TIE – Threat Intelligence Essentials (e-Learning)

EC-Council

Com certificação

- **Nível:**
- **Duração:** 18h

Sobre o curso

Spring Deals: Cursos EC-Council com 5% de desconto até 30 de abril

The **Threat Intelligence Essentials** course equips learners with a strong technical foundational knowledge of threat intelligence concepts and tools. It provides essential knowledge in topics like cyber threat landscape, types of threat landscape, and more preparing you for progressive career paths as a threat intelligence analyst. No IT/Cybersecurity experience required for this course.

Test your learnings with CTF-based Capstone Project and validate your newly acquired skills in proctored exams. Further, the course offers 18+ hours of premium self-paced video training in 10 modules with 5 labs to prepare students for real-world pro

Key Features:

- 18+ hours of premium self-paced video training
- 5 lab activities in a simulated lab environment
- 900+ pages of eCourseware
- Capstone Project
- Year-long access to courseware and 6-month access to labs
- Proctored exam voucher with 1-year validity
- Acquire skills to identify, assess, select, build, and execute threat intelligence workflows
- Earn EC-Council’s globally recognized certificate. Increase your value in the job market

What Skills You’ll Learn

- Essential threat intelligence terminology, the role of intelligence in cybersecurity, and threat intelligence maturity models.
- Evaluating different types of threat intelligence, such as strategic, operational, and more focused forms, which guide vulnerability management or regulatory landscapes.
- The cyber threat landscape, trends, and ongoing challenges

- Data collection and sources of threat intelligence
- Threat Intelligence Platforms (TIPs)
- Threat intelligence analysis
- Threat hunting and detection
- Threat intelligence sharing and collaboration
- Threat intelligence in incident response
- Future trends and continuous learning

Destinatários

Who is T|IE for?

- High School/College/University students
- Teams and organization
- Career starters
- Working professionals

Pré-requisitos

No prior cybersecurity knowledge or IT work experience required.

Metodologia

Training Details: Self-paced in demand lecture videos led by world-class instructors and hands-on labs.

Exam Details:

- Exam Code: 112-54
- Number of Questions: 75
- Duration: 2 hours
- Test Format: Multiple Choice

Programa

- Introduction to Threat Intelligence
- Types of Threat Intelligence
- Cyber Threat Landscape
- Data Collection and Sources of Threat Intelligence
- Threat Intelligence Platforms
- Threat Intelligence Analysis
- Threat Hunting and Detection

- Threat Intelligence Sharing and Collaboration
- Threat Intelligence in Incident Response
- Future Trends and Continuous Learning

Introduction to Threat Intelligence

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

Types of Threat Intelligence

- Understanding the Different Types of Threat Intelligence
- Preview Use Cases for Different Types of Threat Intelligence
- Overview of the Threat Intelligence Generation Process
- Learn How Threat Intelligence Informs Regulatory Compliance
- Augmenting Vulnerability Management with Threat Intelligence
- Explore Geopolitical or Industry Related Threat Intelligence
- Integrating Threat Intelligence with Risk Management

Cyber Threat Landscape

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

Data Collection and Sources of Threat Intelligence

- Making Use of Threat Intelligence Feeds, Sources, and Evaluation Criteria
- Overview of Threat Intelligence Data Collection Methods and Techniques
- Compare and Contrast Popular Data Collection Methods
- Bulk Data Collection Methods and Considerations
- Normalizing, Enriching, and Extracting Useful Intelligence from Threat Data
- Legal and Ethical Considerations for Threat Data Collection Processes
- Threat Data Feed Subscription and OSINT Labs

Threat Intelligence Platforms

- Introduction to Threat Intelligence Platforms (TIPs), Roles, and Features
- Aggregation, Analysis, and Dissemination within TIPs
- Automation and Orchestration of Threat Intelligence within TIPs
- Bulk Data Collection Methods and Considerations
- Evaluating and Integrating TIPs into Existing Cybersecurity Infrastructure
- Collaboration, Sharing, and Threat Hunting Features of TIPs
- Customizing TIPs for Organizational Needs
- Using TIPs for Visualization, Reporting, and Decision Making
- AlienVault OTX and MISP TIP Platform Labs

Threat Intelligence Analysis

- Introduction to Data Analysis and Techniques
- Applying Statistical Data Analysis, Including Analysis of Competing Hypothesis
- Analysis Methods for Threat Actor Artifacts
- Threat Prioritization, Threat Actor Profiling, and Attribution Concepts
- Leveraging Predictive and Proactive Threat Intelligence
- Reporting, Communicating, and Visualizing Intelligence Findings
- Threat Actor Profile Labs and MISP Report Generation Lab

Threat Hunting and Detection

- Operational Overview of Threat Hunting and Its Importance
- Dissecting the Threat Hunting Process
- Threat Hunting Methodologies and Frameworks
- Explore Proactive Threat Hunting
- Using Threat Hunting for Detection and Response
- Threat Hunting Tool Selection and Useful Techniques
- Forming Threat Hunting Hypotheses for Conducting Hunts

Threat Hunt Lab

Threat Intelligence Sharing and Collaboration

- Importance of Information Sharing Initiatives in Threat Intelligence
- Overview of Additional Threat Intelligence Sharing Platforms
- Building Trust Within Intelligence Communities
- Sharing Information Across Industries and Sectors
- Building Private and Public Threat Intelligence Sharing Channels
- Challenges and Best Practices for Threat Intelligence Sharing
- Legal and Privacy Implications of Sharing Threat Intelligence
- Sharing Threat Intelligence Using MISP and Installing Anomali STAXX

Threat Intelligence in Incident Response

- Introduction to Threat Intelligence Platforms (TIPs), Roles, and Features
- Aggregation, Analysis, and Dissemination within TIPs

- Automation and Orchestration of Threat Intelligence within TIPs
- Bulk Data Collection Methods and Considerations
- Evaluating and Integrating TIPs into Existing Cybersecurity Infrastructure
- Collaboration, Sharing, and Threat Hunting Features of TIPs
- Customizing TIPs for Organizational Needs
- Using TIPs for Visualization, Reporting, and Decision Making
- AlienVault OTX and MISP TIP Platform Labs

Future Trends and Continuous Learning

- Emerging Technologies in Threat Intelligence
- Evolution of Threat Intelligence in Response to Advanced Threats
- Threat Intelligence for Emerging Technologies
- The Role of Threat Intelligence in Evolving Cyber Threats
- The Convergence of Threat Intelligence and Risk Management
- Importance of Continuous Learning and Professional Development in Threat Intelligence
- Career Paths and Opportunities in the Threat Intelligence Field
- Anticipating Future Challenges and Opportunities in Threat Intelligence
- Engaging with the Threat Intelligence Community
- Keeping Up to Date with Evolving Threat Landscapes
- Ethical Considerations in Threat Intelligence Research and Reporting
- Global and Regional Threat Intelligence Trends and Challenges
- The Role of Threat Intelligence in National Security and Defense
- The Influence of Threat Intelligence on Cybersecurity Regulations