Description:

Mile2’s CTIA course will help security professionals learn how to make good use of the many sources of threat intelligence. It will aid an individual to understand what threat sources are helpful, which specific threats are targeted and which ones may need minor adjustments to monitor within your organization.   
 Mile2’s CTIA course focuses heavily on hands-on labs, concentrating on discerning and interpreting threats and responding to them.  The CTIA course focuses

Arrow

Description automatically generated

overall on current significant threats, threat actors, and identification procedures so that cyber-security professionals can implement the best policies and procures for their organizational security posture.   
 Once complete, the student will be competent toward improving a company’s existing security infrastructure. Policies and methodologies learned in the CTIA will allow the student to use threat intelligence concepts to decrease overall company risk. [NICE FRAMEWORK WORK-ROLE ID: AN-TWA-001](https://niccs.cisa.gov/workforce-development/cyber-security-workforce-framework/workroles?name=Threat%2FWarning+Analyst&id=All)

Annual Salary Potential $85,000 AVG/year

Icon

Description automatically generated

Key Course Information

**Live Class Duration:** 4 Days

**CEUs:** 40

**Language:** English

**Class Formats Available:**

Instructor Led

Self-Study

Live Virtual Training

**Suggested Prerequisites:**

- 12 months vulnerability testing

- Mile2’s C)VA and C)PEH

Hands-On Labs

**Module 01**: Threat Intelligence Basics

**Module 02**: Cyber Threats

**Module 03**: Threat Actors

**Module 04**: Case Studies

**Module 05**: Threat Identification

**Module 06**: Proactive Approach

Key Course Information

Modules/Lessons

**Lab 01**: Practical Threat Analysis

**Lab 02**: Hunting Active Threats

**Lab 03**: Defensive Threat Development

**Lab 04**: Integration with SIEM

**Lab 05**: OSINT Methodology

Upon Completion

Course FAQ’s

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.

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.

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.

\* Penetration Testers

\* Microsoft Administrator

\* Security Administrators

\* Active Directory

Administrators

\* Anyone looking to learn

more about security

**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](http://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.

Who Should Attend

Re-Certification Requirements

Accreditations



Logo

Description automatically generated





Course and Certification Learning Options

Graphical user interface, application

Description automatically generated





Detailed Outline:

**Course Introduction**

Introduction

**Module 1: Threat Intelligence Basics**

1. Threat Intelligence Basics
2. Threat Intelligence Use Cases
3. Threat Intelligence Development

**Module 2: Cyber Threats**

1. Cyber Threat Overview
2. Cyber Threats Classification
3. Prevention Against Cyber Threats
4. Examples of Cyber Threats in History

**Module 3: Threat Actors**

1. Threat Actors Overview
2. Threat Actors Classification
3. Examples of threat Actors in History

**Module 4: Cyber Threats & Malicious Actors Case Studies**

1. Student
2. EternalBlue
3. WannaCry
4. Wizard Spider Group
5. Operation Aurora
6. Zerologon

**Module 5: Threats Identification**

1. Threat Hunting
   1. Introduction to IoC (Indicators of Compromise)
   2. Backdoors Hunting (Manual and Automated)
   3. Malware Hunting (Manual and Automated)
   4. APT Hunting (Manual and Automated)
2. Threats Analysis Framework
   1. Kill Chain
   2. MITRE ATT&CK
   3. Diamond Model
   4. Determining Tactics, Techniques, and Procedures (TTP) of a Threat

**Module 6: Implementing a Proactive Threat Intelligence Approach**

1. Scope, Goals, and Characteristics of a Proactive Threat Intelligence Approach
2. Implementation and Practicability
   1. Threat Intelligence Feeds
   2. Threat Intelligence Communities
   3. Threat Intelligence Tools

Detailed Lab Outline:

**Lab 1 – Practical Analysis of Well-Known Threats**

1. Stuxnet Analysis
2. EternalBlue Analysis
3. WannaCry Analysis
4. Zerologon Analysis

**Lab 2 – Hunting for Active Threat Through Collected Logs**

1. Hunting for Backdoors
2. Hunting for Malware
3. Automated Threat Hunting
4. **Lab 3 – Defensive Trheat Intelligence Development**
5. YARA Rules Usage, Development, and Improvement
6. Stort Rules Usage, Development and Improvement
7. Threat Simulation
8. **Lab 4 – Threat Intelligence Data Integration with SIEM**
9. Collection
10. Ingestion
11. Threat Simulation
12. **OSINT Methodology to Identify Latest Threats**
13. Discovering Cyber Threats Through Social Media OSINT
14. Discovering Cyber Threats Through Dark Web OSINT