EC-Council
Building A Culture Of Security

T | I E
Threat | Intelligence Essentials

Threat Intelligence Essentials

Begin Your Cybersecurity Journey with Hands-On, Technical Foundational Skills in Threat Intelligence

No IT / Cybersecurity Experience Required

Video Lessons • Hands-on Labs • CTF Challenges • Proctored Exam

EC-COUNCIL ESSENTIALS SERIES

Navigating the intricate landscape of cybersecurity can be challenging due to its numerous specialized domains, making it difficult to focus on a specific area and develop essential foundational skills. Introducing the Essentials Series—a carefully curated program aimed at nurturing a new generation of skilled cybersecurity professionals right from the start of their careers. This hands-on, immersive program is designed to help learners develop fundamental technical proficiency in cybersecurity without compromising affordability.

Best-suited for school students, recent graduates, career switchers, beginners, and IT/Technology teams with limited or no prior experience in IT/Cybersecurity, the program empowers learners to independently explore and determine their areas of specialization while building a diverse skill set across essential domains. Gain skills for your first CTF competition with this Essentials Series Course. The final module of lab capstone project features a simulated CTF to test your skills in a controlled environment. Use live virtual machines, real software, and networks to solve real-world challenges as a hacker or defender.

EC-Council's Essentials Series covers 8 essential skills, which include Ethical Hacking, Network Defense, Digital Forensics, Cloud Security, IoT Security, SOC, Threat Intelligence, and DevSecOps.

What is EC-Council Threat Intelligence Essentials?

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!

Threat Intelligence Essentials Program Information

Course Outline

Module 1: Introduction to Threat Intelligence

This section will introduce you to the program and provide you with foundational information about threat intelligence.

Lab: Students will install the DetectionLab Security Operations Center (SOC) virtual environment. This Detection Lab environment will assist students in completing hands-on threat intelligence exercises found in Modules 3, 6, and 7.

Module Objectives:

1. Students will learn fundamental principles and terminology, allowing them to quickly identify, separate, and act upon useful threat intelligence.
2. Students will better understand threat intelligence's role in enhancing a cybersecurity function, maximizing organizational value, and implementing frameworks to increase threat intelligence effectiveness.
3. Students will install a defensive cybersecurity lab environment that will be useful throughout this program and as they advance further in their cybersecurity or threat intelligence careers.

Topics Covered:

- 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 2: Types of Threat Intelligence

This section will focus on helping students understand key distinctions and use cases for various threat intelligence types. Students will further understand how various sources generate threat intelligence and how it informs downstream cybersecurity processes or compliance functions.

Module Objectives:

1. Students will be able to articulate and explain the core differences between types of threat intelligence.
2. Students will understand how threat intelligence is created and how it impacts regulatory decisions or essential cybersecurity controls.
3. After completing this section, students will be able to comprehend the importance of various threat intelligence types and how to effectively select or integrate appropriate threat intelligence into specific business processes or situational scenarios.

Topics Covered:

- 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 3: Cyber Threat Landscape

This section will help students better understand the current state of cybersecurity threats, emerging trends, obstacles, and how current threat actors are impacting society.

Labs:

(1) Previewing MITRE ATT&CK in DetectionLab
(2) Indicators of Compromise Overview in DetectionLab

Module Objectives:

1. Students will learn the key concepts surrounding cyber threats and how to define them.
2. Students will understand how threat actors, attack vectors, vulnerabilities, and exploits generate Indicators of Compromise (IoC) and how emerging technologies can complicate defensive efforts.
3. After completing this section, students will be able to understand cyber threat actor profiles, their operational models, telemetry generated by threat actors, and how IoCs inform threat intelligence efforts.

Topics Covered:

- 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 4: Data Collection and Sources of Threat Intelligence

This section will teach students how to conduct searches or acquire threat intelligence from reputable sources. Students will also learn how to conduct Open-Source Intelligence (OSINT) gathering activities and other threat intelligence collection methods directly.

Labs:

(1) Registering for MS-ISAC, Center for Internet Security (CIS) and other Threat Intelligence Advisories

(2) Methodologies & Techniques for Conducting OSINT Investigations with TraceLab

Module Objectives:

1. Students will learn how to assess threat intelligence sources for credibility, different data collection methods, and concepts useful for managing threat intelligence data.
2. Students will be introduced to several direct and indirect threat intelligence collection methods, such as OSINT, HUMINT, and IoC analysis.
3. After completing this section, students will gain competence in directly assessing threat intelligence data sources, acquiring reputable threat intelligence, focusing data collection efforts, and exploiting useful elements from acquired threat intelligence.

Topics Covered:

- 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

Module 5: Threat Intelligence Platforms

This section will show students how to access and use several leading Threat Intelligence Platforms (TIPs), such as the AlienVault Open Threat Exchange (OTX) and MISP.

Labs:
(1) Accessing and Searching for IoC data in AlienVault Open Threat Exchange
(2) Setting up and Deploying MISP to enrich threat intelligence data

Module Objectives:

1. Students will learn how to leverage external or internal Threat Intelligence Platforms (TIPs) to gather actionable data to reduce their attack surface.
2. Students will be introduced to data management concepts for threat intelligence to drive efficiencies and effective use of threat intelligence received from TIPs.
3. After completing this section, students will gain competence in accessing and directly leveraging TIPs for threat hunting, cybersecurity risk validation, and data aggregation or information sharing purposes.

Topics Covered:

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

Module 6: Threat Intelligence Analysis

This section will help students explore and apply data analysis techniques against acquired threat intelligence, including Indicators of Compromise (IoC) and tactics, techniques, or procedures generated by threat actors. Students will learn how to prioritize multiple threats, comprehensive threat intelligence reporting, and concepts for visualizing threat intelligence data sets.

Labs:
(1) Generating and Reviewing TTP data in DetectionLab
(2) Building a sample Threat Actor Profile

Module Objectives:

1. Students will learn the importance and differences of threat intelligence data analysis methods.

2. Students will learn how to correlate, enrich, and build essential reporting metrics around acquired threat intelligence.
3. After completing this section, students will acquire hands-on experience with identifying relevant threats in their environment, communicating threat actor data using key metrics, and focusing defensive efforts using actionable threat intelligence.

Topics Covered:

- 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, and Attribution Concepts
- Leveraging Predictive and Proactive Threat Intelligence
- Reporting, Communicating, and Visualizing Intelligence Findings
- Threat Actor Profile Labs and MISP Report Generation Labs

Module 7: Threat Hunting and Detection

This section will provide an operational overview of Threat Hunting, contemporary threat hunting methodologies, and tools or techniques students can leverage to perform hypothesis-driven threat hunts.

Labs:
(1) Conducting a guided Threat Hunt in DetectionLab

Module Objectives:

1. Students will learn core threat-hunting terminology, methods, and frameworks used to conduct threat hunts.
2. Students will learn how threat hunting may be achieved through monitored endpoint solutions and/or across a network.
3. After completing this section, students will gain direct experience in developing and executing threat-hunting hypotheses to drive proactive cybersecurity processes within an organization.

Topics Covered:

- 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 Hunting Lab in SPLUNK ATT&CK Range

Module 8: Threat Intelligence Sharing and Collaboration

This section will discuss the benefits of threat intelligence information sharing, platforms used to share industry-specific threat intelligence, and the cybersecurity or regulatory concerns that influence information sharing.

Labs:
(1) Sharing Threat Intelligence using the Anomali Platform

Module Objectives:

1. Students will learn how proper information sharing can decrease the cybersecurity attack surface for organizations.
2. Students will be introduced to threat intelligence information-sharing platforms, products, and techniques.
3. After completing this section, students will understand how to properly share or receive shared threat intelligence using available open-source or free platforms.

Topics Covered:

- 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 9: Threat Intelligence in Incident Response

This section will discuss methods students can adopt to integrate threat intelligence effectively into cybersecurity Incident Response (IR) plans or processes. Concepts covered in this section include incorporating threat intelligence into triage, forensics, lessons learned, and other incident response processes.

Module Objectives:

1. Students will learn how threat intelligence can be incorporated into cybersecurity incident response plans and processes, including its role in incident prevention or post-mortem activities.
2. Students will be introduced to concepts that allow them to build or update incident response playbooks that are driven by appropriate and relevant threat intelligence.
3. After completing this section, students will better understand how threat intelligence can shorten incident resolution and reduce future cybersecurity attacks against organizations.

Topics Covered:

- Integrating Threat Intelligence into Incident Response Processes
- Role of Threat Intelligence in Incident Prevention Using Workflows and 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

This section will discuss the impact of technological developments like Artificial Intelligence (AI) that are helping to drive innovation in the Threat Intelligence community. This section will also explore complementary educational sources that will allow them to enhance their professional development or pursue threat intelligence career options and approaches that are useful for staying current with modern threat intelligence practices.

Module Objectives:

1. Students will learn about emerging technologies that are impacting the threat intelligence community, core security processes, and technology frameworks like IoT.
2. Students will overview threat intelligence career paths, approaches to ongoing professional development, and engagement with the broader threat intelligence community.
3. After completing this section, students will understand future risks and technologies impacting the threat intelligence community and educational approaches they can adopt to keep pace with this fast-paced industry.

Topics Covered:

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

What Skills You'll Learn

1. Essential threat intelligence terminology, the role of intelligence in cybersecurity, and threat intelligence maturity models.
2. Evaluating different types of threat intelligence, such as strategic, operational, and more focused forms, which guide vulnerability management or regulatory landscapes.
3. The cyber threat landscape, trends, and ongoing challenges
4. Data collection and sources of threat intelligence
5. Threat Intelligence Platforms (TIPs)
6. Threat intelligence analysis
7. Threat hunting and detection
8. Threat intelligence sharing and collaboration
9. Threat intelligence in incident response
10. Future trends and continuous learning

Who Is It For?

- 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.

Training & Exam

Training Details: Self-paced in-demand lecture videos led by world-class instructors and hands-on labs.
Pre-requisite: No prior cybersecurity knowledge or IT work experience required.

Exam Details:

- Exam Code: 112-57
- Number of Questions: 75
- Duration: 2 hours
- Test Format: Multiple Choice

Key Features

- Engage in 5 practical lab exercises to comprehensively understand how to conduct threat intelligence operations directly.
- 18+ hours of premium self-paced video training
- 900+ pages of ecourseware
- Capstone Projects with Real-World CTF Challenges
- Year-long access to courseware and 6-month access to labs
- Proctored exam voucher with one-year validity
- Acquire skills to identify, assess, select, build, and execute threat intelligence workflows.
- Increase your value in the job market to advance your career.
- Earn EC-Council's globally recognized certificate.

Why EC-Council's Essentials Series is the Most Popular and Fastest Growing Beginner Level Training Program for Career Starters and Career Changers

213,000+ Learners Trust EC-Council's Essentials Series

150+ Countries

85+ Million Minutes Watched

4.95/5.0 Average Ratings

96.46% of Learners Gave a 5* Rating

Why Do Professionals, Students, Career Starters and Changers Worldwide Choose the EC-Council's Essentials Certification?

Gene (USA)

Strong Cybersecurity Foundation.

★★★★★

It has given me a solid foundation in the basics of cybersecurity. I now have a better understanding of the different types of cyberattacks, the tools and techniques that attackers use, and the ways to protect myself and my organization from these attacks.

Taylor Cooper (USA)

Career Advancement through Ethical Hacking.

★★★★★

This has helped me enhance my knowledge and skills in tech. I will be able to showcase my knowledge by certifying myself as an ethical hacker and adding it to my resume, which will give me an opportunity to advance in my career and opt for higher-paying roles.

Deeptankshu (USA)

Top Notched Cyber Investigation Skills.

★★★★★

It helped by teaching me how to collect data and evidence to solve crimes and prevent wrongdoers in the Cyber realm. As a Security and Intelligence major, I want to be well-versed in the Cyber realm as well as other realms.

Samuel Tetteh (USA)

Strong Foundation for Digital Forensics

★★★★★

After completing this course, I had the foundation I needed. It assisted me in completing my MS Cybersecurity course in digital forensics, which expanded my knowledge even further. This foundation is perfect for a start in Digital forensics.

Brian (USA)

Rebuilding Network Defense Knowledge.

★★★★★

This course helped rebuild my baseline knowledge of network defense, which I required before progressing toward more advanced studies in the field.

Nicolas Ntibaziyaremye (USA)
Practical Learning for Career Growth.
★★★★★

The course is project-based. This allows me to apply what I learn in the lectures to real-world problems. I have learned a lot from this course, and I am confident that it will help me in my career.

Learn Foundational Cybersecurity Skills with EC-Council's 8 Essential Series

E|HE Ethical Hacking Essentials	**N|DE** Network Defense Essentials
D|SE DevSecOps Essentials	**I|SE** IoT Security Essentials
D|FE Digital Forensic Essentials	**C|SE** Cloud Security Essentials
S|CE SOC Essentials	**T|IE** Threat Intelligence Essentials

About
EC-Council

EC-Council's sole purpose is to build and refine the cybersecurity profession globally. We help individuals, organizations, educators, and governments address global workforce problems by developing and curating world-class cybersecurity education programs and their corresponding certifications. We also provide cybersecurity services to some of the largest businesses globally. Trusted by 7 of the Fortune 10, 47 of the Fortune 100, the Department of Defence, Intelligence Community, NATO, and over 2,000 of the best Universities, Colleges, and Training Companies, our programs have proliferated through over 140 countries. They have set the bar in cybersecurity education. Best known for the Certified Ethical Hacker programs, we are dedicated to equipping over 2,30,000 information age soldiers with the knowledge, skills, and abilities required to fight and win against the black hat adversaries. EC-Council builds individual and team/organization cyber capabilities through the Certified Ethical Hacker Program, followed by a variety of other cyber programs, including Certified Secure Computer User, Computer Hacking Forensic Investigator, Certified Security Analyst, Certified Network Defender, Certified SOC Analyst, Certified Threat Intelligence Analyst, Certified Incident Handler, as well as the Certified Chief Information Security Officer.

We are an ANAB 17024 accredited organization and have earned recognition by the DoD under Directive 8140/8570 in the UK by the GCHQ, CREST, and various other authoritative bodies that influence the entire profession.

Founded in 2001, EC-Council employs over 400 individuals worldwide with ten global offices in the USA, UK, Malaysia, Singapore, India, and Indonesia. Its US offices are in Albuquerque, NM, and Tampa, FL.

Learn more at www.eccouncil.org

T | I E

Threat | Intelligence Essentials

Threat Intelligence Essentials

www.eccouncil.org