CREST

CREST. Representing the technical information security industry

Assessors Panel

CREST Practitioner Threat Intelligence Analyst

Notes for Candidates

Contents

1. Introduction

1.1. Examination

The CREST Practitioner Threat Intelligence Analyst (CPTIA) 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, and under the guidance of more experienced colleagues (CCTIM, CRTIA qualified personnel). Success will confer CREST Practitioner Threat Intelligence Analyst status to the individual.

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

The examination has one component: a multiple-choice written question section.

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

2.1. Written Component

2.1.1 Format

The written component of the CPTIA 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.

2.1.2 Timings

There are 2 hours available in total for the exam.

Note that your permitted maximum session time at Pearson Vue is 2.5 hours in total, allowing you time to read the Code of Conduct and also to provide feedback following the examination.

2.1.3 Open Book /Closed Book

The written multiple choice 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.

2.2. 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 and practical 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	Total Marks
Written (multiple choice)	120

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

- at least **84 marks** from the **written component** (possible total: 120 marks).

Unsuccessful candidates will be told their final scores in the sections where they didn't reach the required pass mark.

4. Examination Logistics

4.1. 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.

4.2. 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**.

4.3. Communication of Results

Examination results from the automated process are provided to the candidate at the end of the exam session.

Examination scripts will be reviewed within fifteen working days of the examination and formal certificates produced where appropriate and posted to the candidate in hard copy.

5. Example questions

5.1. Written Questions Multiple choice

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

5.1.1 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

5.1.2 Answer

The correct answer is (B).

5.1.3 Marking scheme

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

.

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