



**EC-Council**



# **Certified Threat Intelligence Analyst (CTIA)**



Exam Blueprint v1

Domains	Sub Domain	Description	Number of Questions	Weightage
<b>1. Introduction to Threat Intelligence</b>	1.1 Understanding Intelligence	<ol style="list-style-type: none"> <li>1. Definition of Intelligence and Its Essential Terminology</li> <li>2. Intelligence vs. Information vs. Data</li> <li>3. Intelligence-Led Security Testing (Background and Reasons)</li> </ol>	3	18%
	1.2 Understanding Cyber Threat Intelligence	<ol style="list-style-type: none"> <li>1. Definition of Cyber Threat Intelligence</li> <li>2. Stages of Cyber Threat Intelligence</li> <li>3. Characteristics of Threat Intelligence</li> <li>4. Benefits of Cyber Threat Intelligence</li> <li>5. Enterprise Objectives for Threat Intelligence Programs</li> <li>6. How Can Threat Intelligence Help Organizations?</li> <li>7. Types of Threat Intelligence                             <ol style="list-style-type: none"> <li>7.1 Strategic Threat Intelligence</li> <li>7.2 Tactical Threat Intelligence</li> <li>7.3 Operational Threat Intelligence</li> <li>7.4 Technical Threat Intelligence</li> </ol> </li> <li>8. Threat Intelligence Generation</li> <li>9. Threat Intelligence Informed Risk Management</li> <li>10. Integration of Threat Intelligence into SIEM</li> <li>11. Leverage Threat Intelligence for Enhanced Incident Response                             <ol style="list-style-type: none"> <li>11.1 Enhancing Incident Response by Establishing SOPs for Threat Intelligence</li> </ol> </li> <li>12. Organizational Scenarios Using Threat Intelligence</li> <li>13. What Do Organizations and Analysts Expect?</li> <li>14. Common Information Security Organization Structure                             <ol style="list-style-type: none"> <li>14.1 Responsibilities of Cyber Threat Analyst</li> </ol> </li> <li>15. Threat Intelligence Use Cases</li> </ol>	3	

Domains	Sub Domain	Description	Number of Questions	Weightage
	1.3 Overview of Threat Intelligence Lifecycle and Frameworks	<ol style="list-style-type: none"> <li>1. Threat Intelligence Lifecycle</li> <li>2. Role of Threat Analyst in Threat Intelligence Lifecycle</li> <li>3. Threat Intelligence Strategy</li> <li>4. Threat Intelligence Capabilities</li> <li>5. Capabilities to Look for in Threat Intelligence Solution</li> <li>6. Threat Intelligence Maturity Model</li> <li>7. Threat Intelligence Frameworks</li> <li>7.1 Collective Intelligence Framework (CIF)</li> <li>7.2 CrowdStrike Cyber Threat Intelligence Solution</li> <li>7.3 NormShield Threat and Vulnerability Orchestration</li> <li>7.4 MISP - Open-Source Threat Intelligence Platform</li> <li>7.5 TC Complete™</li> <li>7.6 Yeti</li> <li>7.7 ThreatStream</li> <li>8. Additional Threat Intelligence Frameworks</li> </ol>	3	
<b>2. Cyber Threats and Kill Chain Methodology</b>	2.1 Understanding Cyber Threats	<ol style="list-style-type: none"> <li>1. Overview of Cyber Threats</li> <li>2. Cyber Security Threat Categories</li> <li>3. Threat Actors/Profiling the Attacker</li> <li>4. Threat: Intent, Capability, Opportunity Triad</li> <li>5. Motives, Goals, and Objectives of Cyber Security Attacks</li> <li>6. Hacking Forums</li> </ol>	2	18%
	2.2 Understanding Advanced Persistent Threats	<ol style="list-style-type: none"> <li>1. Definition of Advanced Persistent Threats</li> <li>2. Characteristics of Advanced Persistent Threats</li> <li>3. Advanced Persistent Threat Lifecycle</li> </ol>	2	
	2.3 Understanding Cyber Kill Chain	<ol style="list-style-type: none"> <li>1. Cyber Kill Chain Methodology</li> <li>2. Tactics, Techniques, and Procedures</li> <li>3. Adversary Behavioral Identification</li> </ol>	2	

Domains	Sub Domain	Description	Number of Questions	Weightage
		4. Kill Chain Deep Dive Scenario - Spear Phishing		
	2.4 Understanding Indicators of Compromise	<ol style="list-style-type: none"> <li>1. Indicators of Compromise</li> <li>2. Why Indicators of Compromise Important?</li> <li>3. Categories of Indicators of Compromise</li> <li>4. Key Indicators of Compromise</li> <li>5. Pyramid of Pain</li> </ol>	3	
<b>3. Requirements, Planning, Direction, and Review</b>	3.1 Understanding Organization's Current Threat Landscape	<ol style="list-style-type: none"> <li>1. Identify Critical Threats to the Organization</li> <li>2. Assess Organization's Current Security Pressure Posture                             <ol style="list-style-type: none"> <li>2.1 Assess Current Security Team's Structure and Competencies</li> <li>2.2 Understand Organization's Current Security Infrastructure and Operations</li> </ol> </li> <li>3. Assess Risks for Identified Threats</li> </ol>	2	16%
	3.2 Understanding Requirements Analysis	<ol style="list-style-type: none"> <li>1. Map Out Organization's Ideal Target State</li> <li>2. Identify Intelligence Needs and Requirements</li> <li>3. Define Threat Intelligence Requirements                             <ol style="list-style-type: none"> <li>3.1 Threat Intelligence Requirement Categories</li> </ol> </li> <li>4. Business Needs and Requirements                             <ol style="list-style-type: none"> <li>4.1 Business Units, Internal Stakeholders, and Third Parties</li> <li>4.2 Other Teams</li> </ol> </li> <li>5. Intelligence Consumers Needs and Requirements</li> <li>6. Priority Intelligence Requirements</li> <li>7. Factors for Prioritizing Requirements</li> <li>8. MoSCoW Method for Prioritizing Requirements</li> <li>9. Prioritize Organizational Assets</li> <li>10. Scope of the Threat Intelligence Program</li> <li>11. Rules of Engagement</li> </ol>	1	


Domains	Sub Domain	Description	Number of Questions	Weightage
		12. Non-disclosure Agreements 13. Avoid Common Threat Intelligence Pitfalls		
	3.3 Planning a Threat Intelligence Program	1. Prepare People, Processes, and Technology 2. Develop a Collection Plan 3. Schedule a Threat Intelligence Program 4. Plan a Budget 5. Develop a Communication Plan to Update Progress to Stakeholders 6. Aggregate Threat Intelligence 7. Select a Threat Intelligence Platform 8. Consuming Intelligence for Different Goals 9. Track Metrics to Keep Stakeholders Informed	1	
	3.4 Establishing Management Support	1. Prepare Project Charter and Policy to Formalize the Initiative 1.1 Establish Your Case to Management for a Threat Intelligence Program 1.2 Apply a Strategic Lens to the Threat Intelligence Program	1	
	3.5 Building a Threat Intelligence Team	1. Satisfy Organizational Gaps with the Appropriate Threat Intelligence Team 1.1 Understand different Threat Intelligence Roles and Responsibilities 1.2 Identify Core Competencies and Skills 1.3 Define Talent Acquisition Strategy 1.4 Building and Positioning an Intelligence Team 1.5 How to Prepare an Effective Threat Intelligence Team	1	
	3.6 Overview of Threat Intelligence Sharing	1. Establishing Threat Intelligence Sharing Capabilities 2. Considerations for Sharing Threat Intelligence	1	

Domains	Sub Domain	Description	Number of Questions	Weightage
		<ul style="list-style-type: none"> <li>3. Sharing Intelligence with Variety of Organizations</li> <li>4. Types of Sharing Partners</li> <li>5. Important Selection Criteria for Partners</li> <li>6. Sharing Intelligence Securely</li> </ul>		
	3.7 Reviewing Threat Intelligence Program	<ul style="list-style-type: none"> <li>1. Threat Intelligence-Led Engagement Review</li> <li>2. Considerations for Reviewing Threat Intelligence Program</li> <li>3. Assessing the Success and Failure of the Threat Intelligence Program</li> </ul>	1	
<b>4. Data Collection and Processing</b> 	4.1 Overview of Threat Intelligence Data Collection	<ul style="list-style-type: none"> <li>1. Introduction to Threat Intelligence Data Collection</li> <li>2. Data Collection Methods</li> <li>3. Types of Data</li> <li>4. Types of Threat Intelligence Data Collection</li> </ul>	2	16%
	4.2 Overview of Threat Intelligence Collection Management	<ul style="list-style-type: none"> <li>1. Understanding Operational Security for Data Collection</li> <li>2. Understanding Data Reliability</li> <li>3. Ensuring Intelligence Collection Methods Produce Actionable Data</li> <li>4. Validate the Quality and Reliability of Third-Party Intelligence Sources</li> <li>5. Establish Collection Criteria for Prioritization of Intelligence Needs and Requirements</li> <li>6. Building a Threat Intelligence Collection Plan</li> </ul>	1	
	4.3 Overview of Threat Intelligence Feeds and Sources	<ul style="list-style-type: none"> <li>1. Threat Intelligence Feeds</li> <li>2. Threat Intelligence Sources</li> </ul>	1	
	4.4 Understanding Threat Intelligence Data Collection and Acquisition	<ul style="list-style-type: none"> <li>1. Threat Intelligence Data Collection and Acquisition</li> <li>2. Data Collection through Open-Source Intelligence (OSINT)                             <ul style="list-style-type: none"> <li>2.1 Data Collection through Search Engines</li> <li>2.2 Data Collection through Web Services</li> </ul> </li> </ul>	2	

Domains	Sub Domain	Description	Number of Questions	Weightage
		<p>2.3 Data Collection through Website Footprinting</p> <p>2.4 Data Collection through Emails</p> <p>2.5 Data Collection through Whois Lookup</p> <p>2.6 Data Collection through DNS Interrogation</p> <p>2.7 Automating OSINT Effort Using Tools/Frameworks/Scripts</p> <p>3. Data Collection through Human Intelligence (HUMINT)</p> <p>3.1 Data Collection through Human-based Social Engineering Techniques</p> <p>3.2 Data Collection through Interviewing and Interrogation</p> <p>3.3 Social Engineering Tools</p> <p>4 Data Collection through Cyber Counterintelligence (CCI)</p> <p>4.1 Data Collection through Honeypots</p> <p>4.2 Data Collection through Passive DNS Monitoring</p> <p>4.3 Data Collection through Pivoting Off Adversary's Infrastructure</p> <p>4.4 Data Collection through Malware Sinkholes</p> <p>4.5 Data Collection through YARA Rules</p> <p>5. Data Collection through Indicators of Compromise (IoCs)</p> <p>5.1 IoC Data Collection through External Sources</p> <p>5.2 IoC Data Collection through Internal Sources</p> <p>5.3 Tools for IoC Data Collection through Internal Sources</p> <p>5.4 Data Collection through Building Custom IoCs</p> <p>5.5 Tools for Building Custom IoCs</p> <p>5.6 Steps for Effective Usage of Indicators of Compromise (IoCs) for Threat Intelligence</p>		

Domains	Sub Domain	Description	Number of Questions	Weightage
		6. Data Collection through Malware Analysis 6.1 Preparing Testbed for Malware Analysis 6.2 Data Collection through Static Malware Analysis 6.3 Data Collection through Dynamic Malware Analysis 6.4 Malware Analysis Tools 6.5 Tools for Malware Data Collection		
	4.5 Understanding Bulk Data Collection	1. Introduction to Bulk Data Collection 2. Forms of Bulk Data Collection 3. Benefits and Challenges of Bulk Data Collection 4. Bulk Data Management and Integration Tools	1	
	4.6 Understanding Data Processing and Exploitation	1. Threat Intelligence Data Collection and Acquisition 2. Introduction to Data Processing and Exploitation 3. Structuring/Normalization of Collected Data 4. Data Sampling 4.1 Types of Data Sampling 5. Storing and Data Visualization 6. Sharing the Threat Information	1	
<b>5. Data Analysis</b>	5.1 Overview of Data Analysis	1. Introduction to Data Analysis 2. Contextualization of Data 3. Types of Data Analysis	1	16%
	5.2 Understanding Data Analysis Techniques	1. Statistical Data Analysis 1.1 Data Preparation 1.2 Data Classification 1.3 Data Validation 1.4 Data Correlation 1.5 Data Scoring 1.6 Statistical Data Analysis Tools 2. Analysis of Competing Hypotheses 2.1 Hypothesis 2.2 Evidence 2.3 Diagnostics	1	



Domains	Sub Domain	Description	Number of Questions	Weightage
		2.4 Refinement 2.5 Inconsistency 2.6 Sensitivity 2.7 Conclusions and Evaluation 3. ACH Tool 3.1 PARC ACH 4. Structured Analysis of Competing Hypotheses 5. Other Data Analysis Methodologies		
	5.3 Overview of Threat Analysis	1. Introduction to Threat Analysis 2. Types of Threat Intelligence Analysis	1	
	5.4 Understanding the Threat Analysis Process	1. Threat Analysis Process and Responsibilities 2. Threat Analysis Based on Cyber Kill Chain Methodology 3. Aligning the Defensive Strategies with the Phases of the Cyber Kill Chain Methodology 4. Perform Threat Modeling 4.1 Asset Identification 4.2 System Characterization 4.3 System Modeling 4.4 Threat Determination and Identification 4.5 Threat Profiling and Attribution 4.6 Threat Ranking 4.7 Threat Information Documentation 5. Threat Modeling Methodologies 5.1 STRIDE 5.2 PASTA 5.3 TRIKE 5.4 VAST 5.5 DREAD 5.6 OCTAVE 6. Threat Modeling Tools 6.1 Microsoft Threat Modelling Tool 6.2 ThreatModeler 6.3 securiCAD Professional 6.4 IriusRisk	1	

Domains	Sub Domain	Description	Number of Questions	Weightage
		7. Enhance Threat Analysis Process with the Diamond Model Framework 8. Enrich the Indicators with Context 9. Validating and Prioritizing Threat Indicators		
	5.5 Overview of Fine-Tuning Threat Analysis	1. Fine-Tuning Threat Analysis 2. Identifying and Removing Noise 3. Identifying and Removing Logical Fallacies 4. Identifying and Removing Cognitive Biases 5. Automate Threat Analysis Processes 6. Develop Criteria for Threat Analysis Software 7. Employ Advanced Threat Analysis Techniques 7.1 Machine Learning-Based Threat Analysis 7.2 Cognitive-Based Threat Analysis	1	
	5.6 Understanding Threat Intelligence Evaluation	1. Threat Intelligence Evaluation 2. Threat Attribution	1	
	5.7 Creating Runbooks and Knowledge Base	1. Developing Runbooks 2. Create an Accessible Threat Knowledge Base 3. Organize and Store Cyber Threat Information in Knowledge Base	1	
	5.8 Overview of Threat Intelligence Tools	1. Threat Intelligence Tools 1.1 AlienVault® USM® Anywhere 1.2 IBM X-Force Exchange 1.3 ThreatConnect 1.4 SurfWatch Threat Analyst 1.5 AutoFocus 1.6 Additional Threat Intelligence Tools	1	
<b>6. Intelligence Reporting and Dissemination</b>	6.1 Overview of Threat Intelligence Reports	1. Threat Intelligence Reports 2. Types of Cyber Threat Intelligence Reports 2.1 Threat Analysis Reports 2.2 Threat Landscape Reports	1	16%

Domains	Sub Domain	Description	Number of Questions	Weightage
		<ul style="list-style-type: none"> <li>3. Generating Concise Reports</li> <li>4. Threat Intelligence Report Template</li> <li>5. How to Maximize the Return from Threat Intelligence Report</li> <li>6. Continuous Improvement via Feedback Loop</li> <li>7. Report Writing Tools</li> <li>7.1 MagicTree</li> <li>7.2 KeepNote</li> </ul>		
	6.2 Introduction to Dissemination	<ul style="list-style-type: none"> <li>1. Overview of Dissemination</li> <li>2. Preferences for Dissemination</li> <li>3. Benefits of Sharing Intelligence</li> <li>4. Challenges to Intelligence Sharing</li> <li>5. Disseminate Threat Intelligence Internally</li> <li>6. Building Blocks for Threat Intelligence Sharing</li> <li>7. Begin Intelligence Collaboration</li> <li>8. Establish Information Sharing Rules</li> <li>9. Information Sharing Model</li> <li>10. Information Exchange Types</li> <li>11. TI Exchange Architectures</li> <li>12. TI Sharing Quality</li> <li>13. Access Control on Intelligence Sharing</li> <li>14. Intelligence Sharing Best Practices</li> </ul>	1	
	6.3 Participating in Sharing Relationships	<ul style="list-style-type: none"> <li>1. Why Sharing Communities are Formed?</li> <li>2. Join a Sharing Community</li> <li>3. Factors to be Considered When Joining a Community</li> <li>4. Engage in Ongoing Communication</li> <li>5. Consume and Respond to Security Alerts</li> <li>6. Consume and Use Indicators</li> <li>7. Produce and Publish Indicators</li> <li>8. External Intelligence Sharing</li> <li>9. Establishing Trust</li> <li>10. Organizational Trust Models</li> </ul>	1	

Domains	Sub Domain	Description	Number of Questions	Weightage
	6.4 Overview of Sharing Threat Intelligence	<ol style="list-style-type: none"> <li>1. Sharing Strategic Threat Intelligence</li> <li>2. Sharing Tactical Threat Intelligence</li> <li>3. Sharing Operational Threat Intelligence</li> <li>4. Sharing Technical Threat Intelligence</li> <li>5. Sharing Intelligence Using YARA Rules</li> <li>6. IT-ISAC (Information Technology - Information Security and Analysis Center)</li> </ol>	1	
	6.5 Overview of Delivery Mechanisms	<ol style="list-style-type: none"> <li>1. Forms of Delivery</li> <li>2. Machine-Readable Threat Intelligence</li> <li>3. Standards and Formats for Sharing Threat Intelligence                             <ol style="list-style-type: none"> <li>3.1 Traffic Light Protocol (TLP)</li> <li>3.2 MITRE Standards</li> <li>3.3 Managed Incident Lightweight Exchange (MILE)</li> <li>3.4 VERIS</li> <li>3.5 IDMEF</li> </ol> </li> </ol>	1	
	6.6 Understanding Threat Intelligence Sharing Platforms	<ol style="list-style-type: none"> <li>1. Information Sharing and Collaboration Platforms                             <ol style="list-style-type: none"> <li>1.1 Blueliv Threat Exchange Network</li> <li>1.2 Anomali STAXX</li> <li>1.3 MISP (Malware Information Sharing Platform)</li> <li>1.4 Cyware Threat Intelligence eXchange (CTIX)</li> <li>1.5 Soltra Edge</li> <li>1.6 Information Sharing and Collaboration Platforms</li> </ol> </li> </ol>	1	
	6.7 Overview of Intelligence Sharing Acts and Regulations	<ol style="list-style-type: none"> <li>1. Cyber Intelligence Sharing and Protection Act (CISPA)</li> <li>2. Cybersecurity Information Sharing Act (CISA)</li> </ol>	1	
	6.8 Overview of Threat Intelligence Integration	<ol style="list-style-type: none"> <li>1. Integrating Threat Intelligence</li> <li>2. How to Integrate CTI into the Environment</li> </ol>	1	

Domains	Sub Domain	Description	Number of Questions	Weightage
		3. Acting on the Gathered Intelligence 4. Tactical Intelligence Supports IT Operations: Blocking, Patching, and Triage 5. Operational Intelligence Supports Incident Response: Fast Reaction and Remediation 6. Strategic Intelligence Supports Management: Strategic Investment and Communications		