Certified Cybersecurity Operations Analyst™ (CCOA)

Duration: 5 Days

Course Description:

ISACA's Certified Cybersecurity Operations Analyst™ (CCOA™) certification focuses on the technical skills to evaluate threats, identify vulnerabilities, and recommend countermeasures to prevent cyber incidents. As emerging technologies like automated systems using AI evolve, the role of the cyber analyst will only become more critical in protecting digital ecosystems. Analysts specialize in understanding the what, where and how behind cybersecurity incidents. By identifying patterns, anomalies and indicators of compromise, you become the eyes and ears of your organization's defense.

CCOA is administered through a hybrid exam that assesses a candidate's knowledge and skills using a blend of traditional multiple-choice and performance-based questions.

Target Audience:

The Certified Cybersecurity Operations Analyst™ (CCOA) course equips professionals with essential skills in cybersecurity principles, incident response, and vulnerability management, targeting those keen on safeguarding digital assets.

- IT Professionals
- Network Administrators
- System Administrators
- Cybersecurity Analysts
- Incident Response Teams
- Risk Management Specialists
- Compliance Officers
- Security Operations Center (SOC) Analysts
- Security Engineers
- IT Security Managers
- Threat Intelligence Analysts
- Application Security Specialists
- Security Consultants
- Students pursuing a career in cybersecurity

Prerequisites:

To ensure students can fully engage with the content and obtain the most from their training experience, we recommend the following minimum knowledge and skills prerequisites for those looking to undertake the CCOA course:

- Basic Understanding of Networking Concepts: Familiarity with fundamental networking concepts such as IP addressing, protocols, and network topologies is beneficial.
- General Knowledge of Operating Systems: A working knowledge of various operating systems (e.g., Windows, Linux) and their typical functionalities will aid in understanding systems and endpoints.
- Awareness of Cybersecurity Principles: A fundamental grasp of basic cybersecurity concepts and terminologies will help students navigate risks and security frameworks effectively.
- Problem-Solving Skills: The ability to think critically and approach problems methodically will enhance learning and application of incident detection and response strategies.

These prerequisites are intended to give aspiring students a solid foundation for the course material, helping to ensure their success in understanding and applying the concepts covered in the CCOA training.

Course Objectives:

- Understand foundational networking concepts and their role in cybersecurity.
- Analyze systems and endpoints to identify vulnerabilities.
- Examine key applications and their security implications.
- Apply cybersecurity principles to assess and mitigate risks.
- Identify various adversarial tactics, techniques, and procedures.
- Recognize different types of cyber attacks and their impact.
- Develop skills in detecting security incidents effectively.
- Formulate and implement incident response strategies.
- Implement security controls to safeguard organizational assets.
- Conduct vulnerability management to enhance security posture.

Course Outlines:

DOMAIN 1 – TECHNOLOGY ESSENTIALS

Identify the key components of computer and cloud networking, understand how databases, virtualization, and containerization are leveraged, and become familiar with command-line interfaces, programming, scripting, and more.

A–NETWORKING

- Cloud Networking
- Computer Networking
- Devices, Ports, and Protocols
- Network Access
- Network Tools
- Network Topology
- Segmentation (Logical, Physical)

B–SYSTEMS/ENDPOINT
- Databases
- Command Line
- Containerization/Virtualization
- Middleware
- Operating Systems

C –APPLICATIONS
- Application Programming Interface (API)
- Automated Deployment
- Cloud Applications
- Scripting/Coding

DOMAIN 2 – CYBERSECURITY PRINCIPLES AND RISK

Understand cybersecurity governance and alignment with business drivers, define cybersecurity strategy based on enterprise objectives, establish effective cross-organizational communication for cybersecurity and more.

A–CYBERSECURITY PRINCIPLES
- Compliance
- Cybersecurity Objectives
- Governance
- Risk Management
- Roles and Responsibilities
- Cybersecurity Models

B–CYBERSECURITY RISK
- Application Risk
- Cloud Technology Risk
- Data Risk
- Network Risk
- Supply Chain Risk
- System/Endpoint Risk
- Web Application Risk

DOMAIN 3 – ADVERSARIAL TACTICS, TECHNIQUES, AND PROCEDURES

Understand common adversarial tactics, techniques, and procedures (TTPs), develop critical and creative thinking skills for threat detection and response, differentiate between dashboard events, attacker mindset insights and more.

A–THREAT LANDSCAPE
- Attack Vectors
- Threat Actors/Agents
- Threat Intelligence Sources

B–MEANS AND METHODS
- Attack Types
- Cyber Attack Stages
- Exploit Techniques
- Penetration Testing

DOMAIN 4 – INCIDENT DETECTION AND RESPONSE

Understand the importance of cybersecurity-incident preparedness, recognize the significance of incident detection and response in mitigating their impact, appreciate the role of proactive planning, practice, process refinement and more.

A–INCIDENT DETECTION
- Data Analytics
- Detection Use Cases
- Indicators of Compromise and/or Attack
- Logs and Alerts
- Monitoring Tools and Technologies

B–INCIDENT RESPONSE
- Incident Containment
- Incident Handling
- Forensic Analysis
- Malware Analysis
- Network Traffic Analysis
- Packet Analysis
- Threat Analysis

DOMAIN 5 – SECURING ASSETS

Understand the importance of designing countermeasures to protect digital assets, recognize the iterative nature of securing systems and their ecosystems, appreciate the holistic approach to securing assets, consider technical aspects and organizational products, services and critical business processes, and more.

A–CONTROLS
- Contingency Planning
- Controls and Techniques
- Identity and Access Management
- Industry Best Practices, Guidance, Frameworks, and Standards

B–VULNERABILITY MANAGEMENT
- Vulnerability Assessment
- Vulnerability Identification
- Vulnerability Remediation
- Vulnerability Tracking