when submitting any project, share the Google drive link to the doc/ folder where you have saved your final project. Ensure that you have selected the option to allow access to all.
- To submit your project, use the *Project Submission* button given at the top and follow the instructions.

> After you have submitted the report, you may also share it with your peers on Discord. This allows you to understand the list sensors and systems they decide to monitor, along with with their prioritized thresholds, and compare it with your approach and decisions.

Evaluation Guidelines

Here are some things you'll need to keep in mind for this evaluated project:

- Familiarize yourself with the Eval Rubric tab so you can read about the competencies you will be evaluated on for this particular project, and review what the different levels of each competency require.
- If you receive Unsatisfactory for any competency, your project will be rejected. If this happens, you will need to review the feedback provided, make changes to your project based on that, and resubmit your updated project within 48 hours in order to get it accepted and stay on track. This is not a bad thing; having to resubmit is an opportunity for you to improve.
- Please ensure that you submit your project in a timely fashion to help ensure you get feedback as soon as possible.

Citation Requirements

Whenever you use an idea or information from a work originally written/ developed by someone else (a journal article, textbook, website, etc.), you must cite the original author or the source to clearly identify where the information came from. You must cite sources of information. For example: - When looking up IoCs, cite NIST NVD - When looking up vulnerabilities, cite MITRE CVE - When looking up industry standard mitigations, cite MITRE ATT&CK, etc.

> ⚠ Note, a citation format for an online resource (such as a website) is different from that for a publication (such as a textbook).

For example, if you utilize information from this website in your work, the citation would look like this:

A guide to digital forensics and cybersecurity tools. Forensics Colleges. (2022, May 19). https://www.forensicscolleges.com/blog/resources/guide-digital-forensics-tools

However, if the information is coming from a textbook (such as, Principles of Information Security (6th Edition), the citation would look like this:

Whitman, M., & Mattord, H. (2017). Principles of information security (6th ed.). CENGAGE Learning Custom Publishing.

> ℹ You may use tools, like Citation Machine, to generate citations for your work.

All the resources you access should be listed in a References List at the end of your work.

> ℹ In the Cyber Security industry, there is no one format for citing references that is broadly accepted for generally all situations. However, the widely accepted citation format is the APA format which you may also follow for your project work. Once you enter the industry, you may follow the citation style followed by your organization.

Report on Risks & Vulnerabilities

Mon Jul 22

Project Details »