Certified Threat Intelligence Analyst

Description:

In today's evolving cyber landscape, reactive security isn't enough—organizations need a proactive, intelligence-driven defense to stay ahead of adversaries. The Certified Threat Intelligence Analyst (CTIA) course equips SOC teams, security engineers, and cyber threat intelligence (CTI) professionals with the practical skills and technical expertise to implement real-world threat intelligence strategies effectively.

This comprehensive, hands-on course covers threat intelligence gathering, operationalization, and automation, ensuring students build and deploy intelligence-driven detection rules across SIEMs, Snort, Elastic Security, MISP, and more. With real-world labs, practical case studies, and deep technical insights, participants will master Sigma rule creation, OpenIOC structuring, STIX/TAXII automation, and custom scripting—empowering them to detect, analyze, and mitigate cyber threats before they strike. Whether you're building a new threat intelligence program or enhancing SOC operations, CTIA delivers the skills needed to turn intelligence into action.

Annual Salary Potential $96,000 AVG/year

Key Course Information

Live Class Duration: 5 Days

CEUs: 40

Language: English

Class Formats Available:

Instructor Led

Self-Study

Live Virtual Training

Suggested Prerequisites:

- 12 months vulnerability testing

- Mile2's C)SP, C)IHE, and C)PTE

Or equivalent

Modules/Lessons

Module 01: Threat Intelligence Basics

Module 02: Security Analysis Basics

Module 03: Cyber Threats

Module 04: Threat Actors

Module 05: Case Studies

Module 06: Threat Identification

Module 07: Proactive Approach

Hands-On Labs

Lab 01: Setting up SIEM Environment

Lab 02: Practical Threat Analysis

Lab 03: Hunting for Active Threats through Collected Logs

Lab 04: Defensive Threat Intelligence Development

Lab 05: Threat Intelligence Data Integration with SIEM

Lab 06: Leveraging MISP for Threat Intelligence

Lab 07: OSINT Methodology to Identify Threats

Lab 08: Exploitation, Analyzing, and Research

Lab 09: Integrating Elastic & MISP

www.mile2.com 10213 Wilsky Blvd, Tampa, FL 33625 813-920-6779

Certified Threat Intelligence Analyst

Upon Completion

Upon completion, Certified Threat Intelligence Analyst course students will have knowledge to perform thorough threat analysis on any information system. Be able to accurately report on their findings, and be ready to sit for the C)TIA exam.

Who Should Attend

* Penetration Testers
* Microsoft Administrator
* Security Administrators
* Active Directory Administrators
* Anyone looking to learn more about security

Accreditations

Exam Information

The Certified Threat intelligence 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.

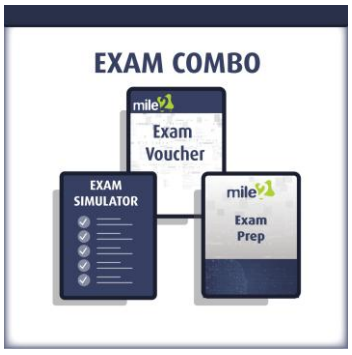
Question: Are all courses available as self-study courses?

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.com 10213 Wilsky Blvd, Tampa, FL 33625 813-920-6779

Detailed Outline:

Course Introduction

Module 1: Threat Intelligence Basics

a. Threat Intelligence Basics
b. Threat Intelligence Use Cases
c. Threat Intelligence Development
d. Types of Threat Intelligence
e. Tools of the Trade

Module 2: Security Analysis Basics

a. What is Security Analysis
b. How Security Analysis support Threat Intelligence
c. Static Analysis
d. Dynamic Analysis
e. Rule Based Detection

Module 3: Cyber Threats

a. Cyber Threat Overview
b. Cyber Threats Classification
c. Prevention Against Cyber Threats
d. Examples of Cyber Threats in History

Module 4: Threat Actors

a. Threat Actors Overview
b. Threat Actors Classification
c. Examples of threat Actors in History

Module 5: Cyber Threats & Malicious Actors Case Studies

a. Stuxnet
b. EternalBlue
c. WannaCry
d. Wizard Spider Group
e. Operation Aurora
f. Zerologon
g. MOVEit

www.mile2.com 10213 Wilsky Blvd, Tampa, FL 33625 813-920-6779

Module 6: Threats Identification

a. Threat Hunting
b. Threats Analysis Frameworks
c. Leveraging Tools for Threat Discovery

Module 7: Implementing a Proactive Threat Intelligence Approach

a. Foundations of Proactive Threat Intelligence
b. Operationalizing Threat Intelligence in an Organization
c. Threat Intelligence Sharing & Exchange Standards
d. Rule Creation for Threat Hunting & Automation

Detailed Lab Outline:

Lab 1 – Setting up SIEM Environment

Section 1 – Setup Elastic Search

Lab 2 – Practical Threat Analysis

Section 1 – Static Analysis on WannaCry Threat
Section 2 – Dynamic Analysis on WannaCry Threat
Section 3 – Perform an Analysis on your own

Lab 3 – Hunting for Active Threats through Collected Logs

Section 1 – Hunting for Backdoors
Section 2 – Hunting for Intrusions
Section 3 – Threat Actor Profiling using MITRE ATT&CK.

Lab 4 – Defensive Threat Intelligence Development

Section 1 – YARA Rules Usage, Development, and Improvement
Section 2 – Snort Rules Usage, Development, and Improvement

Lab 5 – Threat Intelligence Data Integration with SIEM

Section 1 – Implement Real-Time Threat Intelligence within SIEM

www.mile2.com 10213 Wilsky Blvd, Tampa, FL 33625 813-920-6779

Lab 6 – Leveraging MISP for Threat Intelligence

Section 1 – Analyzing an Attack by adding an Event
Section 2 – Add an event based on actual attack
Section 3 – Decay and Warning Lists
Section 4 – MISP feeds

Lab 7 – OSINT Methodology to Identify Threats

Section 1 – Discovering Threats through Google Dorks OSINT
Section 2 – Discovering Threats through Social Media OSINT
Section 3 – Discovering Threats through Intelligence Sharing
Section 4 – Discovering Threats through Dark Web OSINT
Section 5 – Discovering Threats through Vulnerabilities Databases OSINT

Lab 8 – Exploitation, Analyzing, and Research

Section 1 – Exploitation and Analysis of SIEM Logs
Section 2 – Analyzing Exported SIEM logs
Section 3 – Researching OTX for threats affecting a specific industry

Lab 9 – Integrating Elastic and MISP

Section 1 – Manual Ingestion of MISP Events into Elastic
Section 2 – Visualize Threat Feeds in Elasticsearch
Section 3 – Ingesting MISP Events to Elastic Defender Rules
Section 4 – Automate IOC Ingestion into Elastic's Detection Rules