Assessors Panel

CREST Certified Threat Intelligence Manager Examination

Notes for Candidates

Issued by	CREST Assessors Panel
Document Reference	CCTIM-NFC
Version Number	3.5
Status	Published
Issue Date	31 March 2020

Table of Contents

1 Introduction 4

1.1 Examination 4

1.2 Confidentiality 4

2 Examination Details 5

2.1 Short Form Questions (TIM 1) 5

2.2 Long Form Questions (TIM 1) 5

2.3 Long Form & Scenario Questions (TIM 2) 5

2.4 Timings 5

2.5 Open Book / Closed Book 6

2.6 Invigilation 6

3 Marking Scheme / Pass Mark 6

4 Recommended Reading 7

5 Examination Logistics 9

5.1 Location and Timing 9

5.2 Communication of Results 9

6 Example Question 10

Version History

Version	Date	Authors	Status
0.1	2nd March 2015	Technical Committee and Assessors Panel	Internal Release
1.0	2nd March 2015	Technical Committee and Assessors Panel	Public Release
1.1	14th April 2015	Technical Committee and Assessors Panel	Public Release
2.0	11th May 2015	Technical Committee and Assessors Panel	Public Release
2.1	16th June 2015	Technical Committee and Assessors Panel	Public Release
2.2	3rd April 2017	Technical Committee and Assessors Panel	Public Release
2.3	16th February 2019	CTIPs Committee	Internal
2.4	14th March 2019	Quality Review	Internal
3.0	18th March 2019	Final	Published
3.1	24 May 2019	Final (updated TIM2 response numbers)	Published
3.2	5 June 2019	Final (updated with max. period between parts 1&2)	Published
3.3	20 Sept. 2019	CCTIM2 longform correction	Published
3.4	8 Nov 2019	Short Form sample question	Published
3.5	31 Mar. 2020	Updated marking section	Published

Document Review

Reviewer	Position
Chair	
Chair	
Ops Manager	

1 INTRODUCTION

1.1 Examination

The CREST Certified Threat Intelligence Manager (CCTIM) has three components:

- short form questions;
- long form questions; and
- a scenario-based element.

The examination is delivered in two parts at a Pearson Vue Centre.

Success at the Certification Examination will confer upon candidates the status of CREST Certified Threat Intelligence Manager

The CREST Certification qualification is valid for three (3) years.

It should be noted that this exam does not confer any status under the NCSC CHECK scheme and is not recognised for the purposes of equivalency with any other schemes.

1.2 Confidentiality

CREST takes the confidentiality of the Examination very seriously. The retention or dissemination of data relating to the CREST Examination (other than what is contained in the Notes for Candidates and Technical Syllabus documentation that is available from the CREST web site http://www.crest-approved.org) is not permitted.

Candidates must sign Non-Disclosure Agreement to this effect, before they start the Examination.

2 EXAMINATION DETAILS

The CREST Certified Threat Intelligence Manager examination contains only written components – there is no practical element to this exam. There are three elements to the written component: short form questions, long form questions and a more detailed scenario-based element.

The CC TIM examination is delivered in two separate sessions at a Pearson Vue Centre. The Sessions are identified as TIM 1 and TIM 2. TIM 1 must be taken before TIM 2, and TIM 2 must be taken within three months of TIM 1. The award of CCTIM certification will not be made until both TIM 1 and TIM 2 have been passed.

If a candidate fails the examination, both parts must be retaken (see above).

2.1 Short Form Questions (TIM 1)

There are one hundred and fifty (150) questions, all of which the candidate must complete. Each of these questions requires a single word, or a short sentence for an answer.

2.2 Long Form Questions (TIM 1)

The candidate will be presented with one (1) compulsory long form question.

2.3 Long Form & Scenario Questions (TIM 2)

The candidate will be presented with three (3) long form questions of which the candidate must choose and complete two (2) in addition to the one (1) scenario-based question.

The Scenario question is similar in nature to the Long Form questions, although more detail is expected and more time is allocated as a result.

2.4 Timings

The CC TIM examination is delivered in two separate sessions as a Pearson Vue Centre. The Sessions are identified as TIM 1 and TIM 2. TIM 1 must be taken before TIM 2.

TIM 1 will consist of a set of short form questions and a single compulsory long form question, all of which are completed within 3 hours; TIM 2 is also 3 hours long and will comprise both long form and scenario questions. Note that your permitted maximum session time at Pearson Vue is 3.5 hours for each exam, allowing you time to read the Code of Conduct and also to provide feedback following each examination.

Candidates should take great care to note that the breakdown of marks approximates to one mark per minute throughout each phase of the exam. If a candidate spends significantly more time than suggested by the marks for any one section or question, they are potentially missing out on marks that could have been obtained more quickly later in the paper. Where candidates are struggling with a particular question or section, they are strongly advised to move on and return later in the session if remaining time permits.

2.5 Open Book / Closed Book

The whole CCTIM exam is a closed book exam; candidates will not have access to reference material or the Internet for its duration.

2.6 Invigilation

An invigilator will be present throughout the assessment. The Invigilator is not there to assess candidates' capabilities: all assessment is via the objective, written component which will be blind marked by a number of qualified assessors. However, the Invigilator will be able to answer any procedural questions that candidates may have.

3 MARKING SCHEME / PASS MARK

The marking scheme is given in the table below:

Section	Component	Number of questions	Total Marks
CCTIM1	Written (short form) Written (long form)	150: 1 mark each 1: 30 marks	180
CCTIM2	Written (long form)	2: 30 marks each	60
	Scenario	1: 120 marks	120

Successful candidates must score 70% of the available marks in each component.

That is:

- at least **126 marks** from the **CCTIM1** (possible total: 180 marks), and
- at least **42 marks** from the **CCTIM2 Long Form** (possible total: 60 marks), and
- at least **84 marks** from the **Scenario component** (possible total: 120 marks).

This represents an overall pass mark of approximately 70%, but note **that candidates must score the minimum number of marks in each section: candidates who score very well in one component but not in the other will not pass.**

Unsuccessful candidates will be told their final scores in each component where less than 70% of the marks were attained, along with feedback as to the general areas in which they fell short.

4 RECOMMENDED READING

The CREST Certified Threat Intelligence Manager exam covers a number of areas which are detailed in the syllabus.

The following list of resources are relevant to the some areas covered in the syllabus. However the examination is designed to test candidates' knowledge, experience and ability to manage complex engagements, therefore it is not expected that an individual would be able to successfully pass the exam through self-study alone.

The following list is not exhaustive and CREST has not verified any of the resources for accuracy:

- Farnham, G. (2013). Tools and standards for cyber threat intelligence projects. The SANS Institute.
- Poputa-Clean, P. (2015). Automated Defense – Using Threat Intelligence to Augment Security. The SANS Institute.
- Lawson, C. and McMillan, R. (2014). Technology overview for machine-readable threat intelligence. Gartner, Inc.
- Cabinet Office (2016). National cyber security strategy 2016-21. Crown Copyright.
- Marinos, L. (2019). ENISA Threat Landscape 2018. European Union Agency for Network and Information Security (ENISA).
- Heuer, R. (1999). Psychology of intelligence analysis. Center for the Study of Intelligence, CIA.
- KPMG (2013). Cyber threat intelligence and the lessons from law enforcement. KPMG International Cooperative.
- Holland, R. (2013). Five steps to building an effective threat intelligence capability. Forrester Research, Inc.
- Mitre (2018c). ATT&CK Resources. Retrieved from https://attack.mitre.org/resources/. The MITRE Corporation.
- ACPO (2007). Practical Advice: Introduction to Intelligence-Led Policing. ACPO Centrex.
- Caltagirone, S. et al (2013). The Diamond Model of Intrusion Analysis. ThreatConnect.
- Bazzell, M. (2018). Open Source Intelligence Techniques. CCI Publishing.
- Moore, David T., (2007). Critical Thinking and Intelligence Analysis. National Defense Intelligence College Occasional Paper #14.
- Butterfield, A. (1993). The Accuracy of Intelligence Assessment. United States Naval War College.
- Wheaton, K et al. (2006). Structured Analysis of Competing Hypotheses. Strategic and Competitive Intelligence Professionals (SCIP).
- Dartnall, R. (2018). Intelligence Preparation of the Cyber Environment. Retrieved from: https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1517245731.pdf. SANS.
- Dartnall, R. (2017). The use of conventional intelligence methodologies in Cyber Threat Intelligence. Retrieved from: https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1492113006.pdf. SANS.
- CTIPs (2019). What is Cyber Threat Intelligence and how is it used?
- Bank of England (2016): CBEST Intelligence-Led Testing, CBEST Implementation Guide. Version 2.0. Retrieved from: https://www.bankofengland.co.uk/-/media/boe/files/financial-stability/financial-sector-continuity/cbest-implementation-guide
- European Central Bank (2018): Tiber-EU Framework. How to implement the European framework for Threat Intelligence-based Ethical Red Teaming. Retrieved from: https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf
- Bertram, S (2017): F3EAD: Find, Fix, Finish, Exploit, Analyze and Disseminate – The Alternative Intelligence Cycle. Retrieved from: https://www.digitalshadows.com/blog-and-

research/f3ead-find-fix-finish-exploit-analyze-and-disseminate-the-alternative-intelligence-cycle/

5 EXAMINATION LOGISTICS

5.1 Location and Timing

This examination is delivered at a Pearson Vue centre of your choice. Please visit www.pearsonvue.com and follow the on-screen instructions to schedule your chosen examination.

Before the Examination starts

Before the examination starts, Candidates will:

- Need to show suitable office ID (eg military ID, driver's license or passport)
- **Have to sign an NDA**. This is to help us maintain the confidentiality of the Examination.
- Have to sign the **CREST Code of Conduct**.

5.2 Communication of Results

Candidates will receive the overall result of their examination on completion of TIM 2.

Note, no results will be released after completion of TIM 1.

CREST makes every effort to email candidates with their result letters (only) within 14 days of the examination being taken. However, examinations that require second marking may take up to 30 working days for the results to be sent to candidates. This is to ensure both probity and accuracy of results. CREST will make every effort to reduce this period where possible.

6 EXAMPLE QUESTION

6.1 Short Form question

6.1.1 Question

In a commonly accepted formulation, Capability + Intent + Opportunity = What?

6.1.2 Answer

Threat

6.1.3 Marking scheme

Each short form question is worth one mark, though some questions will require multiple answers to earn the full mark. No points are deducted for incorrect answers.