T | I E
Threat | Intelligence Essentials

EC-Council
Building A Culture Of Security

Threat Intelligence Essentials

COURSE OUTLINE

EC-Council Official Curricula

Threat Intelligence Essentials (TIE)

Course Outline

(Version 1)

Module 01: Introduction to Threat Intelligence

- Threat Intelligence and Essential Terminology
  - What is Threat Intelligence?
  - Core Threat Intelligence Terminology
- Key Differences Between Intelligence, Information, and Data
  - Threat Intelligence vs. Threat Data
- The Importance of Threat Intelligence
- Integrating Threat Intelligence in Cyber Operations
  - Modern Threat Intelligence vs. Traditional Cybersecurity
- Threat Intelligence Lifecycles and Maturity Models
  - Threat Intelligence Lifecycle and Processes
  - Threat Intelligence Maturity Model
- Threat Intelligence Roles, Responsibilities, and Use Cases
  - Threat Intelligence Team Roles & Responsibilities
  - Threat Intelligence Use Cases
  - Ethical and Legal Considerations
- Using Threat Intelligence Standards or Frameworks to Measure Effectiveness
  - Frameworks and Standards
  - KPI's for Measuring Effectiveness

- Establishing SPLUNK Attack Range for Hands-on Experience
  - Module 1 Lab: SPLUNK Attack Range 3.0 Overview
  - Attack Range Setup

Module 02: Types of Threat Intelligence

- Understanding the Different Types of Threat Intelligence
  - General Sources of Threat Intelligence
  - The Threat Intelligence Array
- Preview Use Cases for Different Types of Threat Intelligence
  - Navigating Different Uses of Intelligence
  - Specific Uses of Threat Intelligence by Type
- Overview of the Threat Intelligence Generation Process
  - The Threat Intelligence Generation Process
  - Sources of Generated Threat Intelligence
- Learn How Threat Intelligence Informs Regulatory Compliance
  - How Regulation Influences Threat Intelligence Processes
  - Other Regulatory Factors to Consider
- Augmenting Vulnerability Management with Threat Intelligence
  - Threat Intelligence and Vulnerability Management
  - Additional Best Practices to Consider
- Explore Geopolitical or Industry Related Threat Intelligence
  - Geopolitical and Industry Focused Threat Intelligence
  - How Cybersecurity Can Leverage These Sources
- Integrating Threat Intelligence with Risk Management
  - Threat Intelligence in Risk Management

Module 03: Cyber Threat Landscape

- Overview of Cyber Threats Including Trends and Challenges
  - Defining the Cyber Threat Challenge
- Emerging Threats, Threat Actors, and Attack Vectors
  - Threat Actor Types and Their Motivations

- Trends and Challenges Impacting Threat Intelligence

- Deep Dive on Advanced Persistent Threats
  - Getting to Know Your Advanced Persistent Threat
  - High Profile Threat Actors in Modern Times
- The Cyber Kill Chain Methodology
  - What's the Cyber Kill Chain Methodology?
  - Exploring Other Cyber Kill Chains
- Vulnerabilities, Threat Actors, and Indicators of Compromise (IoC)
  - Indicators of Compromise (IoCs) Explained
  - Key Vulnerability Management Control Considerations
- Geopolitical and Economic Impacts Related to Cyber Threats
  - Impact of Geopolitics and Economics on Cyber Threats
- How Emerging Technology is Impacting the Threat Landscape
- MITRE ATT&CK & SPLUNK Attack Range IOC Labs
  - Module 3 Lab Part 1: MITRE ATT&CK Navigator
  - Module 3 Lab Part 2: Reviewing Indicators of Compromise (IoC) in Attack Range

Module 04: Data Collection and Sources of Threat Intelligence

- Making Use of Threat Intelligence Feeds, Sources, & Evaluation Criteria
  - Maximizing Use of Threat Data Feeds
  - Popular Sources of Threat Data
  - Evaluating Threat Data Credibility & Effectiveness
- Overview of Threat Intelligence Data Collection Methods & Techniques
  - Overview of Threat Data Collection Methods
  - Dissemination Channels for Threat Data
- Compare & Contrast Popular Data Collection Methods
  - Active vs Passive Threat Data Collection
  - Effective Uses for Active & Passive Data Collection
  - Other Intelligence Gathering Techniques
- Bulk Data Collection Methods & Considerations
  - Bulk Data Collection Types

- Bulk Data Collection Considerations

- Normalizing, Enriching, & Extracting Useful Intelligence from Threat Data
  - Normalizing Threat Data Before Enrichment
  - The Data Enrichment Process
  - Additional Tips for Extracting Actionable Intelligence from Threat Data
- Legal & Ethical Considerations for Threat Data Collection Processes
  - Ethical and Legal Risks Data Collection Must Account For
- Threat Data Feed Subscription and OSINT Labs
  - Module 4 Lab Part 1: Subscribing to and Ingesting FREE Threat Data from APIs

Module 05: Threat Intelligence Platforms

- Introduction Threat Intelligence Platforms (TIPs), Roles, & Features
  - Primary Features of a Threat Intelligence Platform
  - Notable TIP Providers & Solutions
- Aggregation, Analysis, & Dissemination within TIPs
  - From Threat Data Aggregation to TIP Dissemination
  - Risks of TIP Mismanagement
  - Driving TIP Effectiveness & Accuracy
- Automation & Orchestration of Threat Intelligence in TIPs
  - The Importance of Automation & Orchestration within TIPs
  - Desired Automation Outcomes
  - Orchestration Benefits Within a TIP
- Evaluating & Integrating TIPs into Existing Cybersecurity Infrastructure
  - TIP Evaluation Criteria: The Tangible vs Intangible
  - Elements to Consider During Trials
  - Integration Consideration for TIPs
- Collaboration, Sharing, and Threat Hunting Features of TIPs
  - Macro Vs Micro Collaboration Goals of TIPs
  - Ways That Threat Intelligence Platforms Share Data
  - Threat Hunting on TIPs
- Customizing TIPs for Organizational Needs

- The Customization Solution
- Ideal TIP Customization Features and Criteria

- Using TIPs for Visualization, Reporting, & Decision Making
  - How TIP Reporting and Visualizations Drive Key Business Decisions
  - Driving Effective Practices in TIP Reporting and Visualization
- AlienVault OTX and MISP TIP Platform Labs
  - Module 5 Lab 1 Overview: AlienVault OTX and Pulses
  - Module 5 Lab 2: Exploring MISP

Module 06: Threat Intelligence Analysis

- Introduction to Data Analysis and Techniques
  - Data Analysis Defined
  - Using Data Analysis for Threat Intelligence
  - Other Uses & Analysis Considerations
- Applying Statistical Data Analysis, Including Analysis of Competing Hypothesis
  - A Deeper Look into Statistical Analysis for Threat Intelligence: Malware Inspection
  - Analysis of Competing Hypothesis
- Identifying and Analyzing Threat Actor Artifacts
  - Applying Analysis Techniques to IoC Data
  - Applying Analytical Techniques to TTP Data
  - Driving Excellence in Data Analysis Practices
- Threat Prioritization, Threat Actor Profiling & Attribution Concepts
  - How Data Analysis Assists Threat Prioritization
  - Intro to Threat Actor Profiling
  - Understanding and Improving Threat Attribution
- Leveraging Predictive and Proactive Threat Intelligence
  - Predictive vs Proactive Threat Intelligence
  - Maximizing the Use of Predictive Threat Intelligence
  - Rewinding on Proactive Threat Intelligence
- Reporting, Communicating, and Visualizing Intelligence Findings
  - Tips for Highly Effective Threat Reporting

- Using MISP for Threat Intelligence Reporting & Visualization
- Using Jupyter Notebooks to Visualize Data

- Threat Actor Profile Labs & MISP Report Generation Labs
  - Module 6 Lab 1 – Cyber Threat Actor Profile Exercise
  - Module 6 – Lab 2: Generating MISP Threat Reports and Connecting MISP To Jupyter Notebooks

Module 07: Threat Hunting and Detection

- Operational Overview of Threat Hunting & Its Importance
  - What Is Threat Hunting?
  - General Threat Hunting Approach
  - Characteristics of Successful Threat Hunters
- Dissecting the Threat Hunting Process
  - Considerations Before Conducting Threat Hunts
  - Deep Diving the Threat Hunting Process
  - Key Metrics to Guide Effective Threat Hunting
- Threat Hunting Methodologies & Frameworks
  - What are Threat Hunting Frameworks and Why Use Them?
  - Hunting Framework Concepts: The Pyramid of Pain
  - Using the PEAK Methodology for Threat Hunting
- Explore Proactive Threat Hunting
  - The Need for Proactive Threat Hunting
  - Key Differences Between Proactive & Unstructured Threat Hunting
  - When Proactive Threat Hunts Shine
- Using Threat Hunting for Detection & Response
  - The Role of Threat Hunting in Incident Detect & Response
  - Common Ground Between Incident Response & Threat Hunting
- Threat Hunting Tool Selection & Useful Techniques
  - Types of Threat Hunting Tools
  - Popular Threat Hunting Tools & Techniques
  - Best Practices for Tool Selection

- Forming Threat Hunting Hypotheses & Conducting Hunts
  - The Value of Threat Hunting Hypotheses
  - Hunting Tactics, Techniques & Procedures (TTP)
  - Overview of MITRE's TTP Hunting Methodology
- Threat Hunting Lab in SPLUNK ATT&CK Range
  - Overview of Threat Hunting Lab

Module 08: Threat Intelligence Sharing and Collaboration

- Importance of Information Sharing Initiatives in Threat Intelligence
  - The Importance of Information Sharing Initiatives
  - Types of Information Sharing Arrangements
  - Threat Information Sharing Frameworks
- Overview of Additional Threat Intelligence Sharing Platforms
  - Threat Information Sharing Platforms
  - Desirable Features of Sharing Platforms
  - Potential Platform Pitfalls
- Building Trust Within Intelligence Communities
  - Primary Trust Builders
  - How Trust in Small Private Circles or Larger Public Communities is Achieved
- Sharing Information Across Industries and Sectors
  - Benefitting from Cross-Industry Threat Sharing
  - Sector Specific Threat Sharing
  - Cross-Sector Collaboration Communities
- Building Private and Public Threat Intelligence Sharing Channels
  - Approaches for Establishing Private Threat Intel Channels
  - Approaches for Establishing Public Threat Intel Channels
- Challenges and Best Practices for Threat Intelligence Sharing
  - Best Practices for Sharing Threat Intel
  - Threat Intelligence Sharing Challenges
  - Modern Examples of Overcoming Sharing Challenges
- Legal and Privacy Implications of Sharing Threat Intelligence

- Legal and Compliance Impacts
- Privacy Implications of Careless Intel Sharing

- Sharing Threat Intelligence Using MISP and Installing Anomali STAXX
  - Module 8 Lab: MISP to MISP Intel Sharing and Setting Up & Navigating Anomali STAXX

Module 09: Threat Intelligence in Incident Response

- Integrating Threat Intelligence into Incident Response Processes
  - Overview of the Security Incident Response Lifecycle
  - Threat Intelligence Integration Examples
  - Potential Threat Intelligence Integration Drawbacks
- Role of Threat Intelligence in Incident Prevention Using Workflows & Playbooks
  - Threat Intelligence's Role in Incident Prevention
  - Malicious Process Real-Time Response (RTR) Workflow Example
  - Ransomware Playbook Example
- Using Threat Intelligence for Incident Triage and Forensic Analysis
  - How Threat Intelligence Aids Incident Triage
  - The Role of Threat Intelligence During Forensic Analysis
- Adapting Incident Response Plans Using New Intelligence
  - Threat Intel as an Incident Response Adaptation Pathway
  - Best Practice Considerations
  - Adaptation Pitfalls to Avoid
- Coordinating Response With External Partners
  - Applying Threat Intelligence to Different Incidents
  - How Threat Intelligence Assists External Partner Collaboration
- Threat Intelligent Incident Handling and Recovery Approaches
  - Applying Threat Intelligence to Different Incident Types
  - Using Threat Intelligence During Incident Recovery
- Post Incident Analysis and Lessons Learned Considerations
  - Post-Incident Analysis and Areas of Emphasis
  - Merging Threat Intelligence Into Lessons Learned Activities

- Measurement and Continuous Improvement for Intelligence Driven Incident Response
  - Approaches for Achieving Continuous Improvement
  - KPIs to Measure Threat Intelligence's Influence on Incident Response

Module 10: Future Trends and Continuous Learning

- Emerging Threat Intelligence Approaches & Optimizing Their Use
  - Complimentary Approaches to Threat Intelligence
  - Applying Threat Intelligence to Emerging Technologies
  - Optimizing Use of Emergent Technology for Threat Intelligence Operations
- Convergence of Threat Intelligence & Risk Management
  - Getting Started with Converging Threat Intelligent Risk Management
  - A More Methodological Approach
- Continuous Learning Approaches for Threat Intelligence
  - Contemporary vs Evolving Learning Models
  - Striking an Effective Balance
- Adapting Professional Skillsets for Future in Threat Intelligence
  - Adapting Existing Career Paths to Threat Intelligence
  - Skills to Future Proof A Threat Intelligence Career
- Anticipating Future Challenges & Opportunities in Threat Intelligence
  - Potential Challenges Down the Road
  - The Upside Opportunities of Threat Intelligence
- Engaging in the Threat Intelligence Community & Keeping a Pulse on the Threat Landscape
  - Engaging in Threat Intelligence Communities
  - Keeping a Pulse on the Cyber Threat Landscape
- The Role of Threat Intelligence in National Security & Defense
  - Threat Intelligence For National Defense Use Cases
  - Providers of National Defense Quality Threat Intelligence
- Potential Influence of Threat Intelligence on Future Cybersecurity Regulations
  - Historical Examples & Benefits of Threat Intelligence's Influence on Regulation
  - The Potential Downsides of Shaping Policy With Threat Intelligence