EC-COUNCIL 112-57

EC-COUNCIL TIE Certification Questions & Answers

Exam Summary – Syllabus –Questions

112-57

EC-Council Threat Intelligence Essentials (TIE)

75 Questions Exam – 70% Cut Score – Duration of 120 minutes

Table of Contents:

Know Your 112-57 Certification Well:.....2

EC-Council 112-57 TIE Certification Details:.....2

112-57 Syllabus:.....2

EC-Council 112-57 Sample Questions:.....6

Study Guide to Crack EC-Council TIE 112-57 Exam: 9

Know Your 112-57 Certification Well:

The 112-57 is best suitable for candidates who want to gain knowledge in the EC-Council Essentials Series. Before you start your 112-57 preparation you may struggle to get all the crucial TIE materials like 112-57 syllabus, sample questions, study guide.

But don't worry the 112-57 PDF is here to help you prepare in a stress-free manner. The PDF is a combination of all your queries like-

- What is in the 112-57 syllabus?
- How many questions are there in the 112-57 exam?
- Which Practice test would help me to pass the 112-57 exam at the first attempt?

Passing the 112-57 exam makes you EC-Council Threat Intelligence Essentials (TIE). Having the TIE certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

EC-Council 112-57 TIE Certification Details:

Exam Name	EC-Council Threat Intelligence Essentials (TIE)
Exam Code	112-57
Exam Price	$299 (USD)
Duration	120 mins
Number of Questions	75
Passing Score	70%
Schedule Exam	**ECC Exam Center**
Sample Questions	**EC-Council TIE Sample Questions**
Practice Exam	**EC-Council 112-57 Certification Practice Exam**

112-57 Syllabus:

Topic	**Details**
Introduction to Threat Intelligence	- Threat Intelligence and Essential Terminology - Key Differences Between Intelligence, Information, and Data

Topic	Details
	- 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

Topic	Details
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 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
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, and Attribution Concepts - Leveraging Predictive and Proactive Threat Intelligence - Reporting, Communicating, and Visualizing Intelligence Findings

Topic	Details
	- Threat Actor Profile Labs and MISP Report Generation Labs
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 Hunting Lab in SPLUNK ATT&CK Range
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	- 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

Topic	Details
	Approaches - Post Incident Analysis and Lessons Learned Considerations - Measurement and Continuous Improvement for Intelligence Driven Incident Response
Future Trends and Continuous Learning	- 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

EC-Council 112-57 Sample Questions:

Question: 1

Why is it crucial to integrate threat intelligence with risk management?

a) To increase the financial risks to the organization
b) To focus risk management on external business investments
c) To reduce the importance of risk management
d) To ensure that threat intelligence efforts are aligned with the organization's risk appetite and management strategies

Answer: d

Question: 2

How does establishing a defensive cybersecurity lab environment benefit students in threat intelligence?

a) It provides a controlled setting for practical application and experimentation with threat intelligence tools and techniques
b) It reduces the cost of cybersecurity education
c) It eliminates the need for real-world experience
d) It focuses on theoretical knowledge only

Answer: a

Question: 3

What is a key benefit of visualizing intelligence findings?

a) It makes reports less detailed
b) It uses more resources without providing additional insights
c) It helps stakeholders quickly understand complex data and trends
d) It is only for aesthetic purposes

Answer: c

Question: 4

Why is it important for cybersecurity professionals to understand threat intelligence lifecycles and maturity models?

a) To manage payroll systems more effectively
b) To increase social media engagement
c) To improve sales strategies
d) To develop and enhance threat intelligence programs systematically

Answer: d

Question: 5

Why is hands-on experience with threat intelligence platforms essential for cybersecurity professionals?

a) It is not essential but provides a minor benefit
b) Hands-on experience is only necessary for senior management
c) It helps them practically apply theoretical knowledge and improve their ability to use threat intelligence effectively
d) It is only needed for compliance purposes

Answer: c

Question: 6

What is the role of the MITRE ATT&CK framework in understanding the cyber threat landscape?

a) It provides a comprehensive matrix of tactics and techniques used by threat actors
b) It is used to train new employees about general IT skills
c) It simplifies legal compliance unrelated to cybersecurity
d) It is unrelated to cybersecurity and focuses on physical security

Answer: a

Question: 7

In what way do TIPs facilitate better information sharing within and between organizations?

a) By limiting access to information
b) Through collaboration features that allow secure sharing of intelligence
c) By only allowing top management to access intelligence
d) They do not support information sharing

Answer: b

Question: 8

How do threat actors, attack vectors, and vulnerabilities collectively shape the cyber threat landscape?

a) They have no significant interaction
b) They are independent factors that do not influence each other
c) They collectively define the nature and potential impact of threats in the landscape
d) They decrease the need for cybersecurity

Answer: c

Question: 9

What is the significance of the geopolitical and economic context in analyzing the cyber threat landscape?

a) It is only relevant for multinational corporations
b) It has no real impact on cyber security
c) It is primarily important for historical research
d) It provides key insights that influence cyber threats and their impacts on global security

Answer: d

Question: 10

Describe the importance of identifying Indicators of Compromise (IoCs) in the cyber threat landscape.

a) IoCs are only useful for post-incident reporting
b) They help in identifying signs of potential or actual security breaches
c) They are primarily used for financial audits
d) They decrease the operational efficiency of security teams

Answer: b

Study Guide to Crack EC-Council TIE 112-57 Exam:

- Getting details of the 112-57 syllabus, is the first step of a study plan. Completion of the syllabus is must to pass the 112-57 exam.
- Making a schedule is vital. A structured method of preparation leads to success.
- Joining the EC-Council provided training for 112-57 exam could be of much help. If there is specific training for the exam, you can discover it from the link above.
- Read from the 112-57 sample questions to gain your idea about the actual exam questions. In this PDF useful sample questions are provided to make your exam preparation easy.
- Practicing on 112-57 practice tests is must. Continuous practice will make you an expert in all syllabus areas.