C)CSA: Certified Cybersecurity

Description:

This course helps you 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.

Annual Salary Potential $70,351 AVG/year

* CySA+ and CS0-001 are registered trademarks of CompTia

Key Course Information

Live Class Duration: 5 Days

CEUs: 40

Language: English

Class Formats Available:

Instructor Led

Self-Study

Live Virtual Training

Suggested Prerequisites:
(Any of the following Mile2 Courses)

- Certified Security Principles
- Certified Digital Forensics Examiner
- Certified Incident Handling Engineer
- Certified Professional Ethical Hacker

Modules/Lessons

Module 01: Blue Team Principles

Module 02: Digital Forensics

Module 03: Malware Analysis

Module 04: Traffic Analysis

Module 05: Assessing the Current State of Defense within an Organization

Module 06: Leveraging SIEM for Advances Analytics

Module 07: Defeating the Red Team with Purple Team Tactics

Labs

Lab 01: Establishing Ips and Logging into the VMs

Lab 02: Blue Team Principles

Lab 03: Digital Forensics

Lab 04: Malware Analysis

Lab 05: Traffic Analysis

Lab 06: Assessing Current State of Defense within an Organization

Lab 07: Leveraging SIEM for Advanced Analytics

Lab 08: Defeating the Red Team with Purple Team Tactics

*All labs are performed in our Cyber Range® on our Ghost Pentesting Platform®

www.mile2.ca 403 Bank St Ottawa, ON K2P 1Y6 613-416-8898

C)CSA: Certified Cybersecurity

Who Should Attend

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

Upon Completion

Upon completion, the Certified Cybersecurity Analyst candidate will be able to competently take the C)CSA Exam. They will also be ready to prepare an organization for proactive defense against today's hackers.

Accreditations

Exam Information

The Certified Cybersecurity Analyst exam is taken online through Mile2's Learning Management System and is accessible on you Mile2.com account. The exam will take approximately 2 hours and consist of 100 multiple choice questions.

A minimum grade of 70% is required for certification.

Re-Certification Requirements

All Mile2 certifications will be awarded a 3-year expiration date.

There are two requirements to maintain Mile2 certification:

1) Pass the most current version of the exam for your respective existing certification
2) Earn and submit 20 CEUs per year in your Mile2 account.

Course FAQ's

Question: Do I have to purchase a course to buy a certification exam?

Answer: No

Question: Do all Mile2 courses map to a role-based career path?

Answer: Yes. You can find the career path and other courses associated with it at www.mile2.com.

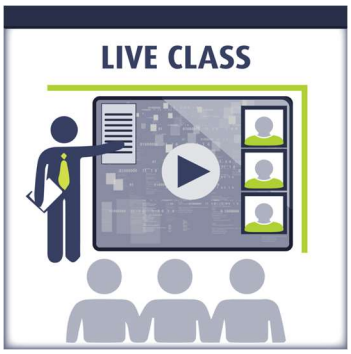
Question: Are all courses available as self-study courses?

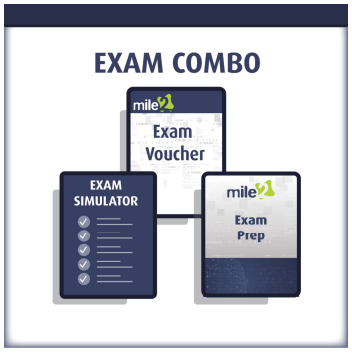
Answer: Yes. There is however 1 exception. The Red Team vs Blue Team course is only available as a live class.

Question: Are Mile2 courses transferable/shareable?

Answer: No. The course materials, videos, and exams are not meant to be shared or transferred.

Course and Certification Learning Options





www.mile2.ca 403 Bank St Ottawa, ON K2P 1Y6 613-416-8898

Detailed Outline:

Course Introduction

- **Chapter 1: Blue Team Principles**
  1. Network Architecture and how it lays the groundwork
     a. Defensive Network
  2. Security Data Locations and how they tie together
  3. Security Operations Center
     a. The People, Processes, and Technology
     b. Triage and Analysis
     c. Digital Forensics
     d. Incident Handling
     e. Vulnerability Management
  4. Automation, Improvement, and Tuning

- **Chapter 1 Labs: Blue Team Principles**
  1. Analyze Initial Compromise Vector
  2. Network Forensics
  3. System Forensics

- **Chapter 2: Digital Forensics**
  1. Investigative Theory and Processes
     a. Digital Acquisition
     b. Evidence Protocols
     c. Evidence Presentation
  2. Computer Forensics Laboratory
     a. Protocols
     b. Processing Techniques
     c. Specialized Artifacts
  3. Advanced Forensics for Today's Exploitations

- **Chapter 2 Labs: Digital Forensics**
  1. Analysis of Captured Network Activity
  2. Analysis of Captured Zip File

- **Chapter 3: Malware Analysis**
  1. Creating the Safe Environment
  2. Static Analysis
  3. Dynamic Analysis
  4. Behavior Based Analysis
  5. What is different about Ransomware?
  6. Manual Code Reversing

www.mile2.ca 403 Bank St Ottawa, ON K2P 1Y6 613-416-8898

- **Chapter 3 Labs: Malware Analysis**
  1. Analysis of an MSFVenom Executable
  2. Analysis of Locky Ransomware
  3. Creating YARA Rules based on Analysis Results
  4. Final Assessment

- **Chapter 4: Traffic Analysis**
  1. Manual Analysis Principles
  2. Automated Analysis Principles
     a. Signatures compared to Behaviors
  3. Application Protocols Analysis Principles
  4. Networking Forensics

- **Chapter 4 Labs: Traffic Analysis**
  1. Traffic Analysis of a Website Defacement Attack
  2. Traffic Analysis Based on IDS Alerts
  3. Traffic Analysis of a ZLoader Delivery Attempt
  4. Bonus: Find the Backdoor!!!

- **Chapter 5: Assessing the Current State of Defense with the Organization**
  1. Network Architecture and Monitoring
  2. Endpoint Architecture and Monitoring
  3. Automation, Improvement, and continuous monitoring

- **Chapter 5 Labs: Assessing the Current State of Defense within the Organization**
  1. Configuring a Firewall
  2. Configuring SIEM
  3. Configuring IPDS
  4. Upgrading Detection/Protection Capabilities

- **Chapter 6: Leveraging SIEM for Advanced Analytics**
  1. Architectural Benefits
  2. Profiling and Baselining
  3. Advanced Analytics

- **Chapter 6 Labs: Leveraging SIEM for Advanced Analytics**
  1. Deploying Agent
  2. Implementing User Behavior Analytics through Machine Learning
  3. Simulate an Attack and Analyze Alerts

www.mile2.ca 403 Bank St Ottawa, ON K2P 1Y6 613-416-8898

- **Chapter 7: Defeating the Red Team with Purple Team tactics**
  1. Penetration Testing with full knowledge
     a. Reconnaissance
     b. Scanning
     c. Enumeration
     d. Exploitation
     e. Lateral Movement

- **Chapter 7 Labs: Defeating the Red Team with Purple Team Tactics**
  2. Configuring Defensive Systems
  3. Purple Team Testing
  4. Mitigation
  5. Bypass Anti-Virus and LSASS Patch through edited Mimikatz

www.mile2.ca 403 Bank St Ottawa, ON K2P 1Y6 613-416-8898