



Certified Threat Intelligence Analyst

Course Outline

Module 01: Introduction to Threat Intelligence

Understanding Intelligence

- Intelligence Definition and Essential Terminology
- Intelligence vs. Information vs. Data
- Intelligence-Led Security Testing (Background and Reasons)

Understanding Cyber Threat Intelligence

- Cyber Threat Intelligence (CTI)
- Cyber Threat Intelligence Stages
- Characteristics of Threat Intelligence
- Benefits of CTI
- Enterprise Objectives for Threat Intelligence Programs
- How can Threat Intelligence Help Organizations
- Types of Threat Intelligence
 - Strategic Threat Intelligence
 - Tactical Threat Intelligence
 - Operational Threat Intelligence
 - Technical Threat Intelligence
- Threat Intelligence Generation
- Threat Intelligence Informed Risk Management
- Integration of Threat Intelligence into SIEM
- Leverage Threat Intelligence for Enhanced Incident Response
 - Enhancing Incident Response by Establishing SOPs for Threat Intelligence
- Organizational Scenarios using Threat Intelligence

- What Organizations and Analysts Expect?
- Common Information Security Organization (CISO) Structure
 - Cyber Threat Analyst Responsibilities
- Threat Intelligence Use Cases

Overview of Threat Intelligence Lifecycle and Frameworks

- Threat Intelligence Lifecycle
- Threat Analyst Roles in Threat Intelligence Lifecycle
- Threat Intelligence Strategy
- Threat Intelligence Capabilities
- Capabilities to Look for in Threat Intelligence Solution
- Threat Intelligence Maturity Model
- Threat Intelligence Frameworks
 - Collective Intelligence Framework (CIF)
 - CrowdStrike Cyber Threat Intelligence Solution
 - NormShield Threat and Vulnerability Orchestration
 - MISP - Open Source Threat Intelligence Platform
 - TC Complete
 - Yeti
 - ThreatStream
- Additional Threat Intelligence Frameworks

Module 02: Cyber Threats and Kill Chain Methodology

Understanding Cyber Threats

- Overview of Cyber Threats
- Cyber Security Threat Categories
- Threat Actors/Profiling the Attacker
- Threat: Intent, Capability, Opportunity Triad
- Motives, Goals, and Objectives of Cyber Security Attacks
- Hacking Forums

Understanding Advanced Persistent Threats (APTs)

- Advanced Persistent Threats (APTs)

- Characteristics of Advanced Persistent Threats (APTs)
- Advanced Persistent Threat Lifecycle

Understanding Cyber Kill Chain

- Cyber Kill Chain Methodology
- Tactics, Techniques, and Procedures (TTPs)
- Adversary Behavioral Identification
- Kill Chain Deep Dive Scenario - Spear Phishing

Understanding Indicators of Compromise (IoCs)

- Indicators of Compromise (IoCs)
- Why Indicators of Compromise Important?
- Categories of IoCs
- Key Indicators of Compromise
- Pyramid of Pain

Module 03: Requirements, Planning, Direction, and Review

Understanding Organization's Current Threat Landscape

- Identify Critical Threats to the Organization
- Assess Organization's Current Security Pressure Posture
 - Assess Current Security Team's Structure and Competencies
 - Understand Organization's Current Security Infrastructure and Operations
- Assess Risks for Identified Threats

Understanding Requirements Analysis

- Map out Organization's Ideal Target State
- Identify Intelligence Needs and Requirements
- Define Threat Intelligence Requirements
 - Threat Intelligence Requirement Categories
- Business Needs and Requirements
 - Business Units, Internal Stakeholders, and Third-Parties
 - Other Teams
- Intelligence Consumers Needs and Requirements
- Priority Intelligence Requirements (PIRs)

- Factors for Prioritizing Requirements
- MoSCoW Method for Prioritizing Requirements
- Prioritize Organizational Assets
- Scope Threat Intelligence Program
- Rules of Engagement
- Non-Disclosure Agreements
- Avoid Common Threat Intelligence Pitfalls

Planning Threat Intelligence Program

- Prepare People, Processes, and Technology
- Develop a Collection Plan
- Schedule Threat Intelligence Program
- Plan a Budget
- Develop Communication Plan to Update Progress to Stakeholders
- Aggregate Threat Intelligence
- Select a Threat Intelligence Platform
- Consuming Intelligence for Different Goals
- Track Metrics to Keep Stakeholders Informed

Establishing Management Support

- Prepare Project Charter and Policy to Formalize the Initiative
 - Establish Your Case to Management for a Threat Intelligence Program
 - Apply a Strategic Lens to the Threat Intelligence Program

Building a Threat Intelligence Team

- Satisfy Organizational Gaps with the Appropriate Threat Intelligence Team
 - Understand different Threat Intelligence Roles and Responsibilities
 - Identify Core Competencies and Skills
 - Define Talent Acquisition Strategy
 - Building and Positioning an Intelligence Team
 - How to Prepare an Effective Threat Intelligence Team

Overview of Threat Intelligence Sharing

- Establishing Threat Intelligence Sharing Capabilities
- Considerations for Sharing Threat Intelligence

- Sharing Intelligence with Variety of Organizations
- Types of Sharing Partners
- Important Selection Criteria for Partners
- Sharing Intelligence Securely

Reviewing Threat Intelligence Program

- Threat Intelligence Led Engagement Review
- Considerations for Reviewing Threat Intelligence Program
- Assessing the Success and Failure of the Threat Intelligence Program

Module 04: Data Collection and Processing

Overview of Threat Intelligence Data Collection

- Introduction to Threat Intelligence Data Collection
- Data Collection Methods
- Types of Data
- Types of Threat Intelligence Data Collection

Overview of Threat Intelligence Collection Management

- Understanding Operational Security for Data Collection
- Understanding Data Reliability
- Ensuring Intelligence Collection Methods Produce Actionable Data
- Validate the Quality and Reliability of Third Party Intelligence Sources
- Establish Collection Criteria for Prioritization of Intelligence Needs and Requirements
- Building a Threat Intelligence Collection Plan

Overview of Threat Intelligence Feeds and Sources

- Threat Intelligence Feeds
- Threat Intelligence Sources

Understanding Threat Intelligence Data Collection and Acquisition

- Threat Intelligence Data Collection and Acquisition
- Data Collection through Open Source Intelligence (OSINT)
 - Data Collection through Search Engines
 - Data Collection through Advanced Google Search
 - Data Collection through Google Hacking Database

- Data Collection through ThreatCrowd
- Data Collection through Deep and Dark Web Searching
- Data Collection through Web Services
 - Finding Top-level Domains (TLDs) and Sub-domains
 - Data Collection through Job Sites
 - Data Collection through Groups, Forums, and Blogs
 - Data Collection through Social Networking Sites
 - Data Collection related to Blacklisted and Whitelisted Sites
- Data Collection through Website Footprinting
 - Data Collection through Monitoring Website Traffic
 - Data Collection through Website Mirroring
 - Extracting Website Information from <https://archive.org>
 - Extracting Metadata of Public Documents
- Data Collection through Emails
 - Data Collection by Tracking Email Communications
 - Data Collection from Email Header
 - Data Collection through Emails: eMailTrackerPro
- Data Collection through Whois Lookup
- Data Collection through DNS Interrogation
 - Data Collection through DNS Lookup and Reverse DNS Lookup
 - Fast-Flux DNS Information Gathering
 - Dynamic DNS (DDNS) Information Gathering
 - DNS Zone Transfer Information Gathering
- Automating OSINT effort using Tools/Frameworks/Scripts
 - Maltego
 - OSTRiCa (Open Source Threat Intelligence Collector)
 - OSRFramework
 - FOCA
 - GOSINT
 - Automating OSINT effort using Tools/Frameworks/Scripts
- Data Collection through Human Intelligence (HUMINT)

- Data Collection through Human-based Social Engineering Techniques
- Data Collection through Interviewing and Interrogation
- Social Engineering Tools
- Data Collection through Cyber Counterintelligence (CCI)
 - Data Collection through Honeypots
 - Data Collection through Passive DNS Monitoring
 - Data Collection through Pivoting Off Adversary's Infrastructure
 - Data Collection through Malware Sinkholes
 - Data Collection through YARA Rules
- Data Collection through Indicators of Compromise (IoCs)
 - IoC Data Collection through External Sources
 - Commercial and Industry IoC Sources
 - IT-ISAC
 - Free IoC Sources
 - AlienVault OTX
 - Blueliv Threat Exchange Network
 - MISP
 - threat_note
 - Cacador
 - IOC Bucket
 - Tools for IoC Data Collection through External Sources
 - IoC Data Collection through Internal Sources
 - Tools for IoC Data Collection through Internal Sources
 - Splunk Enterprise
 - Valkyrie Unknown File Hunter
 - IOC Finder
 - Redline
 - Data Collection through Building Custom IoCs
 - Tools for Building Custom IoCs
 - IOC Editor
 - Steps for effective usage of Indicators of Compromise (IoCs) for Threat Intelligence

- Data Collection through Malware Analysis
 - Preparing Testbed for Malware Analysis
 - Data Collection through Static Malware Analysis
 - Data Collection through Dynamic Malware Analysis
 - Malware Analysis Tools
 - Blueliv Threat Exchange Network
 - Valkyrie
 - Tools for Malware Data Collection

Understanding Bulk Data Collection

- Introduction to Bulk Data Collection
- Forms of Bulk Data Collection
- Benefits and Challenges of Bulk Data Collection
- Bulk Data Management and Integration Tools

Understanding Data Processing and Exploitation

- Threat Intelligence Data Collection and Acquisition
- Introduction to Data Processing and Exploitation
- Structuring/Normalization of Collected Data
- Data Sampling
 - Types of Data Sampling
- Storing and Data Visualization
- Sharing the Threat Information

Module 05: Data Analysis

Overview of Data Analysis

- Introduction to Data Analysis
- Contextualization of Data
- Types of Data Analysis

Understanding Data Analysis Techniques

- Statistical Data Analysis
 - Data Preparation
 - Data Classification

- Data Validation
- Data Correlation
- Data Scoring
- Statistical Data Analysis Tools
 - SAS/STAT Software
 - IBM SPSS
- Analysis of Competing Hypotheses (ACH)
 - Hypothesis
 - Evidence
 - Diagnostics
 - Refinement
 - Inconsistency
 - Sensitivity
 - Conclusions and Evaluation
- ACH Tool
 - PARC ACH
- Structured Analysis of Competing Hypotheses (SACH)
- Other Data Analysis Methodologies

Overview of Threat Analysis

- Introduction to Threat Analysis
- Types of Threat Intelligence Analysis

Understanding Threat Analysis Process

- Threat Analysis Process and Responsibilities
- Threat Analysis based on Cyber Kill Chain Methodology
- Aligning the Defensive Strategies with the Phases of the Cyber Kill Chain Methodology
- Perform Threat Modeling
 - Asset Identification
 - System Characterization
 - System Modeling
 - Threat Determination and Identification
 - Threat Profiling and Attribution

- Threat Ranking
- Threat Information Documentation
- Threat Modeling Methodologies
 - STRIDE
 - PASTA
 - TRIKE
 - VAST
 - DREAD
 - OCTAVE
- Threat Modeling Tools
 - Microsoft Threat Modelling Tool
 - ThreatModeler
 - securiCAD Professional
 - IriusRisk
- Enhance Threat Analysis Process with the Diamond Model Framework
- Enrich the Indicators with Context
- Validating and Prioritizing Threat Indicators

Overview of Fine-Tuning Threat Analysis

- Fine-Tuning Threat Analysis
- Identifying and Removing Noise
- Identifying and Removing Logical Fallacies
- Identifying and Removing Cognitive Biases
- Automate Threat Analysis Processes
- Develop Criteria for Threat Analysis Software
- Employ Advanced Threat Analysis Techniques
 - Machine Learning based Threat Analysis
 - Cognitive based Threat Analysis

Understanding Threat Intelligence Evaluation

- Threat Intelligence Evaluation
- Threat Attribution

Creating Runbooks and Knowledge Base

- Developing Runbooks
- Create an Accessible Threat Knowledge Repository
- Organize and Store Cyber Threat Information in Knowledge Base

Overview of Threat Intelligence Tools

- Threat Intelligence Tools
 - AlienVault USM Anywhere
 - IBM X-Force Exchange
 - ThreatConnect
 - SurfWatch Threat Analyst
 - AutoFocus
 - Additional Threat Intelligence Tools

Module 06: Intelligence Reporting and Dissemination

Overview of Threat Intelligence Reports

- Threat Intelligence Reports
- Types of Cyber Threat Intelligence Reports
 - Threat Analysis Reports
 - Threat Landscape Reports
- Generating Concise Reports
- Threat Intelligence Report Template
- How to Maximize the Return from Threat Intelligence Report
- Continuous Improvement via Feedback Loop
- Report Writing Tools
 - MagicTree
 - KeepNote

Introduction to Dissemination

- Overview of Dissemination
- Preferences for Dissemination
- Benefits of Sharing Intelligence
- Challenges to Intelligence Sharing

- Disseminate Threat Intelligence Internally
- Building Blocks for Threat Intelligence Sharing
- Begin Intelligence Collaboration
- Establish Information Sharing Rules
- Information Sharing Model
- Information Exchange Types
- TI Exchange Architectures
- TI Sharing Quality
- Access Control on Intelligence Sharing
- Intelligence Sharing Best Practices

Participating in Sharing Relationships

- Why Sharing Communities are Formed?
- Join a Sharing Community
- Factors to be Considered When Joining a Community
- Engage in Ongoing Communication
- Consume and Respond to Security Alerts
- Consume and Use Indicators
- Produce and Publish Indicators
- External Intelligence Sharing
- Establishing Trust
- Organizational Trust Models

Overview of Sharing Threat Intelligence

- Sharing Strategic Threat Intelligence
- Sharing Tactical Threat Intelligence
- Sharing Operational Threat Intelligence
- Sharing Technical Threat Intelligence
- Sharing Intelligence using YARA Rules
- IT-ISAC (Information Technology - Information Security and Analysis Center)

Overview of Delivery Mechanisms

- Forms of Delivery
- Machine Readable Threat Intelligence (MRTI)

- Standards and Formats for Sharing Threat Intelligence
 - Traffic Light Protocol (TLP)
 - MITRE Standards
 - Managed Incident Lightweight Exchange (MILE)
 - VERIS
 - IDMEF

Understanding Threat Intelligence Sharing Platforms

- Information Sharing and Collaboration Platforms
 - Blueliv Threat Exchange Network
 - Anomali STAXX
 - MISP (Malware Information Sharing Platform)
 - Cyware Threat Intelligence eXchange (CTIX)
 - Soltra Edge
 - Information Sharing and Collaboration Platforms

Overview of Intelligence Sharing Acts and Regulations

- Cyber Intelligence Sharing and Protection Act (CISPA)
- Cybersecurity Information Sharing Act (CISA)

Overview of Threat Intelligence Integration

- Integrating Threat Intelligence
- How to Integrate CTI into the Environment
- Acting on the Gathered Intelligence
- Tactical Intelligence Supports IT Operations: Blocking, Patching, and Triage
- Operational Intelligence Supports Incident Response: Fast Reaction and Remediation
- Strategic Intelligence Supports Management: Strategic Investment and Communications