CREST. Representing the technical information security industry

Assessors Panel

CREST Threat Intelligence Manager Syllabus

Contents

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 Manager Certification. The exam covers a common set of core skills and knowledge as well as more specific role related areas

Success at the CREST Certified Threat Intelligence Manager (CCTIM) examination will confer CREST Certified status to the individual.

1.2. Role definition

A Threat Intelligence Manager (TIM) is a senior role responsible for managing a multi-disciplinary team in the production of threat intelligence for end-users. The team managed by the TIM divides into two broad sub-roles:

- Cyber Intelligence Contextual Analyst: performs core intelligence tasks focussing on social, cultural and geopolitical analysis, with generalists synthesising disparate research and specialists applying a deep understanding of particular domains, applies these skills to the topic of attack performed by electronic means and understands the methodology and trade craft of producing accurate intelligence.
- Cyber Intelligence Technical Analyst: performs a broad range of tasks ranging from malware reverse engineering (analysing malicious code samples and monitoring their behaviour inside a controlled environment) to technical security engineering (developing collection and analysis tools, analysing network traffic and undertaking vulnerability research).

Because of these two entry points into the TIM role, the TIM should therefore be knowledgeable in both disciplines. A TIM may have a background in information security or may come from the private security, police, military or intelligence communities.

1.3. CREST Certified Threat Intelligence Manager (CCTIM)

The (CCTIM) examination tests candidates' knowledge and expertise in leading a team that specialises in the production of threat intelligence. The candidate is expected to have a good breadth of knowledge in all areas of threat intelligence and proven experience in managing a team of threat intelligence analysts from across a variety of disciplines. The exam will assess the candidate's ability to produce threat intelligence in a realistic, legal and safe manner with appropriate supporting evidence. The aim is to provide the customer with actionable threat intelligence relating to organisational risks to the customer's staff, data and systems.

2. Certification Examination Structure

2.1. CREST Certified Threat Intelligence Manager (CCTIM)

The CCTIM Examination is a purely written exam consisting of three sections:

- a set of short-form questions (requiring a single word or short sentence answer);
- a selection of long form questions (requiring longer, more in-depth written answers); and finally
- a section that based around a scenario (requiring the evaluation and assessment of intelligence material).

The scenario questions are designed to assess the candidate's practical experience in leading a team of threat analysts to produce actionable real-world intelligence.

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

3. Syllabus Structure

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

For each skill area, CREST has indicated where and how the area will be assessed: in which Certification Examination and in which component (Written Multiple Choice, Written Long Form or Scenario).

Within the tables, the following acronyms apply:

CCTIM	CREST Certified Threat Intelligence Manager
SF	Written Short Form
LF	Written Long Form
SC	Written Scenario Question

4. Appendix A - Key Concepts

The key concepts underlying intelligence-led cyber threat assessments.

ID	Skill	Details	CCTIM
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.	SF LF SC
A2	Terminology	Knowledge of common terms relating to threat intelligence, business risk and information security.	SF
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.	SF LF SC
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.	SF LF SC
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.	SF LF SC
A6	Process and intelligence lifecycle	Ability to plan and execute an intelligence-led engagement start to finish, including providing direction to 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 SC
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	CCTIM
B1	Requirements analysis (scoping)	Analysing a 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.	SF LF SC
B2	Intelligence planning	Prioritising intelligence requirements (e.g. MoSCoW). Basic mapping of how a customer will consume and apply threat intelligence.	SF LF SC
B3	Project review	Conducting a review after an intelligence-led engagement, assessing the successes and failures in conjunction with the customer.	LF SC

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	CCTIM
C1	Collection planning	Knowledge of building a collection plan that is efficient, agile, robust and appropriate.	LF SC
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.	SF LF SC
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.	SF LF SC
C4	Registration records	Knowledge of the information contained within IP and domain registries (WHOIS).	SF
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	SF
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.	SF LF SC
C7	Document metadata	Awareness of metadata contained within common document formats, such as author, application versions, machine names, printer and operating system information.	SF
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.	SF

ID	Skill	Details	CCTIM
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.	SF LF SC
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.	SF LF SC
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.	SF LF

7. Appendix D – Data Analysis

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

ID	Skill	Details	CCTIM
D1	Contextualisation	Understanding of the environment surrounding data and data sources, for example political, economic, social and technological contexts.	SF LF SC
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.	SF LF SC
D3	Machine based techniques	Awareness of structured and unstructured data analysis techniques. Awareness of machine learning techniques, for example supervised and unsupervised learning.	SF
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	SF
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.	SF LF SC

ID	Skill	Details	CCTIM
D6	Consistency	Ability to achieve consistency in analysis outputs and intelligence products throughout multiple engagements for a single customer or across industry sectors.	LF SC

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	CCTIM
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.	SF LF SC
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.	SF LF SC
E3	Intelligence sharing initiatives	Knowledge of intelligence sharing initiatives and their relevance to individual clients.	LF SC
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).	SF LF SC

9. Appendix F – Management

General management of operations, projects and quality.

ID	Skill	Details	CCTIM
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.	SF LF SC
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.	SF LF SC
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 SC
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	SF LF SC

ID	Skill	Details	CCTIM
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.	SF LF SC
F6	Regulator Mandated TI schemes	Basic understanding of the range of regulator mandated, intelligence led, penetration testing schemes, their format and requirements.	SF LF SC

10. Appendix G - Legal and Ethical

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

ID	Skill	Details	CCTIM
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.	SF LF SC
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.	SF LF SC

11. Appendix H - Technical Cyber Security

Fundamental technical concepts, attack methods and countermeasures.

ID	Skill	Details	CCTIM
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.	SF
H2	Cryptography	Fundamental understanding of cryptography, including the differences between encryption and encoding, symmetric and asymmetric encryption, common algorithms.	SF
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.	SF
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.	SF LF SC
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.	SF

ID	Skill	Details	CCTIM
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.	**SF** **LF** **SC**
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

.

Telephone: +44 (0)20 3058 3122

General enquiries: info@crest-approved.org

Membership: newmembers@crest-approved.org

Examinations: exambookings@crest-approved.org

Press / Public Relations: media@crest-approved.org