CREST

CREST. Representing the technical information security industry

Assessors Panel

CREST Registered Threat Intelligence Analyst Examination

Notes for Candidates

This document and any information therein are confidential property of CREST and without infringement neither the whole nor any extract may be disclosed, loaned, copied or used for manufacturing, provision of services or other purposes whatsoever without prior written consent of CREST, and no liability is accepted for loss or damage from any cause whatsoever from the use of the document. CREST retain the right to alter the document at any time unless a written statement to the contrary has been appended..

Contents

1. Introduction

1.1. Examination

The CREST Registered Threat Intelligence Analyst (CRTIA) examination tests candidates' knowledge in collecting and analysing information to generate threat intelligence. The exam covers a common set of core skills and knowledge as well as more specific role related areas.

The candidate must demonstrate that they have the knowledge to perform threat intelligence activity safely and effectively, operating within relevant legal and ethical guidelines. Success will confer CREST Registered Threat Intelligence Analyst status to the individual.

The CREST Registered Threat Intelligence Analyst qualification is valid for three (3) years.

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

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 Registered Threat Intelligence Analyst examination contains only written components – there is no practical element to this exam.

There are two elements to the written component: Multiple-choice questions and long-form questions.

2.1. Multiple Choice Questions

2.1.1 Format

The multiple choice component of the CRTIA Examination will comprise one hundred and twenty (120) multiple choice questions, all of which the candidate must complete.

Details of the areas covered can be found in the Syllabus document.

2.2. Long Form Questions

The candidate will be presented with three (3) questions, each worth 25 marks of which **the candidate should select and answer only two (2)**.

2.2.1 Timings

There are 3 hours available in total for the exam.

2.2.2 Open Book /Closed Book

The exam is conducted as a completely closed book process, reference material or access to the Internet is not permitted. Interactive chat or message systems are not permitted.

2.3. Invigilation

An invigilator will be present throughout the examination as Invigilator. The Invigilator is not there to assess candidates' capabilities: all assessment is via the objective written components. However, the Invigilator will be able to answer any procedural questions that candidates may have, and assist in troubleshooting.

3. Marking Scheme / Pass Mark

The marking scheme is given in the table below:

Component	Number of Questions	Total Marks
Written (multiple choice)	120: - 1 mark each	120
Written (long form)	2: - 25 marks each	50

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

- at least **84 marks** from the **multiple choice component** (possible total: 120 marks) and
- At least **35 marks** from the **long form component** (possible total: 50 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.

4. Recommended Reading

The CREST Registered 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 effectively undertake cyber threat intelligence 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

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.

5.2. Before the Examinations 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**.

5.3. Communication of Results

Examination results will be communicated with the candidate within 30 working days of completion of the exam.

6. Example questions

6.1. Written Questions Multiple choice

An example multiple choice question is given below, along with the answer.

6.1.1 Question

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

6.1.2 Answer

The correct answer is (B).

6.1.3 Marking scheme

Each multiple choice answer is worth one (1) mark. No points are deducted for incorrect answers.

CREST

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

www.crest-approved.org