C)TIA: Certified Threat Intelligence Analyst

Course ID #: 7000-780-ZZ-Z
Hours: 35

Course Content

Course Description:

In this course you will cover 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. This 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.

Course Objectives:

Upon successful completion of this course, students will:

- Have knowledge to perform thorough threat analysis on any information system
- Be able to accurately report on their findings
- Be ready to sit for the C)TIA exam

Prerequisites:

- 12 months vulnerability testing
- C)VA and C)PEH

Target Audience:

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

Topics:

Module 1: Threat Intelligence Basics

- Threat Intelligence Basics
- Threat Intelligence Use Cases
- Threat Intelligence Development

Module 2: Cyber Threats

- Cyber Threat Overview
- Cyber Threats Classification
- Prevention Against Cyber Threats
- Examples of Cyber Threats in History

Module 3: Threat Actors

- Threat Actors Overview
- Threat Actors Classification
- Examples of threat Actors in History

C)TIA: Certified Threat Intelligence Analyst

Course ID #: 7000-780-ZZ-Z
Hours: 35

Module 4: Cyber Threats & Malicious Actors Case Studies

- Student
- EternalBlue
- WannaCry
- Wizard Spider Group
- Operation Aurora
- Zerologon

Module 5: Threats Identification

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

Module 6: Implementing a Proactive Threat Intelligence Approach

- Scope, Goals, and Characteristics of a Proactive Threat Intelligence Approach
- Implementation and Practicability
  - Threat Intelligence Feeds
  - Threat Intelligence Communities
  - Threat Intelligence Tools

Labs:

Lab 1: Identifying Incident Triggers
Lab 2: Drafting Incident Response Procedures
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

Accreditations:

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