SSDN TECHNOLOGIES
Evolving Your Skills

EC-Council

Threat Intelligence Essentials Program Information

Course Duration: 16 Hrs. **Course code: 112-57**

Course Overview

The Threat Intelligence Essentials course provides learners with a strong foundational knowledge of threat intelligence concepts and tools. Covering essential topics such as the cyber threat landscape and its various types, this course prepares you for a progressive career path as a threat intelligence analyst.

What you'll learn?

- Understand foundational principles and terminology of threat intelligence.
- Differentiate between various types of threat intelligence and their use cases.
- Analyze the current cyber threat landscape and identify key threat actors.
- Conduct effective data collection from credible threat intelligence sources.
- Utilize Threat Intelligence Platforms (TIPs) for data aggregation and analysis.
- Apply data analysis techniques to evaluate and prioritize threats.
- Develop and execute hypothesis-driven threat hunts within networks.

Target Audience

- Security Professionals: Security analysts, engineers, architects, and managers.
- Threat Intelligence Analysts: Those already working in threat intelligence roles, as well as those looking to enter the field.
- SOC Professionals: Security Operations Center analysts and staff.
- Incident Response Team Members: Individuals involved in responding to security incidents.
- Cybersecurity Enthusiasts: Individuals interested in learning about cybersecurity and threat intelligence.
- Ethical Hackers: Professionals involved in ethical hacking and penetration testing.

Phone: +91-999-911-1686 **Mail Us:** info@ssdntech.com

Pre-Requisites

- Basic understanding of cybersecurity concepts and terminology.
- Familiarity with networking fundamentals, including knowledge of TCP/IP and common protocols.
- Experience using Windows and Linux operating systems, as well as basic command-line skills.
- Awareness of common security threats and vulnerabilities.
- Interest in threat intelligence and a willingness to explore advanced cybersecurity topics.

Course content

Module 1: Introduction to Threat Intelligence

A. Threat Intelligence and Essential Terminology
B. Key Differences Between Intelligence, Information, and Data
C. The Importance of Threat Intelligence
D. Integrating Threat Intelligence in Cyber Operations
E. Threat Intelligence Lifecycles and Maturity Models
F. Threat Intelligence Roles, Responsibilities, and Use Cases
G. Using Threat Intelligence Standards or Frameworks to Measure Effectiveness
H. Establishing SPLUNK Attack Range for Hands-on Experience

Module 2: Types of Threat Intelligence

A. Understanding the Different Types of Threat Intelligence
B. Preview Use Cases for Different Types of Threat Intelligence
C. Overview of the Threat Intelligence Generation Process
D. Learn How Threat Intelligence Informs Regulatory Compliance
E. Augmenting Vulnerability Management with Threat Intelligence
F. Explore Geopolitical or Industry Related Threat Intelligence
G. Integrating Threat Intelligence with Risk Management

Phone: +91-999-911-1686 **Mail Us:** info@ssdntech.com

Module 3: Cyber Threat Landscape

A. Overview of Cyber Threats Including Trends and Challenges
B. Emerging Threats, Threat Actors, and Attack Vectors
C. Deep Dive on Advanced Persistent Threats
D. The Cyber Kill Chain Methodology
E. Vulnerabilities, Threat Actors, and Indicators of Compromise (IoC)
F. Geopolitical and Economic Impacts Related to Cyber Threats
G. How Emerging Technology is Impacting the Threat Landscape
H. MITRE ATT&CK & Splunk Attack Range IOC Labs

Module 4: Data Collection and Sources of Threat Intelligence

A. Making Use of Threat Intelligence Feeds, Sources, and Evaluation Criteria
B. Overview of Threat Intelligence Data Collection Methods and Techniques
C. Compare and Contrast Popular Data Collection Methods
D. Bulk Data Collection Methods and Considerations
E. Normalizing, Enriching, and Extracting Useful Intelligence from Threat Data
F. Legal and Ethical Considerations for Threat Data Collection Processes
G. Threat Data Feed Subscription and OSINT Labs

Module 5: Threat Intelligence Platforms

A. Introduction to Threat Intelligence Platforms (TIPs), Roles, and Features
B. Aggregation, Analysis, and Dissemination within TIPs
C. Automation and Orchestration of Threat Intelligence in TIPs
D. Evaluating and Integrating TIPs into Existing Cybersecurity Infrastructure
E. Collaboration, Sharing, and Threat Hunting Features of TIPs
F. Customizing TIPs for Organizational Needs
G. Using TIPs for Visualization, Reporting, and Decision Making
H. AlienVault OTX and MISP TIP Platform Labs

Module 6: Threat Intelligence Analysis

A. Introduction to Data Analysis and Techniques
B. Applying Statistical Data Analysis, Including Analysis of Competing Hypothesis

C. Identifying and Analyzing Threat Actor Artifacts
D. Threat Prioritization, Threat Actor Profiling, and Attribution Concepts
E. Leveraging Predictive and Proactive Threat Intelligence
F. Reporting, Communicating, and Visualizing Intelligence Findings
G. Threat Actor Profile Labs and MISP Report Generation Labs

Module 7: Threat Hunting and Detection

A. Operational Overview of Threat Hunting and Its Importance
B. Dissecting the Threat Hunting Process
C. Threat Hunting Methodologies and Frameworks
D. Explore Proactive Threat Hunting
E. Using Threat Hunting for Detection and Response
F. Threat Hunting Tool Selection and Useful Techniques
G. Forming Threat Hunting Hypotheses for Conducting Hunts
H. Threat Hunting Lab in SPLUNK ATT&CK Range

Module 8: Threat Intelligence Sharing and Collaboration

A. Importance of Information Sharing Initiatives in Threat Intelligence
B. Overview of Additional Threat Intelligence Sharing Platforms
C. Building Trust Within Intelligence Communities
D. Sharing Information Across Industries and Sectors
E. Building Private and Public Threat Intelligence Sharing Channels
F. Challenges and Best Practices for Threat Intelligence Sharing
G. Legal and Privacy Implications of Sharing Threat Intelligence
H. Sharing Threat Intelligence Using MISP and Installing Anomali STAXX

Module 9: Threat Intelligence in Incident Response

A. Integrating Threat Intelligence into Incident Response Processes
B. Role of Threat Intelligence in Incident Prevention Using Workflows and Playbooks
C. Using Threat Intelligence for Incident Triage and Forensic Analysis
D. Adapting Incident Response Plans Using New Intelligence
E. Coordinating Response with External Partners

Phone: +91-999-911-1686 **Mail Us:** info@ssdntech.com

F. Threat Intelligent Incident Handling and Recovery Approaches
G. Post Incident Analysis and Lessons Learned Considerations
H. Measurement and Continuous Improvement for Intelligence Driven Incident Response

Module 10: Future Trends and Continuous Learning

A. Emerging Threat Intelligence Approaches and Optimizing Their Use
B. Convergence of Threat Intelligence and Risk Management
C. Continuous Learning Approaches for Threat Intelligence
D. Adapting Professional Skillsets for Future in Threat Intelligence
E. Anticipating Future Challenges and Opportunities in Threat Intelligence
F. Engaging in the Threat Intelligence Community and Keeping a Pulse on the Threat Landscape
G. The Role of Threat Intelligence in National Security and Defense
H. Potential Influence of Threat Intelligence on Future Cybersecurity Regulations

Exam Preference

Exam Code	112-57
Number Of Questions	75
Length Of Test	120 Minutes
Passing Score	75%

Phone: +91-999-911-1686 **Mail Us:** info@ssdntech.com