Course Code: 8H161GW

Course Title: Cybersecurity Breach Response Case Studies

Description:

In this course, you will explore incident response methodologies and security models, and will learn to recognize and categorize key types of vulnerabilities and associated attacks against today's organizations. You will do an in-depth review of several past and recent breaches to learn how they were detected and what was done, or could have been done, to reduce the threat risk to the organization. Finally, you will explore the costs of data breaches through research studies and well known breaches.At the end of this course, you will select and research a cybersecurity breach in the news today. You will apply your knowledge and skills from this course and previous cybersecurity courses to analyze the type of attack, attack timeline, vulnerable systems, and any missed opportunities. This project will be graded by the course instructor.This course is intended for anyone who wants to gain a basic understanding of cybersecurity. This is the seventh and final course in a series to acquire the skills to work in the field as a Cybersecurity Analyst**.**

Objectives:

In this course you will learn to:

- Discuss the actions recommended by the National Institute of Standards and Technology (NIST) for establishing an incident response capability
- Describe critical considerations for assembling an incident response team
- Identify the essential requirements of each ase of the incident response lifecycle
- Configure automatic processing of inbound email using the IBM Resilient platform
- Describe each ase of a cyberattack detailed in the IBM X-Force IRIS cyberattack framework
- Identify tips for preventing cyberattacks
- Describe data breaches, including their common characteristics
- Summarize the timeline of the Target Corporation data breach
- Identify vulnerabilities exploited in the Target Corporation data breach
- Describe the cost of the Target Corporation data breach
- List measures that could have prevented the Target Corporation data breach
- Explain how watering hole attacks work
- Explain how ishing scams work
- Describe different types of ishing scams
- Identify the common signs of a ishing email
- Describe the impact of ishing on individuals and corporations
- Identify common types of identity theft
- Summarize the timeline of the Facebook and Google ishing breach
- Identify vulnerabilities exploited in the Facebook and Google ishing breach
- Describe the cost and impact of the Facebook and Google ishing breach
- List measures that could have prevented the Facebook and Google ishing breach
- Explain the objective of a Point-of-Sale (PoS) breach
- Describe PoS systems, including their security standards
- Explain how malware infects PoS devices
- Identify the different types of PoS malware
- Explain what happens to information stolen in a PoS breach
- List best practices for preventing PoS breaches

- Summarize the timeline of the Home Depot PoS breach
- Identify vulnerabilities exploited in the Home Depot PoS breach
- Describe the cost and impact of the Home Depot PoS breach
- List cybersecurity measures implemented to combat attacks such as those used in the Target and Home Depot breaches
- Define third-party breach
- Describe the types of third-party breaches
- List best practices for preventing third-party breaches
- Describe the impact of third-party breaches on individuals and businesses
- Summarize the timeline of the Quest Diagnostics third-party breach
- Identify vulnerabilities exploited in the Quest Diagnostics third-party breach
- Describe the impact of the Quest Diagnostics third-party breach
- Identify third-party breach prevention techniques developed from an analysis of companies that successfully prevent such breaches
- Explain what ransomware is
- Distinguish different types of ransomware
- Describe ways in which users become ransomware targets
- Identify techniques for protecting against ransomware attacks
- List common examples of ransomware
- Identify techniques used to extract money from ransomware victims
- Summarize the timeline of the Atlanta ransomware breach
- Identify vulnerabilities exploited in the Atlanta ransomware breach
- Describe the cost and impact of the Atlanta ransomware breach
- List measures that could have prevented the Atlanta ransomware breach
- Create a data breach case study by applying what you learned in this course and others in the Cybersecurity Security Analyst Professional Certificate program

Duration:

16 Hrs

Topics:

Unit 1: Incident Management Response and Cyberattack Frameworks

Unit 2: ishing Scams

Unit 3: Point of Sale Breach

Unit 4: 3rd Party Breach

Unit 5: Ransomware

Unit 6: Apply Your Skill - Data Breaches

Audience:

Anyone who wants to gain a basic understanding of Cybersecurity or as the seventh course in a series of courses to acquire the skills to work in the Cybersecurity field as a Cybersecurity Analyst.