CREST Certified Threat Intelligence Manager

5-7 minutes

Book now with Pearson Vue

The CREST Certified Threat Intelligence Manager (CCTIM) examination tests candidates' knowledge and expertise in leading a team that specialises in producing threat intelligence. The candidate is expected to have a good breadth of knowledge in all areas of threat intelligence and proven experience in operational security, data collection / analysis and intelligence production.

The exam will assess the candidate's ability to conduct engagements that produce threat intelligence in a realistic, legal and safe manner, ensuring the customer is provided with actionable intelligence which can be used to increase security and reduce corporate risk.

Examination Format
The examination will consist of three components:

- Short-form questions which require single word or short sentence answers;
- Long form questions that require that require detailed written answers;
- A written scenario-based element which reflects tasks which a threat intelligence Manager is likely to perform on a regular basis

The examination is delivered in two parts (see Notes for Candidates) with Part 1 taken first and Part 2 must be taken within three months of Part 1.

You can download the following documents from the links below:
CREST Threat Intelligence Manager Syllabus
CREST Threat Intelligence Manager Notes for Candidates

Cost
For costs and availability please refer to individual country booking. The examination is delivered at Pearson Vue centres.

Training Providers
In our mission to support individuals in their examination preparation and professional growth, we collaborate with training providers. Search for a Training Provider using our Training Provider Search.

Recommended Preparation Material

CREST recommends that candidates familiarise themselves with the content in our FAQS which have been created specifically for those attempting a practical examination.

The following material and media have been cited as helpful preparation for this examination by previous candidates:

Reading Material:
The following list is not exhaustive and CREST has not verified any of the resources for accuracy:
Definitive Guide to Cyber Threat Intelligence (by Jon Friedman/Mark Bouchard)
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: https://www.youtube.com/watch?v=3bXr-CF9NBI&t=602s

Dartnall, R. (2017). The use of conventional intelligence methodologies in Cyber Threat Intelligence: https://www.youtube.com/watch?v=jzHw8lkocXA

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

ENISA Threat Landscape – 2020: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends

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/

Useful Information for Candidates

Details of the Logistics and Timings of CREST examinations can be found in the Examination Preparation pages for your country of choice

CREST's Policy for Candidates requiring special arrangements including additional time to accommodate a medical condition (including examinations delivered via Pearson Vue.

Terms and Conditions for CREST Examinations (includes hard disk drive wiping policy)