CERTIFIED CYBER THREAT
INTELLIGENCE ANALYST
CCTIA

Duration: 5 days; Instructor-led | Virtual Instructor-led

WHAT WILL YOU LEARN

The attendees of this training will learn in-depth about security threats, attacks, vulnerabilities, and attacker behavior. They will also learn about the MITRE ATT&CK Framework and how to identify attacker techniques, tactics, and procedures in order to investigate indicators of compromise and respond to eliminate the attack or incident. The training will also cover the concepts of Threat Intelligence and how to integrate it with various technologies such as SIEM, SOAR, EDR, and other SOC technologies to reduce the time it takes to detect and respond to attacks. Attendees will also learn how to set up a Threat Intelligence Framework and platform for their organization and consume community and commercial feeds to understand attacks and defend their organization from future attacks. Additionally, attendees will learn how to set up a Malware Information Sharing Platform and integrate it with incident response processes using HIVE and automate them as a single workflow.

OBJECTIVES

Threat Intelligence is an evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject’s response to that menace or hazard. With Intelligence and Automation equipping cyber criminals to conduct targeted and stealth attacks, it us utmost important for enterprises to be equipped with cyber threat intelligence to achieve a cyber resilient posture.

- Gain in-depth knowledge of security threats, attacks, vulnerabilities, attacker’s behaviors, cyber kill chain, SOC processes, procedures, technologies, and automation workflows
- Understand the MITRE ATT&CK Framework and Able to identify attacker techniques, tactics, and procedures (TTP) to investigate on indicators of compromise (IOCs) and provide automated / manual responses to eliminate the attack/incident
- Able to understand the concepts of Threat Intelligence and gain in-depth knowledge on how to integrate Threat Intelligence with the SIEM, SOAR, EDR and other SOC technologies to reduce the Mean time to Detect (MTTD) and Mean time to Respond (MTTR)
- Able to Understand and learn how to setup a Threat Intelligence Framework and platform for your organization and consume community and commercial feeds to understand attacks and defend your organization from future attacks
- Gain in-depth knowledge on Malware Information Sharing Platform (MISP) and learn to setup a working instance with configurations and integrations that can be used immediately in your organisation
- Gain knowledge of Incident Response Methodology, processes and in-depth knowledge on how to integrate Threat Intelligence processes with Incident Response processes using HIVE and learn how to automate them as a single workflow

PREREQUISITES

Not applicable.

AUDIENCE

Cybersecurity Analysts, Network and Security Administrators, Entry-level cybersecurity professionals, SOC Analyst

COURSE CONTENTS

Module 1: Introduction to Threat Intelligence

- Understanding Threats, Threat Modeling and Risk
- What is Threat Intelligence
- Need for Threat Intelligence
- Benefits of Threat Intelligence
- Types of Threat Intelligence
- Threat Intelligence Life Cycle
- Sources of Threat Intelligence
- Technologies contributing to Threat Intelligence (SIEM, EDR, Log Sources)
- Threat Intelligence & SOC
- Incident Response & Threat Intelligence
- Applications of Threat Intelligence
- Threat Intelligence Frameworks (CIF, MISP, TAXII)
- Role of Threat Intelligence Analyst & Threat Hunters

Module 2: Technical Deep Dive on Latest Attacks

- What is Security, Vulnerabilities & O-Days, Attack life Cycle, Different Attack Vectors
- Threats Vs. Risks, Why Perimeter defenses are failing? Why Anti-Virus is not enough?
- Introduction to Cyber Kill Chain
- Indicators of Compromise (IOC) & IOC Sources (OTX, MISP)
- Business Email Compromise (BEC) (Lab) with Indicators of Compromise
- Ransomware (Lab) with Indicators of Compromise

- Advanced Persistent Threat (Lab) with Indicators of Compromise
- File-less Malwares (Lab) with Indicators of Compromise
- Mobile Malwares (Lab) with Indicators of Compromise
- Web Data Breach (Lab) with Indicators of Compromise
- Malvertising (Lab) with Indicators of Compromise
- Social Media based attacks (Lab) with Indicators of Compromise
- Password based attacks (Password Stuffing, Account Takeover, Phishing, etc) (Lab)
- What is MITRE ATT&CK Framework ?
- Tactics, Techniques and Procedures (TTP)
- Threat Actors
- ATT&CK Navigator
- The ThreatHunter-Playbook
- Atomic Red Team Library
- Threat-Based Adversary Emulation with ATT&CK
- Behavioral-based analytic detection using ATT&CK
- Mapping to ATT&CK from Raw Data – Lab
- Storing and analyzing ATT&CK-mapped intel

Module 3: Setting up Threat Intel Framework

- Enterprise Threat Landscape Mapping
- Scope & Plan Threat Intel Program
- Setup Threat Intel Team
- Threat Intelligence Feeds, Sources & Data Collections
- Open source Threat Intel Collections (OSINT and more)
- Dark Web Threat Intel Collections
- SIEM / Log Sources Threat Intel Collections
- Pubic Web data Threat Intel Collections (Maltego, OSTrICa, and more)
- Threat Intel collections with YARA
- EDR Threat Intel Collections
- Incorporating Threat Intel into Incident Response
- Threat Intel & Actionable Contextual Data
- Commercial Threat Intel Feed Providers (RecordedFuture, BlueLiv, etc.)
- Commercial Threat Intel Platforms (Anamoli, DigitalShadows, etc.)

Module 4: Malware Information Sharing Platform (MISP)

- MISP Project Overview
- MISP Features & Use cases
- Events, Objects and Attributes in MISP
- MISP Data model & Core data structure
- MISP - Creating and populating events
- MISP - Distribution and Topology
- MISP Galaxy
- MISP Object Templates
- MISP Deployment and Integrations
- Normalizing OSINT and other community & Private Feeds
- SIEM and MISP Integration
- Incident Response and threat hunting using MISP
- Viper and MISP
- MISP Administration
- MISP feeds - A simple and secure approach to generate, select and collect intelligence
- MISP and Decaying of Indicators
- Workflow of a security analyst using Viper as a management console for malware analysis

Module 5: Cybersecurity Incident Response

- Introduction to Incident Response
- Incident Response & Handling Methodology
- MISP & HIVE Integrations
- HIVE Implementation
- Malware Analysis Use case using MISP & HIVE