Course Code: 8H151GW

Course Title: Cybersecurity Threat Intelligence

Description:

This course covers threat intelligence sources. You will learn about data protection risks and explore mobile endpoint protection. Finally, you will recognize various scanning technologies, application security vulnerabilities, and threat intelligence platforms.This course is intended for anyone who wants to gain a basic understanding of cybersecurity. This is the sixth 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:

- Describe cybersecurity trends, drivers, and threats
- List the various costs of a cybersecurity breach
- Identify threat intelligence external sources
- Describe each step in the threat intelligence strategy map
- List key publications to review for insights into strategic threat intelligence plans
- Describe various threat intelligence platforms and resources
- Explain how to use various cyberthreat frameworks
- List best practices for intelligent detection of threats
- Define security intelligence
- Identify the three pillars of effective threat detection
- Explain the importance of improving security effectiveness
- Define data protection and security and explain its purpose
- Describe common data security challenges
- Discuss common pitfalls in data security
- Identify industry-specific data security challenges
- Identify the 12 critical capabilities for a data protection solution
- Describe Guardium as an example of a data protection solution
- Describe the primary vulnerabilities of mobile endpoints
- Discuss the available security options for mobile endpoints
- Explain day-to-day mobile endpoint management
- Manage mobile endpoint security using IBM MaaS360
- Explain how vulnerability scanners work
- Describe how vulnerability scanners are used
- Explain how to use the Common Vulnerability Scoring System (CVSS) to assign vulnerability scores
- Explain the use of the Security Technical Implementation Guide to enhance the overall security posture
- Explain how to use the Center for Internet Security (CIS) Benchmark hardening/vulnerability checklists
- Describe port scanning
- Describe the information gained from port scanning
- Describe the Nmap and Zenmap port scanning applications
- Explain what network protocol analyzers are
- Describe Wireshark
- Describe the packet capture file format
- Identify the characteristics of a security architecture
- Describe the different types of high-level security architectural models
- Describe how to decompose solutions to identify threats and specify security controls

- Explain how to use security patterns to accelerate security development for infrastructure and applications
- Describe the pros and cons of various software development lifecycles
- Describe application security techniques and tools
- Discuss application threats and attacks
- Summarize the OWASP top 10 application security risks
- Describe security standards and regulations
- Explain DevSecOps and its effect on application security
- Explain how to write secure application code
- Define cross-site scripting and describe its dangers
- Explain how to defend against cross-site scripting
- Define the key terms for security information event management (SIEM)
- Explore the role of SIEM in networks and moderate security operation centers
- Describe key considerations for deploying a SIEM system
- Discuss different SIEM solutions and their components
- Explain the features of QRadar for security analysis
- Analyze and report on cybersecurity events using IBM QRadar SIEM
- Investigate user behavior using the IBM QRadar User Behavior Analytics app (UBA)
- Describe use cases for UBA
- List the advantages of an integrated UBA solution in a security operation center (SOC)
- List the challenges that SOCs face
- Explain the benefits of artificial intelligence (AI) for cyberanalysts
- Describe the features and functions of an industry example using QRadar Advisor with Watson
- Investigate cybersecurity events using QRadar Advisor with Watson
- Discuss global cyber trends and challenges
- Explain why SOCs need to perform threat hunting
- Explain the primary goal of SOC cyber threat hunting
- Apply the cyber threat hunting concepts to an industry example
- Describe the structure of a cyber threat hunting team
- Examine cyber threat hunting with i2 use case examples
- Investigate cybersecurity threats using QRadar Analyst Workflow

Duration:

28.8 Hrs

Topics:

Unit 1: Threat Intelligence

Unit 2: Data Loss Prevention and Mobile Endpoint Protection

Unit 3: Scanning

Unit 4: Application Security and Testing

Unit 5: SIEM Platforms

Unit 6: Threat Hunting

Audience:

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