C)CSA: Certified Cybersecurity Analyst

Course ID #: 7000-784-ZZ-Z

Hours: 35

Course Content

Course Description:

In this course, you will cover how to prepare an organization to create a complete end-to-end solution for monitoring, preventing, detecting, and mitigating threats as they arise in real-time. Do not fool yourself, this course is far more advanced than you may expect. It is fast paced and thorough, so you can enjoy a well-rounded experience. Be ready to dig deep into the details of security analysis for today's needs. You will be able to set up and deploy state of the art open source and commercial analysis tools, intrusion detection tools, syslog servers, and SIEMs. You will also be able to integrate them for an entire organization.

*This course maps to the mile2 Certified Cyber Security Analyst Exam as well as the Comp TIA CySA+CS0-001 certification exam.

Course Objectives:

Upon successful completion of this course, students will:

- Be able to competently take the C)CSA Exam
- Be ready to prepare an organization for proactive defense against today's hackers

Prerequisites:

- Certified Security Principles
- Certified Digital Forensics Examiner
- Certified Incident Handling Engineer
- Certified Professional Ethical Hacker
- Certified Penetration Testing Engineer
- or Equivalent Knowledge

Target Audience:

- Security Professionals
- Incident Handling Professionals
- Anyone in a Security Operations Center
- Forensics Experts
- Cybersecurity Analysts

C)CSA: Certified Cybersecurity Analyst

Course ID #: 7000-784-ZZ-Z

Hours: 35

Topics:

Lesson 1: Blue Team Principles

- Network Architecture and how it lays the groundwork
  - Defensive Network
- Security Data Locations and how they tie together
- Security Operations Center
  - The People, Processes, and Technology
  - Triage and Analysis
  - Digital Forensics
  - Incident Handling
  - Vulnerability Management
- Automation, Improvement, and Tuning

Labs:

Analyze Initial Compromise Vector
Network Forensics
System Forensics

Lesson 2: Digital Forensics

- Investigative Theory and Processes
  - Digital Acquisition
  - Evidence Protocols
  - Evidence Presentation
- Computer Forensics Laboratory
  - Protocols
  - Processing Techniques
  - Specialized Artifacts
- Advanced Forensics for Today's Exploitations

Labs:

Analysis of Captured Network Activity
Analysis of Captured Zip File

Lesson 3: Malware Analysis

- Creating the Safe Environment
- Static Analysis
- Dynamic Analysis
- Behavior Based Analysis
- What is different about Ransomware?
- Manual Code Reversing

Labs:

Analysis of an MSFVenom Executable
Analysis of Locky Ransomware
Creating YARA Rules based on Analysis Results
Final Assessment

Lesson 4: Traffic Analysis

- Manual Analysis Principles
- Automated Analysis Principles
  - Signatures compared to Behaviors
- Application Protocols Analysis Principles
- Networking Forensics

Labs:

Traffic Analysis of a Website Defacement Attack
Traffic Analysis Based on IDS Alerts
Traffic Analysis of a ZLoader Delivery Attempt
Bonus: Find the Backdoor!!!

Lesson 5: Assessing the Current State of Defense within the Organization

- Network Architecture and Monitoring
- Endpoint Architecture and Monitoring
- Automation, Improvement, and continuous monitoring

Labs:

Configuring a Firewall
Configuring SIEM
Configuring IPDS
Upgrading Detection/Protection Capabilities

C)CSA: Certified Cybersecurity Analyst

Course ID #: 7000-784-ZZ-Z

Hours: 35

Lesson 6: Leveraging SIEM for Advanced Analytics

- Network Architecture and Monitoring
- Endpoint Architecture and Monitoring
- Automation, Improvement, and continuous monitoring

Labs:

Architectural Benefits
Profiling and Baselining
Advanced Analytics

Lesson 7: Defeating the Red Team with Purple Team tactics

- Penetration Testing with full knowledge
  - Reconnaissance
  - Scanning
  - Enumeration
  - Exploitation
  - Lateral Movement

Labs:

Configuring Defensive Systems
Purple Team Testing
Mitigation
Bypass Anti-Virus and LSASS Patch through edited Mimikatz

Accreditations:

Register for this class by visiting us at:
www.tcworkshop.com or calling us at 800-639-3535