Assessors Panel

CREST Registered Threat Intelligence Analyst Syllabus

Issued by	CREST Assessors Panel
Document Reference	CRTIA-SYLLABUS
Version Number	2.1
Status	Published
Issue Date	2 December 2019
Review Date	

Table of Contents

Version History

Version	Date	Authors & notes	Status
0.1	3rd October 2016	First draft	Internal
0.2	1st June 2017	QA and revisions	Internal
1.0	1st June 2017	First release	Public
1.1	12th March 2019	Refreshed in light of changes to exam	Internal
1.2	13th March 2019	Content review	Internal
2.0	18th March 2019	Final	Published
2.1	2 December 2019	Updated column headings	Published

Document Review

Reviewer	Position
Chair	Technical Committee / Assessors Panel
Chair	CREST Board
Operations Manager	CREST Executive

1 Introduction

1.1 Terms of reference

The technical syllabus identifies at a high level the technical skills and knowledge that CREST expects candidates to possess for the Threat Intelligence Analyst Certification. The exam covers a common set of core skills and knowledge as well as more specific role related areas.

Success at the CREST Registered Threat Intelligence Analyst (CRTIA) examination will confer CREST Registered status to the individual.

1.2 Role definition

A Threat Intelligence Analyst (TIA) is a role responsible for the collection, processing and analysis of data, information and intelligence in order to generate threat intelligence outputs. Analysts are expected to be familiar with both contextual analysis (focussing on social, cultural and geopolitical elements) and technical analysis (analysis of data relating to Indicators of Compromise) and the exam covers both disciplines. Candidates are also expected to understand the legal and ethical frameworks governing threat intelligence work.

A TIA may have a background in information security or may come from the private security, police, military or intelligence communities.

1.3 CREST Registered Threat Intelligence Analyst (CRTIA)

The (CRTIA) examination tests candidates' knowledge and expertise in collecting and analysing information in support of threat intelligence objectives.

The candidate is expected to have a good breadth of knowledge in all areas of threat intelligence and proven experience in conducting collection and analysis activities.

The exam will assess the candidate's understanding of the key phases of intelligence generation, cyber specific information sources and common approaches to collection and analysis. The aim is to demonstrate a high level of competence in the collection, analysis and dissemination of intelligence to a consistently high standard and in accordance with legal and ethical guidelines.

2 Certification Examination Structure

2.1 CREST Registered Threat Intelligence Analyst (CR TIA)

The CRTIA Examination has two components: a multiple-choice written question section and two long-form questions.

The Notes for Candidates (NFC) document provides further information regarding the Certification Examinations in general and the specific skill areas that will be assessed.

3 Syllabus Structure

The syllabus is divided into knowledge groups (Appendices A to F below), each of which is subdivided into specific skill areas.

4 Appendix A – Key Concepts

The key concepts underlying intelligence-led cyber threat assessments.

ID	Skill	Details	CRTIA
A1	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.	MC LF
A2	Terminology	Knowledge of common terms relating to threat intelligence, business risk and information security.	MC
A3	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.	MC LF
A4	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.	MC LF
A5	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.	MC LF

A6	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.	LF
A7	Principles of Intelligence	Understanding of the principles of intelligence and their application in Cyber Threat Intelligence context.	LF

5 Appendix B - Direction and Review

Conducting engagements that encompass the entire intelligence lifecycle, from gathering customer requirements to reviewing outcomes.

ID	Skill	Details	CRTIA
B1	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.	MC LF
B2	Intelligence planning	Prioritising intelligence requirements (e.g. MoSCoW). Basic mapping of how a customer will consume and apply threat intelligence.	MC LF
B3	Project review	Conducting a review after an intelligence-led engagement, assessing the successes and failures in conjunction with the customer.	LF

6 Appendix C – Data Collection

Collection of data relevant to a customer's intelligence requirements and turning it into a format suitable for analysis.

ID	Skill	Details	CRTIA
C1	Collection planning	Knowledge of building a collection plan that is efficient, agile, robust and appropriate.	LF
C2	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.	MC LF
C3	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.	MC LF
C4	Registration records	Knowledge of the information contained within IP and domain registries (WHOIS).	MC
C5	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	MC
C6	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.	MC LF
C7	Document metadata	Awareness of metadata contained within common document formats, such as author, application versions, machine names, printer and operating system information.	MC
C8	Dump site scraping	Knowledge of online services commonly used to leak stolen data and how these have been used historically to share sensitive data.	MC
C9	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.	MC LF

C10	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.	MC LF
C11	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.	MC LF

7 Appendix D – Data Analysis

Using structured techniques and methods to address customer requirements by analysis of collected data.

ID	Skill	Details	CRTIA
D1	Contextualisation	Understanding of the environment surrounding data and data sources, for example political, economic, social and technological contexts.	MC LF
D2	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.	MC LF
D3	Machine based techniques	Awareness of structured and unstructured data analysis techniques. Awareness of machine learning techniques, for example supervised and unsupervised learning.	MC
D4	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	MC
D5	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.	MC LF
D6	Consistency	Ability to achieve consistency in analysis outputs and intelligence products throughout multiple engagements for a single customer or across industry sectors.	LF

8 Appendix E – Product Dissemination

Methods for disseminating intelligence product to consumers and for sharing intelligence with trusted members of the wider intelligence community.

ID	Skill	Details	CRTIA
E1	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.	MC LF
E2	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.	MC LF
E3	Intelligence sharing initiatives	Knowledge of intelligence sharing initiatives and their relevance to individual clients.	LF
E4	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).	MC LF

9 Appendix F – Management

General management of operations, projects and quality.

ID	Skill	Details	CRTIA
F1	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.	MC LF
F2	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.	MC LF
F3	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.	LF
F4	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 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	MC LF

F5	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.	MC LF
F6	Regulator Mandated TI schemes	Basic understanding of the range of regulator mandated, intelligence led, penetration testing schemes, their format and requirements.	MC LF

10 Appendix G - Legal and Ethical

Legal and ethical considerations arising from conducting intelligence-led engagements.

ID	Skill	Details	CRTIA
G1	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.	MC LF
G2	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.	MC LF

11 Appendix H - Technical Cyber Security

Fundamental technical concepts, attack methods and countermeasures.

ID	Skill	Details	CRTIA
H1	IP Protocols	IP protocols: IPv4 and IPv6, TCP, UDP and ICMP. VPN Protocols (e.g. PPTP). Awareness that other IP protocols exist. 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.	MC
H2	Cryptography	Fundamental understanding of cryptography, including the differences between encryption and encoding, symmetric and asymmetric encryption, common algorithms.	MC
H3	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.	MC
H4	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.	MC LF
H5	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.	MC

H6	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.	MC LF
H7	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.	LF