EC-Council Threat Intelligence Essentials (TIE)

Category: Networking & Security | **Vendor:** EC-Council

Duration: 16.00 hours (2 days) **13.0 CPD Hours** **Rating:** ⭐ 4.6 (5,878 reviews)

Course Information

Delivery Format: Instructor Led - Online

Course Overview

Cybersecurity and technology-based mitigation approaches rely heavily on intelligence. This program aims to enhance your understanding and implementation of foundational threat intelligence concepts, including differentiating intelligence from data or information and highlighting its vital role in modern cybersecurity. Additionally, the program enables students to thoroughly explore the threat intelligence lifecycle, understand its significance in shaping team roles, delve into the ethical and legal considerations, and understand the importance of measuring threat intelligence effectiveness. As you progress through the program, you'll master the different types of threat intelligence: strategic, operational, tactical, and technical. You'll learn how each uniquely contributes to areas like regulatory compliance and risk management. In the later modules, you'll engage in hands-on activities that involve data collection, analysis, and the use of Threat Intelligence Platforms (TIPs) for real-world applications in threat hunting and detection. Put your newly acquired abilities to the test with an exhilarating Capture the Flag (CTF) Exercise seamlessly integrated in our Capstone project. This CTF is seamlessly integrated by live virtual machines, genuine software, and real networks, all delivered within a secure and regulated sandbox environment. With these exclusive hands-on, human-versus-machine CTF challenges you will develop the hands-on proficiencies essential for success in your cyber professional role. The program culminates with a forward-looking perspective, emphasizing the importance of continuous learning and staying ahead of future trends in this ever-evolving field. Threat Intelligence Essentials is designed to prepare students for progressive careers as Security Operations Center (SOC) Analysts, Threat Intelligence Analysts, IT Risk Analysts, or Cybersecurity Analysts, enabling them to confidently tackle today's cybersecurity challenges with expertise!

About This Course

Cybersecurity and technology-based mitigation approaches rely heavily on intelligence. This program aims to enhance your understanding and implementation of foundational threat intelligence concepts, including differentiating intelligence from data or information and highlighting its vital role in modern cybersecurity. Additionally, the program enables students to thoroughly explore the threat intelligence lifecycle, understand its significance in shaping team roles, delve into the ethical and legal considerations, and understand the importance of measuring threat intelligence effectiveness. As you progress through the program, you'll master the different types of threat intelligence: strategic, operational, tactical, and technical. You'll learn how each uniquely contributes to areas like regulatory compliance and risk management. In the later modules, you'll engage in hands-on activities that involve data collection, analysis, and the use of Threat Intelligence Platforms (TIPs) for real-world applications in threat hunting and detection. Put your newly acquired abilities to the test with an exhilarating Capture the Flag (CTF) Exercise seamlessly integrated in our Capstone project. This CTF is seamlessly integrated by live virtual machines, genuine software, and real networks, all delivered within a secure and regulated sandbox environment. With these exclusive hands-on, human-versus-machine CTF challenges you will develop the hands-on proficiencies essential for success in your cyber professional role. The program culminates with a forward-looking perspective, emphasizing the importance of continuous learning and staying ahead of future trends in this ever-evolving field. Threat Intelligence Essentials is designed to prepare students for progressive careers as Security Operations Center (SOC) Analysts, Threat Intelligence Analysts, IT Risk Analysts, or Cybersecurity Analysts, enabling them to confidently tackle today's cybersecurity challenges with expertise!

Who Should Attend

- School students, graduates, professionals, career starters and changers, IT/Technology/Cybersecurity teams with little or no work experience.
- Anyone who wants to start a career in cybersecurity or threat intelligence.
- Anyone interested in threat intelligence, Indicators of Compromise (IoC) analysis, defensive cybersecurity operations, and incident response.
- Any professional involved in securing public, private, and hybrid cloud infrastructures, identities, data, and applications.
- IT / Cybersecurity professionals, system administrators, cloud administrators, cybersecurity administrators, engineers, and architects will also benefit from this course.

Learning Outcomes

Upon successful completion of this course, participants will be able to:

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

Detailed Course Outline

Module 01: 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

Module 02: 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

Module 03: 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

Module 04: Data Collection and Sources of Threat Intelligence

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

Module 05: Threat Intelligence Platforms

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

Module 06: Threat Intelligence Analysis

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

Module 07: Threat Hunting and Detection

- Operational Overview of Threat Hunting & Its Importance
- Dissecting the Threat Hunting Process
- Threat Hunting Methodologies & Frameworks
- Explore Proactive Threat Hunting
- Using Threat Hunting for Detection & Response
- Threat Hunting Tool Selection & Useful Techniques
- Forming Threat Hunting Hypotheses & Conducting Hunts
- Threat Hunting Lab in SPLUNK ATT&CK Range

Module 08: 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

Module 09: Threat Intelligence in Incident Response

- Integrating Threat Intelligence into Incident Response Processes
- Role of Threat Intelligence in Incident Prevention Using Workflows & Playbooks
- Using Threat Intelligence for Incident Triage and Forensic Analysis
- Adapting Incident Response Plans Using New Intelligence
- Coordinating Response With External Partners
- Threat Intelligent Incident Handling and Recovery Approaches
- Post Incident Analysis and Lessons Learned Considerations
- Measurement and Continuous Improvement for Intelligence Driven Incident Response

Module 10: Future Trends and Continuous Learning

- Emerging Threat Intelligence Approaches & Optimizing Their Use
- Convergence of Threat Intelligence & Risk Management
- Continuous Learning Approaches for Threat Intelligence
- Adapting Professional Skillsets for Future in Threat Intelligence
- Anticipating Future Challenges & Opportunities in Threat Intelligence
- Engaging in the Threat Intelligence Community & Keeping a Pulse on the Threat Landscape
- The Role of Threat Intelligence in National Security & Defense
- Potential Influence of Threat Intelligence on Future Cybersecurity Regulations

Frequently Asked Questions

Q: What delivery options are available for EC-Council Threat Intelligence Essentials (TIE)?

We offer multiple delivery formats:

- Live Instructor-Led Classroom Online (Virtual/Live Online)
- Traditional Instructor-Led Classroom Training (ILT)
- On-site delivery at your offices anywhere in United Kingdom
- Private dedicated courses customized for your team

Q: How many CPD hours does this course provide?

The 2-day EC-Council Threat Intelligence Essentials (TIE) course provides up to 13.0 CPD hours of structured learning. CPD certificates can be provided upon request.

Q: What is the duration of the EC-Council Threat Intelligence Essentials (TIE) training?

The training takes place over 2 day(s), with each day lasting approximately 16.00 hours including breaks for lunch and refreshments.

Q: Do you provide corporate training for EC-Council Threat Intelligence Essentials (TIE)?

Yes, we provide corporate training, dedicated training, and closed classes for EC-Council Threat Intelligence Essentials (TIE). Training can take place anywhere in United Kingdom including London, Manchester, Birmingham, Edinburgh, or live online allowing teams from across United Kingdom or internationally to attend.

Q: Why choose Nexus Human for EC-Council Threat Intelligence Essentials (TIE)?

Nexus Human is recognized as one of the leading training providers. Our trainers have won multiple awards including:

- Small Firms Best Trainer Award
- National Training Partner of the Year (Ireland) - Multiple Years
- Global Top 30 Instructor Awards (2012, 2019, 2021)
- Tech Excellence Award Nominations
- Learning Performance Institute (LPI) External Training Provider Sponsor 2024

Q: Are there any discount codes available?

Yes! Use discount code **PENPAL5** when booking your EC-Council Threat Intelligence Essentials (TIE) training. Please note that only one discount code can be used per booking and cannot be combined with other special offers.

Nexus Human

Professional Training & Development

Email: info@nexushuman.com

Website: www.nexushuman.com

Phone: +353 1 XXX XXXX (Ireland) | +44 20 XXXX XXXX (UK)