Web: www.secureninja.com
Phone: 703.535.8600
Email: info@secureninja.com

Rocheston Certified Cybersecurity Compliance Officer Training & Certification

Course Description & Overview

SecureNinja's Rocheston Certified Cybersecurity Operations (CCO) certification training delivers an in-depth, modern approach to building and managing advanced cybersecurity infrastructures and operations centers. This course is designed to prepare participants for critical roles in defending enterprise networks, securing cloud and IoT environments, and maintaining compliance with industry security frameworks and standards.

Covering an expansive range of cybersecurity disciplines, the CCO training program is ideal for professionals aiming to lead or contribute to security operations in both public and private sector organizations. Participants will develop technical mastery in areas such as threat intelligence, security analytics, cryptography, malware analysis, vulnerability assessment, and real-time incident response — all taught through an immersive, hands-on learning experience using modern tools and platforms.

Why Choose Rocheston CCO

- Advanced Security Operations Training: Equips learners with the skills to manage real-world security infrastructure and SOC environments.
- Cutting-Edge Curriculum: Includes AI security, zero trust architecture, secure coding, and behavioral analytics.
- Hands-On Labs: Extensive practical exercises using Linux, Python, malware toolkits, and cloud platforms.

Topics Covered

- Cybersecurity Fundamentals: Foundations of security, threat vectors, and attack surfaces.
- Security Operations Center (SOC): Design, operations, incident handling, and SIEM usage.
- Malware and Threat Analysis: Investigating threats, sandboxing, behavioral analysis, and reverse engineering.
- Cryptography: Key management, symmetric and asymmetric encryption, digital certificates, and PKI.
- Vulnerability Assessment and Penetration Testing: Scanning, enumeration, exploitation techniques, and remediation planning.
- Network and Cloud Security: Securing infrastructure, hybrid networks, cloud containers, and DevSecOps integration.
- IoT and AI Security: Protecting smart devices, edge computing nodes, and using AI in cyber defense.

Who is it for

- Security Analysts and Engineers: Professionals working in SOCs or enterprise defense teams.
- Penetration Testers and Red Teamers: Practitioners involved in offensive

Web: www.secureninja.com
Phone: 703.535.8600
Email: info@secureninja.com

operations and vulnerability assessments.
- Cloud and DevOps Professionals: Engineers responsible for integrating security into deployment pipelines and virtual infrastructures.
- IT Administrators: Technologists expanding into threat detection, incident response, and security automation.

Who Would Benefit

- Cybersecurity Managers: Team leaders looking to enhance operational visibility and defense capabilities.
- Network and System Architects: Designers of secure environments and zero trust infrastructure.
- Students and Career Changers: Individuals aiming to launch a career in advanced cybersecurity operations.

Prerequisites

A foundational understanding of networking, operating systems (Windows/Linux), and basic cybersecurity concepts is recommended. Experience with scripting or programming (e.g., Python) is helpful but not mandatory.

Course Outline

1. Cybersecurity Infrastructure and Operations

- Architecture, frameworks, and network defense systems.
- Zero trust and microsegmentation principles.

2. Threat Intelligence and Malware Analysis

- SOC processes, malware lifecycle, reverse engineering, and threat hunting.

3. Cryptography and Data Protection

- Public key infrastructure, TLS, VPNs, and secure file storage.

4. Cloud, IoT, and AI Security

- Securing AWS, Azure, Kubernetes, and containerized environments.
- Risks associated with IoT ecosystems and AI-enhanced threats.

5. Offensive Security and Vulnerability Management

- Penetration testing, red teaming, and risk mitigation planning.

Course Length

- 5 Days
- 40 Hours

Web: www.secureninja.com
Phone: 703.535.8600
Email: info@secureninja.com

Exam Details

- Exam: RCT-90 Certified Cybersecurity Compliance Officer
- Number of Questions: 50
- Question Types: Multiple-choice and practical scenarios
- Duration: 3 Hours
- Passing Score: 70%

The Rocheston Certified Cybersecurity Operations (CCO) certification equips professionals with the capabilities to lead and support sophisticated cybersecurity environments. This course ensures that graduates can not only respond to today’s threats but also architect systems that are resilient, adaptive, and aligned with global security standards.