Course duration

- 5 days

Course Benefits

- Assess information security risk in computing and network environments.
- Analyze reconnaissance threats to computing and network environments.
- Analyze attacks on computing and network environments.
- Analyze post-attack techniques on computing and network environments.
- Implement a vulnerability management program.
- Collect cybersecurity intelligence.
- Analyze data collected from security and event logs.
- Perform active analysis on assets and networks.
- Respond to cybersecurity incidents.
- Investigate cybersecurity incidents.
- Address security issues with the organization's technology architecture.

Course Outline

1. Assessing Information Security Risk
    1. Identify the Importance of Risk Management
    2. Assess Risk
    3. Mitigate Risk
    4. Integrate Documentation into Risk Management
2. Analyzing Reconnaissance Threats to Computing and Network Environments
    1. Assess the Impact of Reconnaissance Incidents
    2. Assess the Impact of Social Engineering
3. Analyzing Attacks on Computing and Network Environments
    1. Assess the Impact of System Hacking Attacks
    2. Assess the Impact of Web-Based Attacks
    3. Assess the Impact of Malware
    4. Assess the Impact of Hijacking and Impersonation Attacks
    5. Assess the Impact of DoS Incidents
    6. Assess the Impact of Threats to Mobile Security
    7. Assess the Impact of Threats to Cloud Security
4. Analyzing Post-Attack Techniques
    1. Assess Command and Control Techniques
    2. Assess Persistence Techniques
    3. Assess Lateral Movement and Pivoting Techniques
    4. Assess Data Exfiltration Techniques
    5. Assess Anti-Forensics Techniques

5. Managing Vulnerabilities in the Organization
    1. Implement a Vulnerability Management Plan
    2. Assess Common Vulnerabilities
    3. Conduct Vulnerability Scans
    4. Conduct Penetration Tests on Network Assets
6. Collecting Cybersecurity Intelligence
    1. Deploy a Security Intelligence Collection and Analysis Platform
    2. Collect Data from Network-Based Intelligence Sources
    3. Collect Data from Host-Based Intelligence Sources
7. Analyzing Log Data
    1. Use Common Tools to Analyze Logs
    2. Use SIEM Tools for Analysis
8. Performing Active Asset and Network Analysis
    1. Analyze Incidents with Windows-Based Tools
    2. Analyze Incidents with Linux-Based Tools
    3. Analyze Malware
    4. Analyze Indicators of Compromise
9. Responding to Cybersecurity Incidents
    1. Deploy an Incident Handling and Response Architecture
    2. Mitigate Incidents
    3. Prepare for Forensic Investigation as a CSIRT
10. Investigating Cybersecurity Incidents
    1. Apply a Forensic Investigation Plan
    2. Securely Collect and Analyze Electronic Evidence
    3. Follow Up on the Results of an Investigation
11. Addressing Security Architecture Issues
    1. Remediate Identity and Access Management Issues
    2. Implement Security During the SDLC

Class Materials

Each student will receive a comprehensive set of materials, including course notes and all the class examples.

Class Prerequisites

Experience in the following *is required* for this CompTIA class:

- At least two years of experience in computer network security technology or a related field.
- The ability to recognize information security vulnerabilities and threats in the context of

risk management.
- Foundation-level operational skills with some of the common operating systems for computing environments.
- Foundational knowledge of the concepts and operational framework of common assurance safeguards in computing environments. Safeguards include, but are not limited to, basic authentication and authorization, resource permissions, and anti-malware mechanisms.
- Foundation-level understanding of some of the common concepts for network environments, such as routing and switching.
- Foundational knowledge of major TCP/IP networking protocols, including, but not limited to, TCP, IP, UDP, DNS, HTTP, ARP, ICMP, and DHCP.
- Foundational knowledge of the concepts and operational framework of common assurance safeguards in network environments. Safeguards include, but are not limited to, firewalls, intrusion prevention systems, and VPNs.