ACC: ACC 3

ACC Bucket: Cybersecurity - 3

Course: Cybersecurity Applications

OVERALL COURSE OBJECTIVES: The objective of this course series is to provide a robust foundation in cybersecurity, emphasizing practical skills in network and database security, the application of generative AI tools in cybersecurity challenges, and detailed methodologies in penetration testing and incident response. This comprehensive approach is designed to prepare students for advanced roles in the cybersecurity field, ensuring they can effectively address and mitigate potential security threats.

LEARNING OUTCOMES: On successful completion of the course the students shall be able to:

1. Understand and deploy various network defensive strategies, including network access controls and the use of network monitoring tools to safeguard organizational data.
2. Identify and mitigate risks associated with data protection, utilizing tools for data loss prevention and mobile endpoint protection.
3. Employ technologies for security vulnerability scanning and recognize application security threats to enhance organizational security.
4. Explore threat intelligence platforms and understand key concepts to effectively respond to cyber threats using Security Information and Event Management (SIEM) products.
5. Analyze past and recent cybersecurity breaches to understand detection methods and mitigation strategies, and apply incident response methodologies to hypothetical scenarios.
6. Demonstrate comprehensive knowledge and skills in cybersecurity through a final assessment, encompassing topics from prior courses to validate readiness for a cybersecurity analyst role.

COURSE CONTENT:

Module 1: Cyber Threat Intelligence [26 Hours]

This course gives you the background needed to gain Cybersecurity skills as part of the Cybersecurity Security Analyst Professional Certificate program.

You will understand network defensive tactics, define network access control and use network monitoring tools. You will understand data protection risks and explore mobile endpoint protection. Finally you will recognize various scanning technologies, application security vulnerabilities and threat intelligence platforms.

This course also gives you hands on access to cybersecurity tools important to a system analyst.

Sub-Topics
Application Security and Testing
Data Loss Prevention and Mobile Endpoint Protection
Scanning
SIEM Platforms
Threat Hunting
Threat Intelligence

Formative Assessments:

6 Graded Quizzes

Module 2: Cybersecurity Capstone: Breach Response Case Studies [16 Hours]

This course gives you the background needed to gain Cybersecurity skills as part of the IBM Cybersecurity Professional Certificate programs.

You will explore incident response methodologies and security models. You will learn to recognize and categorize key types of vulnerabilities and associated attacks against today's organizations. You will explore in depth 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.

This course requires you to select and research a cybersecurity breach in the news today and 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 your peers in the course.

Sub-Topics
3rd Party Breach
Apply Your Skill - Data Breaches
Incident Management Response and Cyberattack Frameworks
Phishing Scams
Point of Sale Breach
Ransomware

Formative Assessments:
1 Peer Review & 5 Graded Quizzes

Module 3: IBM Cybersecurity Analyst Assessment [4 Hours]

A growing number of exciting, well-paying jobs in today's security industry do not require a college degree. This is the final course required to assess your acquired knowledge and skills from from the previous two specializations, IT Fundamentals of Cybersecurity and Security Analyst Fundamentals, to become job-ready for a cybersecurity analyst role.

Sub-Topics
IBM Cybersecurity Analyst Professional Certificate Assessment Exam

Formative Assessments:
1 Graded Quiz

ASSESSMENT:
For summative assessments, Coursera will provide question banks for which exams can be conducted on the Coursera platform or the faculty will create their own assessments.

Note: If a Course or Specialization becomes unavailable prior to the end of the Term, Coursera may replace such Course or Specialization with a reasonable alternative Course or Specialization.