Course Code: 8H121GW

Course Title: Cybersecurity Compliance Framework & System Administration

Description:

This course provides the basic commands for user and server administration as it relates to security. You will need this skill to be able to understand vulnerabilities within your organizations operating systems.You will learn the concepts of endpoint security and patch management. Both of these topics are important to keep systems current to avoid cybersecurity incidents against an organization.Finally, you will learn in-depth skills around cryptogray and encryption to understand how these concepts affect software within a company.This course is intended for anyone who wants to gain a basic understanding of cybersecurity. This is the third 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:

- Define events, attacks, and incidents in the context of cybersecurity
- Describe the cybersecurity challenges that organizations face that require compliance and regulation
- Contrast security, privacy, and compliance in the context of cybersecurity
- Describe the specific checklist of security controls
- Discuss the two main categories of cybersecurity compliance
- Explain each step of the typical process for verifying cybersecurity compliance
- Describe the Computer Fraud and Abuse Act
- Summarize what the National Institute of Standards and Technology (NIST) does
- Describe the requirements for privacy and data protection contained in the General Data Protection Regulation (GDPR)
- Summarize basic aspects of the International Organization for Standardization (ISO) 27001 standard
- Explain the purpose and benefits of System and Organizational Controls (SOC) reports
- Contrast SOC 1, SOC 2, and SOC 3 reports
- Differentiate between Type 1 and Type 2 SOC reports
- Discuss typical Trust Service Principles used to define a SOC 2 report’s scope
- Describe the criteria used in a SOC audit
- Summarize the importance of continuous monitoring between cybersecurity compliance audits
- Explain why organizations in and outside the U.S. comply with the Health Insurance Portability and Accountability Act (HIPAA)
- Define covered entity, business associate, and protected health information (I) in the context of HIPAA
- Describe HIPAA’s Privacy Rule and Security Rule
- Explain the Payment Card Industry Data Security Standard (PCI DSS), including its goals, scope, and audit process
- Describe some of the PCI DSS’s most unique requirements
- Describe the Center for Internet Security (CIS) Critical Security Controls®, including control types and implementation groups
- Define a client in the context of a computer network
- Discuss essential characteristics of client system administration in the context of cybersecurity
- Describe common types of endpoint attacks
- Define endpoint protection
- Explain key characteristics of endpoint protection
- Describe unified endpoint management (UEM)
- Explain what endpoint protection and response (EDR) does

- Summarize useful features of endpoint protection and response (EDR) applications
- Discuss important considerations for evaluating an endpoint security solution
- Manage endpoints using Xcitium OpenEDR
- Summarize key developments in device management that have made UEM a popular approach to endpoint protection
- Define patching
- Explain why patching is essential for protecting against cybersecurity threats
- Differentiate the four types of Windows updates
- Explain why patching applications is essential for cybersecurity
- Summarize the typical patching process that most organizations use
- Describe patch management best practices
- Compare and contrast Windows's two modes: user and kernel
- Define file system and hierarchical structure
- Contrast the NTFS and FAT file systems that Windows uses
- Describe the Windows directory structure
- Summarize how Windows handles the separation of 32-bit and 64-bit applications
- Explain how authentication and authorization work in Windows Access Control
- Define Windows privileged accounts
- Describe the principle of least privilege and its benefits for network administration
- Define local user accounts within Windows
- Describe default local accounts within Windows
- Discuss security considerations for managing local Windows systems
- Describe features of the Windows Security app
- Explain how Active Directory works
- Describe key features of Active Directory
- Differentiate the four types of Active Directory accounts
- Summarize guidelines for restricting and protecting sensitive domain accounts using Active Directory
- Describe the two types of Active Directory groups
- Explain scope as it relates to Active Directory groups
- Summarize what makes Windows Admin Center useful for server management
- Define Kerberos authentication and describe its benefits for Windows security and compliance
- Describe server logs in the context of network administration
- Discuss how to locate and view Windows Server logs
- Explain why an organization should have a security auditing policy
- Describe the nine types of Windows security events that administrators can audit
- Summarize why organizations use Linux
- Explain what the Linux kernel and shell do
- Describe Linux's file system and directory structure
- Explain what happens at each Linux run level
- Describe common shell choices within Linux
- Recall the functions of basic Linux shell commands
- Explain how to install and set up Samba so that Linux and Windows systems can communicate over a network
- Explain why organizations use cryptogray and encryption
- Describe the Open Web Application Security Project (OWASP) Top 10 Project and the SANS Institute Top 25 Software Errors
- Define encryption
- Contrast symmetric and public key cryptogray
- Define cryptograic terms, including hash functions and digital signatures
- Describe common cryptogray pitfalls and recommended solutions
- Describe best practices for encrypting data at rest
- Explain the recommended method for encrypting data in use
- Describe pitfalls and best practices for encrypting data in transit
- Explain the purpose of using hashing
- Discuss common pitfalls of using hashing

- Describe additional considerations when using hashing
- Explain how message authentication codes (MACs) work with hashing to ensure integrity
- List recommended uses for digital signatures
- Explain how to safeguard encryption keys
- Describe recommended ways to secure a key encryption key (KEK)
- Encrypt and decrypt files using ccrypt
- Describe the OpenPGP protocol
- Encrypt and decrypt emails using Mailvelope
- Summarize the impacts of quantum computing on cryptogray
- Set up user and group accounts in Kali Linux
- Encrypt a file using ccrypt
- Create an encrypted email using Mailvelope
- Evaluate your peers' completion of Linux and encryption tasks using the provided rubric

Duration:

12.8 Hrs

Topics:

Unit 1 -Compliance Frameworks and Industry Standards

Unit 2 - Client System Administration, Endpoint protection and Patching

Unit 3 - Server and User Administration

Unit 4 - Cryptogray and Compliance Pitfalls

Audience:

This course is intended for anyone who wants to gain a basic understanding of Security Frameworks, Compliance, endpoint management, encryption or cryptogray or as the third course in a series of courses to gain the skills needed as a Jr Cybersecurity analyst.