EDUSUM

#1 Online Certification Guide

CREST CRTIA

CREST Registered Threat Intelligence Analyst Certification Questions & Answers

Exam Summary – Syllabus –Questions

CRTIA

CREST Registered Threat Intelligence Analyst (CRTIA)

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

Table of Contents:

Know Your CRTIA Certification Well:

The CRTIA is best suitable for candidates who want to gain knowledge in the CREST Threat Intelligence. Before you start your CRTIA preparation you may struggle to get all the crucial Registered Threat Intelligence Analyst materials like CRTIA syllabus, sample questions, study guide.

But don't worry the CRTIA 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 CRTIA syllabus?
- How many questions are there in the CRTIA exam?
- Which Practice test would help me to pass the CRTIA exam at the first attempt?

Passing the CRTIA exam makes you CREST Registered Threat Intelligence Analyst (CRTIA). Having the Registered Threat Intelligence Analyst certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

CREST CRTIA Registered Threat Intelligence Analyst Certification Details:

Exam Name	CREST Registered Threat Intelligence Analyst (CRTIA)
Exam Code	CRTIA
Exam Price	$400 (USD)
Duration	120 mins
Number of Questions	120
Passing Score	70%
Schedule Exam	Pearson VUE
Sample Questions	CREST Registered Threat Intelligence Analyst Sample Questions
Practice Exam	**CREST CRTIA Certification Practice Exam**

CRTIA Syllabus:

Topic	Details
Appendix A – Key Concepts	
Business imperative	- Background and reasons for intelligence-led security testing - Understanding of the range of scenarios in which threat intelligence can be used within an organisation.
Terminology	- Knowledge of common terms relating to threat intelligence, business risk and information security.
Threat actors & attribution	- Knowledge of common attackers (e.g. hacktivists, criminals, nation states) and their motivation and intent. - The benefits of associating activity with real people, places or organisations.
Attack methodology	- Knowledge regarding phases of the cyber 'kill chain' methodology. - Knowledge of common tactics, techniques and procedures (TTPs). - Understanding of, and familiarity with the Mitre ATT&CK framework - Sequences of tool application, behavioural identification/observed behaviour.
Analysis methodology	- Understanding of typical methodologies used to analyse collected intelligence and their application. - Knowledge of methods for analysis of threat, e.g. the diamond model. - Analysis of competing hypotheses (ACH), Intelligence Preparation of the Environment / Battlefield (IPB / IPE). - Familiarity with concepts and terminology concerning forecasting and predictive methodologies.
Process and intelligence lifecycle	- Ability to plan and execute an intelligence-led engagement start to finish, including providing direction to junior staff and managing the client. - Understanding of the intelligence lifecycle (and variations of if including F3EAD) and how it relates to conducting a client engagement.
Principles of Intelligence	- Understanding of the principles of intelligence and their application in Cyber Threat Intelligence context.
Appendix B - Direction and Review	
Requirements analysis (scoping)	- Analysing a intelligence customer's position to understand requirements. Scoping projects to achieve key outcomes relevant to the client's organisation. - Accurate timescale scoping and resource planning. - Establishing rules of engagement, limitations and constraints.

Topic	Details
Intelligence planning	- Prioritising intelligence requirements (e.g. MoSCoW). - Basic mapping of how a customer will consume and apply threat intelligence.
Project review	- Conducting a review after an intelligence-led engagement, assessing the successes and failures in conjunction with the customer.
Appendix C – Data Collection	
Collection planning	- Knowledge of building a collection plan that is efficient, agile, robust and appropriate.
Data sources and acquisition	- Understanding of various intelligence sources and their relevance to an engagement e.g. OSINT, HUMINT, SIGINT. - Knowledge of legal frameworks relevant to collecting data from technical and human sources.
Data reliability	- Understanding of how to assess the relevance of intelligence sources. - Knowledge of factors which affect the credibility of an intelligence source and how to rate specific intelligence sources for reliability. - Understanding of the key differences between deception, disinformation and misinformation. - Understanding of how methods used in data collection can affect the availability or freshness of data.
Registration records	- Knowledge of the information contained within IP and domain registries (WHOIS).
Domain Name Server (DNS)	- Knowledge of DNS queries and responses, zone transfers and common record types. - Awareness of dynamic DNS providers and the concepts of fast-flux DNS
Web enumeration and social media	- Effective use of search engines and other open source intelligence sources to gain information about a target. - Knowledge of information that can be retrieved from common social networking sites and how these platforms are used by threat actors.
Document metadata	- Awareness of metadata contained within common document formats, such as author, application versions, machine names, printer and operating system information.
Dump site scraping	- Knowledge of online services commonly used to leak stolen data and how these have been used historically to share sensitive data.
Operational security	- Understanding of how to securely conduct collection operations online, implementing robust procedures to protect the safety and anonymity of individuals. - Knowledge of how to establish identities for data collection, for example operating alias accounts for monitoring online activity.

Topic	Details
Bulk data collection	- Knowledge of how to collect data in bulk, such as from social media, Passive DNS or online feeds of malware. - Explain the benefits and challenges arising from collecting such data in bulk.
Handling human sources	- Knowledge of interviewing techniques and tactics involved in cultivation of human sources. - Awareness of specific legal and reliability issues relating to human sources.
Appendix D – Data Analysis	
Contextualisation	- Understanding of the environment surrounding data and data sources, for example political, economic, social and technological contexts.
Analysis methodologies	- Ability to sort and filter data. - Ability to use standard qualitative and quantitative analysis methodologies to process data and generate intelligence product. - Awareness of social network analysis and behavioural profiling techniques. - Awareness of threat modelling and techniques such as attack trees.
Machine based techniques	- Awareness of structured and unstructured data analysis techniques. - Awareness of machine learning techniques, for example supervised and unsupervised learning.
Statistics	- Knowledge of fundamental statistical methods used during data analysis, including averages, standard deviation, statistical distributions and techniques for data correlation, for example: • Time-series analysis • Graphing techniques • Charting techniques • Confidence levels
Critique	- Critical analysis of collected data, ensuring that all potential hypotheses are explored and evaluated. - Ability to identify fake or conflicting data, for example misinformation. - Understanding of prediction and forecasting and the differences between secrets and mysteries. - Awareness of the importance of identifying and removing bias should this occur as an artefact of collection methods or analysis techniques.
Consistency	- Ability to achieve consistency in analysis outputs and intelligence products throughout multiple engagements for a single customer or across industry sectors.

Topic	Details
Appendix E – Product Dissemination	
Forms of delivery	- Understanding of effective delivery mechanisms that meet customer requirements, ranging from simple alerts to tailored reports. - Knowledge of why machine-readable data formats are important for efficient intelligence sharing and awareness of common vendor or community sponsored file formats.
Technical data sharing	- Knowledge of what constitutes useful technical defensive intelligence, for example different types of host and network based indicators. - Knowledge of common formats for distributing indicators of compromise to collaboration partners and ability to interpret these.
Intelligence sharing initiatives	- Knowledge of intelligence sharing initiatives and their relevance to individual clients.
Intelligence handling and classification	- Knowledge of formal data classification or handling policies. - Understanding of why and how to establish secure mechanisms for delivery and sharing of intelligence with clients (for example the use of data encryption and strong authentication).
Appendix F – Management	
Client management & communications	- Knowledge sharing, daily checkpoints and defining escalation paths for encountered problems. - Knowledge and practical use of secure out-of-band communication channels. - Regular updates of progress to necessary stakeholders.
Project management	- Ability to manage a team of threat intelligence analysts providing services to customers. - Knowledge of the full engagement lifecycle including scoping, authorisation, non-disclosure agreements and review. - Ability to make decisions using sound judgement and critical reasoning.
Reporting	- Ability to compile concise reporting with clear explanation of limitations, caveats and assumptions. - Ability to concisely communicate technical data and attack techniques in a coherent narrative that addresses the intelligence needs of the consumer. - Knowledge of methods for organising and presenting complicated links between related intelligence in a variety of graphical forms.
Understanding, explaining and managing risk	- Knowledge of the additional risks that threat led engagements pose. - Communication and explanation of the risks relating to intelligence collection. Effective planning for potential problems during later

Topic	Details
	phases of an engagement. - Awareness of relevant risk management standards, for example: • Risk Management ISO 31000 • Information Security ISO 27001 • Business Continuity ISO 22301 • Risk Assessment ISO 27005
Third Parties	- Ability to deal with external third parties in a professional and knowledgeable manner to facilitate threat led engagements. - Knowledge of public organisations, Government departments and regulatory bodies relevant to specific clients and their role in overseeing industry sectors.
Regulator Mandated TI schemes	- Basic understanding of the range of regulator mandated, intelligence led, penetration testing schemes, their format and requirements.
Appendix G - Legal and Ethical	
Law & Compliance	- Knowledge of pertinent UK legal issues: • Computer Misuse Act 1990 • Human Rights Act 1998 • Data Protection Act 1998 • Police and Justice Act 2006 • Official Secrets Act 1989 • Telecommunications (Lawful Business Practice) (Interception of Communications) 2000 • Regulation of Investigatory Powers Act 2000 • Bribery Act 2010 • Proceeds of Crime Act 2002 - Awareness of relevant laws concerning employment rights, copyright and intellectual property. - Awareness of relevant international legislation and the complexities of working with multi-national organisations. - Understanding of how and when to interact with law enforcement during an engagement. - Knowledge of what written authority is necessary to comply with local laws.
Ethics	- Awareness of the strong ethical requirements needed when providing accurate threat intelligence. - Understanding of the CREST Code of Conduct and the responsibilities it places on individuals and companies.
Appendix H - Technical Cyber Security	
IP Protocols	- IP protocols: IPv4 and IPv6, TCP, UDP and ICMP. - VPN Protocols (e.g. PPTP). - Awareness that other IP protocols exist.

Topic	Details
	- Knowledge of how these protocols are used by adversaries when conducting a attacks ways in which analysis can assist in the assessment of adversary capability, sophistication and lead to attribution to a specific threat actor.
Cryptography	- Fundamental understanding of cryptography, including the differences between encryption and encoding, symmetric and asymmetric encryption, common algorithms.
Vulnerabilities	- Knowledge of common vulnerabilities used in the exploitation of popular desktop, web servers and mobile devices, particularly those for which robust exploit code exists in the public domain. - Awareness of zero-day exploits and how these are used by adversaries. - Ability to characterise a threat using vulnerability information and suggest mitigations for common vulnerability classes.
Intrusion Vectors	- Knowledge of the different vectors by which threat actors attempt to compromise a network, for example spear phishing, strategic web compromise / watering holes / drive-by downloads. - Awareness of common definitions of attack patterns and related vulnerabilities (e.g. CAPEC, OWASP) - Awareness of advanced techniques used by some well-funded threat actors which may not be detected by common IDS platforms.
Command & Control and Exfiltration Techniques	- Knowledge of common malware control mechanisms and corresponding detection techniques. - Knowledge of the various protocols and techniques that can be used for egressing data from a network, facilitated by malware or standard operating system / network tools.
Attack Attribution	- Knowledge of techniques that can be used to hide the source of an attack, for example use of VPNs, proxy servers or Tor. - Understanding of difficulties associated with attribution and how technical analysis of malware and related datasets can be used to provide demonstrable links between an attack and a threat actor.
Current threat landscape	- A working knowledge of some threat actors, their objectives, and associated campaigns. - An understanding of how the threat landscape is changing, and factors which are likely to influence future changes.

CREST CRTIA Sample Questions:

Question: 1

What characteristics make asymmetric encryption suitable for public key infrastructure (PKI)?

a) Key pair system supporting confidentiality and digital signatures
b) Real-time symmetric key rotation
c) Supports same-key decryption only
d) Scalability in secure key distribution

Answer: a, d

Question: 2

A business seeks to understand "why threat attribution is valuable." What is the most appropriate reason?

a) Attribution allows automatic malware deletion
b) Attribution helps link campaigns to known threat actors and predict future actions
c) Attribution improves firewall performance
d) Attribution ensures full legal prosecution

Answer: b

Question: 3

Under the Bribery Act 2010, which of the following would most likely constitute an offence?

a) Giving cash to a public official to gain access to restricted cyber data
b) Offering a client a compliance report
c) Publishing redacted threat reports
d) Forwarding malware samples to the SOC

Answer: a

Question: 4

The _____ process focuses on comparing outcomes with original requirements and identifying lessons learned for continuous improvement.

a) scoping
b) delivery
c) dissemination
d) project review

Answer: d

Question: 5

How does the Intelligence Preparation of the Environment (IPE) method assist analysts?

a) It prepares forecasting based on geopolitical, technical, and organizational context
b) It enables malware reverse engineering
c) It performs IP blacklisting
d) It filters out DNS artifacts

Answer: a

Question: 6

To ensure confidentiality, analysts often rely on _____ channels for sensitive communication with clients.

a) shared Slack channels
b) unprotected FTP sites
c) public social media
d) out-of-band secure

Answer: d

Question: 7

During a live threat engagement, what step should be taken if an analyst detects indicators of a breach outside the defined scope?

a) Immediately notify a regulatory body
b) Halt all operations and erase findings
c) Escalate to the engagement manager and follow defined escalation paths
d) Ignore the indicators until the review phase

Answer: c

Question: 8

Which of these is designed as a machine-readable format for storing cyber threat intelligence?

a) CSV
b) STIX
c) APT
d) UBER
e) ElasticSearch

Answer: b

Question: 9

When performing ACH (Analysis of Competing Hypotheses), what is the most critical activity?

a) Creating threat actor personas
b) Classifying indicators of compromise
c) Comparing evidence against multiple explanations
d) Listing all known vulnerabilities

Answer: c

Question: 10

In a threat intelligence context, the framework known as _____ focuses on risk management principles and guidelines.

a) ISO 27005
b) ISO 31000
c) GDPR
d) OWASP

Answer: b

Study Guide to Crack CREST Registered Threat Intelligence Analyst CRTIA Exam:

- Getting details of the CRTIA syllabus, is the first step of a study plan. This pdf is going to be of ultimate help. Completion of the syllabus is must to pass the CRTIA exam.
- Making a schedule is vital. A structured method of preparation leads to success. A candidate must plan his schedule and follow it rigorously to attain success.
- Joining the CREST provided training for CRTIA 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 CRTIA 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 CRTIA practice tests is must. Continuous practice will make you an expert in all syllabus areas.