CREST. Representing the technical information security industry

Assessors Panel

CREST Practitioner Threat Intelligence Analyst 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 Practitioner 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 Practitioner Threat Intelligence Analyst (CPTIA) examination will confer CREST Practitioner status to the individual.

1.2. Role definition

A Practitioner Threat Intelligence Analyst (PTIA) is a role responsible for the collection 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 PTIA may be a comparatively junior member of a threat intelligence team, working under the direction of more senior colleagues (CRTIA, CCTIM qualified personnel).

1.3. CREST Practitioner Threat Intelligence Analyst (CP TIA)

The (CTPIA) examination tests candidates' theoretical knowledge 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 demonstrable understanding of 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 Practitioner Threat Intelligence Analyst (CPTIA)

The CPTIA Examination is a purely multiple-choice based exam.

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
A1	Objectives of Threat Intelligence	Understand the key reasons why an organisation would want TI and how they would use it.
A2	Terminology	Demonstrate familiarity with commonly used terms relating to TI and intelligence processes.
A3	Threat Actor Types / Definitions	Be able to distinguish between different threat actors and their likely objectives.
A4	Threat Vector & Vulnerability Types	Understand the definition of a threat vector, and demonstrate knowledge of key threat vectors. Understand the definition of a vulnerability and demonstrate knowledge of common vulnerability types.
A5	The Intelligence Cycle	Be able to name the stages of the cycle, and explain the key processes that occur at each stage.
A6	Analytic Models	Know the components of the Diamond Model, and understand the relationship between them. Be aware of the meta-features of the model and be able to interpret them.
A7	Attack Lifecycle	Understand the lifecycle of a typical attack, for example using a model such as the “Cyber Kill Chain”.
A8	Understanding Risk	Demonstrate an understanding of the relationship between threat, capability, intent, and motivation.

5. Appendix B – Direction and Review

Understanding how the direction and review processes influence the analyst's workflow.

ID	Skill	Details
B1	Developing Terms of Reference	Be able to list the elements included in a typical Terms of Reference. Know why Terms of Reference are important to have before beginning a job.
B2	Importance of Project Review	Be aware of the criteria used to assess intelligence output (for example Timeliness / Accuracy / Presentation / Answering the IR etc.). Understand why it is important to seek feedback on outputs.
B3	Dealing with Intelligence Gaps	Know what an intelligence gap is, and how to identify one. Be able to identify likely sources of information to fill an intelligence gap.

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
C1	Function & Use of a Collection Plan	Know the key component parts of a collection plan and be able to interpret it effectively.
C2	Use of a Collection Worksheet	Understand the benefit / necessity of recording collection activity. Know what information a collection worksheet should contain (for example what sources were checked, what search terms were used, when, etc.)
C3	Types of Sources	Understand different types of source and their broad classifications (HUMINT, OSINT, etc.).
C4	Source Reliability and Grading	The ability to interpret source reliability grading / information reliability grading (based on the UK 5x5x5 model).
C5	Specific Sources	Know what information can be obtained from typical technical sources such as WHOIS, DNS, malware analysis, social media, document metadata etc. Understand the format of data and be able to interpret it accurately.
C6	Boolean Search Strings	Ability to combine Boolean operators to form a precise search, as used by many search engines and proprietary products.
C7	Basic Source Analysis	Understand reasons why some online sources are likely to be biased / inaccurate.
C8	Operational Security (OPSEC)	Understand requirement for OPSEC and potential implications of failure. Knowledge of anonymization tools such as Tor and i2p. Understand the requirement to separate personal web use from work collection. Know the appropriate course of action in the event of an OPSEC breach.

7. Appendix D – Data Analysis

Understanding common approaches to analysis and potential pitfalls.

ID	Skill	Details
D1	Hypothesis Testing	Ability to outline steps required to prove / disprove a hypothesis.
D2	Facts, Assumptions, Premises & Inferences	Distinguish between facts and assumptions. Make a logical inference from available premises. Understand the requirement to identify assumptions and assessments as different from fact.
D3	Expressing Likelihood / Certainty	Understand applicability of terms such as ‘possible’, ‘likely’ and ‘highly likely’.
D4	Circular Reporting	Know what circular reporting is, and suggest ways in which it can be avoided. Understand the importance of managing sources effectively to prevent this occurring.
D5	Cognitive Biases	Identify some of the major types of bias that can affect intelligence analysis. Know common ways in which analysts attempt to counter common biases.
D6	Analytical Techniques	Be able to interpret data in graphical format, for example: • A network diagram • A timeline • A histogram • A scatterplot • A time series graph

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
E1	Structured / Machine Readable TI	Knowledge of STIX, CYBOX and TAXII and how they relate to each other. Knowledge of the content and format of different types of STIX message. Understanding of the advantages / disadvantages of machine readable TI.
E2	Unstructured / Human Readable TI	Understanding of the key advantages / disadvantages of spoken and written dissemination. Ability to select an appropriate dissemination mechanism, for example written product vs. verbal briefings. Understanding of importance of accuracy, brevity, clarity.
E3	Intelligence Sharing	Understanding of ‘Need to Know’ and ‘Need to Share’ concepts. Ability to identify information that can / cannot be shared publicly. Knowledge of common intelligence sharing initiatives.

9. Appendix F – Legal and Ethical

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

ID	Skill	Details
F1	Understanding Requirement for Adherence to Legal / Ethical Standards	Identify examples of illegal and unethical behaviour. Demonstrate understanding of repercussions of illegal / unethical behaviour.
F2	Handling of Classified Material	Understand GPMS classifications and their meanings. Understand the implications of breaching GPMS. Demonstrate the correct course of action in the event of a breach of GPMS handling.
F3	Key Legislation Pertaining to Intelligence Collection in the UK	Demonstrate working understanding of the constraints on intelligence collection operations imposed by: • 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
F4	Dealing With Legal / Ethical Uncertainty.	Know appropriate action if given a task of questionable legality / ethics.
F5	CREST Code of Conduct	Demonstrate understanding of code as it applies to the individual.

.

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