Certified Threat Intelligence Analyst

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 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

Annual Salary Potential $85,000 AVG/year

Key Course Information

Live Class Duration: 4 days

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

Modules/Lessons

Module 1: Incident Handling Explained

Module 2: Incident Response Policy, Plan and Procedures.

Module 3: Incident Response Team Structure

Module 4: Incident Response Team Services

Module 5: Incident Response Recommendations

Module 6: Preparation

Module 7: Detection and Analysis

Module 8: Containment, Eradication and Recovery

Module 9: GRR Rapid Response

Module 10: Request Tracker

Module 11: Post Incident Activity

Module 12: Recommendations

Module 13: References

Module 14: Information Sharing

Hands-On Labs

Lab 1: Identifying Incident Triggers

Lab 2: Drafting Incident Response Proceedures

Lab 3: Planning for Dependencies

Lab 4: Testing your plan

Lab 5: Drafting Security Policies

Lab 6: Practicing Attack Vectors

Lab 7: Deploy GRR Client

Lab 8: Create Request Tracker Workflow

Lab 9: Lessons Learned

Lab 10: Create a Checklist

Lab 11: Draft Response Improvement Recommendations

Lab 12: Sharing Agreements

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

Detailed Outline:

Course Introduction

Introduction

Module 1: Threat Intelligence Basics

a. Threat Intelligence Basics
b. Threat Intelligence Use Cases
c. Threat Intelligence Development

Module 2: Cyber Threats

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

Module 3: Threat Actors

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

Module 4: Cyber Threats & Malicious Actors Case Studies

a. Student
b. EternalBlue
c. WannaCry
d. Wizard Spider Group
e. Operation Aurora
f. Zerologon

Module 5: Threats Identification

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

Module 6: Implementing a Proactive Threat Intelligence Approach

a. Scope, Goals, and Characteristics of a Proactive Threat Intelligence Approach
b. Implementation and Practicability
    a. Threat Intelligence Feeds
    b. Threat Intelligence Communities
    c. 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

A. Lab 3 – Defensive Trheat Intelligence Development

1. YARA Rules Usage, Development, and Improvement
2. Stort Rules Usage, Development and Improvement
3. Threat Simulation

B. Lab 4 – Threat Intelligence Data Integration with SIEM

1. Collection
2. Ingestion
3. Threat Simulation

C. OSINT Methodology to Identify Latest Threats

1. Discovering Cyber Threats Through Social Media OSINT
2. Discovering Cyber Threats Through Dark Web OSINT