Cybersecurity Analyst

In this document, you'll find all the content covered in the Cybersecurity Analyst program. Our content provider is Coursera, and below are learning objectives for all 7 courses.

Introduction to Cybersecurity Tools & Cyber Attacks

Course Link

Learning Objectives

- Define cybersecurity and describe key terms and key security roles and functions within an IT organization.
- Describe the history of cybersecurity and what events brought it into the national spotlight in the United States.
- Describe why critical thinking is such an important skill for the security analyst to posses in the rapidly evolving cyberattack landscape.
- Describe why it is so hard to secure online resources and what organizations and resources are available to help.
- Describe the different types of cyber-attacks, security attack models, the organizations and actors involved, and their motives.
- Give examples of different types of cyber-attacks and examples of cyberwar attacks.
- Describe social engineering and how it is used in phishing and vishing attacks.
- Describe the various cybersecurity tools and resources available to the cybersecurity analyst such as X-Force Research and the IBM X-Force Command Center.
- Describe the CIA Triad and what is meant by confidentiality, integrity and availability in terms of cybersecurity.
- Describe the access management and incident response processes.
- Describe various cybersecurity frameworks and best practices, including NIST and the other the supporting organizations for each.
- Describe the purpose, function, and types of firewall.
- Explain the role of cryptography in cybersecurity, how it is used and how it can be attacked.
- Describe how penetration testing is used in cybersecurity and the role of digital forensics and Locard's exchange principle.

Cybersecurity Roles, Processes & Operating System Security

Course Link

Learning Objectives

- Discuss the importance of Business Process Management and the advantages of following the IT Service Management best practices documented in ITIL, the IT Infrastructure Library.
- Describe the key roles within Cybersecurity.
- Recall the definition of the CIA Triad.
- Discuss confidentiality, integrity and availability as it relates to cybersecurity.
- Summarize examples of where integrity is important today.
- Describe the Windows components User mode and Kernel mode and how they differ.
- Describe the NTFS and FATxx hierarchical file systems used by Windows.
- Explain the Windows directory structure and how Windows handles the separation of 32-bit and 64-bit applications.
- Recall the various useful keyboard shortcuts provided by Windows.
- Describe the concept of virtualization and what is a hypervisor and a virtual machine.
- Describe Public, Private and Hybrid cloud models. What considerations would lead you to choose one over another?
- Practice researching cybersecurity knowledge areas using the SANS institute's research documents and Internet Storm Center.

Cybersecurity Compliance Framework & System Administration

Course Link

Learning Objectives

- Describe the challenges organizations face which require compliance and regulation.
- Describe the key privacy and data protection requirements of GDPR.
- Describe the differences between SOC1, SOC2, and SOC3 controls and reporting.
- Define the three rules established as standards for the Health Insurance Portability and Accountability Act (HIPAA).
- Describe the Payment Card Industry Data Security Standard (PCI DSS).
- Describe the differences between basic, foundational and organizational Center for Internet Security (CIS) controls.
- Define a client as it relates to a computer system.
- Describe the basics of endpoint protection and response.
- Describe the benefits of Unified Endpoint Management (UEM).
- Understand why patching is important to avoid cybersecurity threats.
- Describe the principle of least privileges.
- Describe Windows security management considerations.
- Describe active directory features.
- Describe the basics of the Linux operating system including user management, commands and components.
- Define cryptography and encryption.
- Describe the digital states of data.
- Define common pitfalls of cryptography.
- Describe hashing and its purpose in encryption.
- Describe common pitfalls of using hashing.

Network Security & Database Vulnerabilities

Course Link

Learning Objectives

- Understand network basics around the TCP/IP and OSI Models.
- Describe the differences between IPS and IDS Systems.
- Discuss Layer 2 and Layer 3 network addressing.
- Describe how Ethernet networks work.
- Understand IP addressing, network address translation and packet sniffing.
- Describe application and transport protocols , UDP and TCP.
- Describe DNS and DHCP servers.
- Define Next Generation Firewalls.
- Describe key characteristics of different data types and models.
- Discuss different data structures.
- Discuss options for protecting your data.
- Describe several use case examples using a data protection solution.
- Describe the nature of various injection attacks and their prevalence on the threat landscape.
- Describe OS Command Injection attacks and the operating system flaws that allow them to occur.
- Describe SQL Injection and what makes an attack possible.
- Describe other types of injection attacks.

Penetration Testing, Incident Response and Forensics

Course Link

Learning Objectives

- Explain the different phases of a penetration test.
- Describe the various ways to gather enough information to gain access to a system.
- Recall the names of popular penetration testing tools and their general function.
- Describe the various phases of an incident response including preparation, detection, analysis, eradication, recovery, and post incident activities.
- Explain the importance of documentation in Incident Response.
- Be able to discuss the components of an incident response policy and how that can help members of an IR team.
- Describe the steps in the forensic process.
- Recognize the different sources of forensic data.
- Describe what chain of custody is and how it relates to forensics in the Court of Law.
- Explain how scripting plays a role in cyber security.
- Review the different scripting languages and understand which ones benefit Pentesting, Incident Response, or Digital Forensics.
- Practice creating a Python Application in the Python lab.

Cyber Threat Intelligence

Course Link

Learning Objectives

- Understand various threat intelligence platforms.
- Understand Data Protection risks.
- Discuss what types of attacks can be identified with endpoint protection solutions.
- Discuss how managing mobile differs from more traditional endpoints.
- Discuss various types of vulnerability assessment scanners.
- Discuss the Common Vulnerability Scoring System and how scores are assigned to vulnerabilities.
- Describe the use of a Security Technical Implementation Guide to enhance the overall security posture.
- Describe how to use the Center for Internet Security Benchmark.
- Use Wireshark network protocol analyzer to perform packet captures.
- Understand SIEM platforms.
- Use a SIEM application to review events and flows.
- Discuss global cyber trends and challenges.
- Describe cyber challenges faced by Security Operation Centers (SOCs) today.
- Apply Cyber Threat Hunting concepts to an industry solution.

Cybersecurity Capstone: Breach Response Case Studies

Course Link

Learning Objectives

- Recall the NIST's Incident Response Lifecycle.
- Describe the key characteristics of incident response.
- Explain the key points of the IBM X-force IRIS Cyberattack Framework.
- Explain what makes an incident a breach.
- Discuss the types of phishing attacks that an organization or individual might encounter.
- Describe the impacts of a phishing attack.
- Recall the Facebook and Google phishing attack's vulnerabilities and prevention recommendations.
- Describe a 3rd party attack and its impacts on an organization.
- Recall the vulnerabilities and impacts of a 3rd party attack based on the case study.
- Discuss 3rd party breach response methodologies.
- Practice recognizing and categorizing types of vulnerabilities and associated attacks.
- Apply your skill in conducting trend analysis.