CS 405 Module Five Case Study Guidelines and Rubric

Overview

Study a specific case of your choice that documents a notable, large-scale security breach and provide an analysis based on the outline provided below.

Prompt

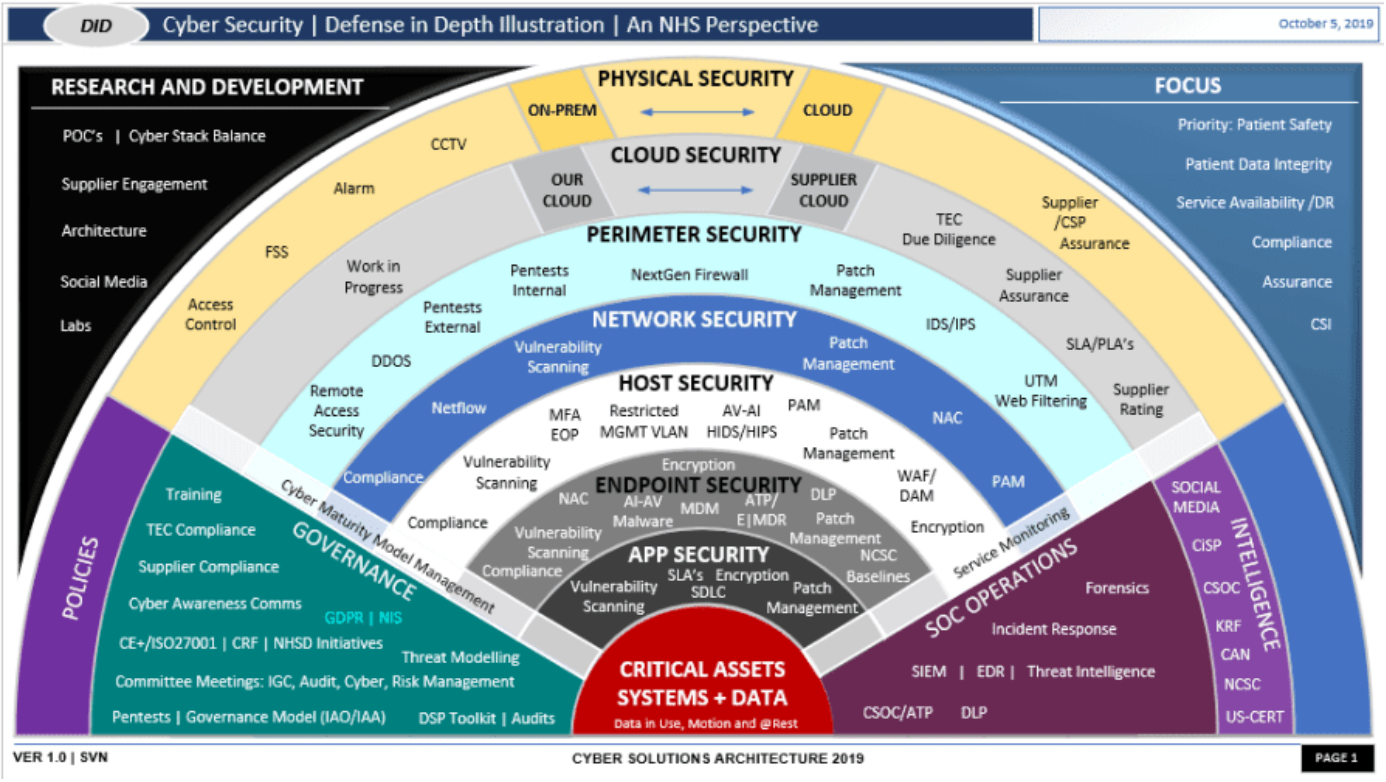
The purpose of this case study analysis is to present a short analysis of a security breach of your choice and reflect on the lessons learned. Your chosen security breach should be recent or within the last five years. It is best to avoid selecting politically charged topics. Refer to the Norton article What Is a Security Breach? for language describing security breaches. You may use the outline provided below to produce your case study analysis.

Examples of security breaches: Use the list in The 15 Biggest Data Breaches of the 21st Century as a starting point to research your chosen case. Other examples include the following:

- A Breakdown and Analysis of the December 2014, Sony Hack
- A Case Study of the Capital One Data Breach PDF

Defense-in-Depth Illustration

This illustration provides a visual representation of the defense-in-depth best practice of layered security.



(Source: https://www.peerlyst.com/posts/nhs-healthcare-defense-in-depth-shaun-van-niekerk)

Outline

- Introduction
  - Name of case and link
  - Date of case
  - Why did this case make the news?
- Describe the breach
  - Type of security or data breach or combination

- Why was this company a target?

- Identify the threat(s)
  - Immediate threat(s)
  - Potential threat(s) if the vulnerability goes unresolved
- What could a developer have done to prevent this breach?
  - Which policy or policies will help prevent this type of attack?
- Summarize the case by explaining the role of best practices, Triple A and defense in depth in preventing future attacks.
  - Authentication
  - Authorization
  - Accounting
  - Defense in depth

What to Submit

Submit a 1- to 2-page Word document with 12-point Times New Roman font, double spacing, and one-inch margins.

Module Five Case Study Rubric

Criteria	Exemplary (100%)	Proficient (85%)	Needs Improvement (55%)	Not Evident (0%)	Value
Introduction	Meets "Proficient" criteria and the details of the explanation reveal a comprehensive grasp of the connection between the security issues and the risks associated with them	Introduces the name of the case, provides a link to the case and the date of the case, and explains why the case made the news	Shows progress toward proficiency, but with errors or omissions; areas for improvement may include organization of elements	Does not attempt criterion	10
Breach Description	Meets "Proficient" criteria and the details of the explanation reveal a comprehensive grasp of the connection between the security issues and the risks associated with them	Describes the type or types of security breach and thoroughly explains why the organization was a target	Shows progress toward proficiency, but with errors or omissions; areas for improvement may include organization of elements	Does not attempt criterion	10
Threat(s) Identification	Meets "Proficient" criteria and the details of the explanation reveal a comprehensive grasp of the connection between the security issues and the risks associated with them	Explains the various threats and the consequences if the threat goes unresolved	Shows progress toward proficiency, but with errors or omissions; areas for improvement may include organization of elements	Does not attempt criterion	15
Attack Prevention Strategies	Meets "Proficient" criteria and the details of the explanation reveal a comprehensive grasp of the connection between the security issues and the risks associated with them	Describes how the attack exploits the vulnerability and how secure coding and principles could prevent a future attack	Shows progress toward proficiency, but with errors or omissions; areas for improvement may include organization of elements	Does not attempt criterion	20
Application of Triple A	Meets "Proficient" criteria and the details of the explanation reveal a comprehensive grasp of the connection between the security issues and the risks associated with them	Describes how at least two out of the three Triple-A concepts could be used to mitigate or respond to this risk	Shows progress toward proficiency, but with errors or omissions; areas for improvement may include organization of elements	Does not attempt criterion	20
Application of Defense in Depth	Exceeds proficiency in an exceptionally clear, insightful, sophisticated, or creative manner	Defends against a single attack using multiple strategies	Shows progress toward proficiency, but with errors or omissions; areas for improvement may include organization of elements	Does not attempt criterion	20

Articulation of Response	Exceeds proficiency in an exceptionally clear, insightful, sophisticated, or creative manner	Clearly conveys meaning with correct grammar, sentence structure, and spelling, demonstrating an understanding of audience and purpose	Shows progress toward proficiency, but with errors in grammar, sentence structure, and spelling, negatively impacting readability	Submission has critical errors in grammar, sentence structure, and spelling, preventing understanding of ideas	5
				Total:	100%