



Vendor: EC-Council

Exam Code: 312-85

Exam Name: Certified Threat Intelligence Analyst (CTIA)
Exam

Version: DEMO

QUESTION 1

Which of the following characteristics of APT refers to numerous attempts done by the attacker to gain entry to the target's network?

- A. Risk tolerance
- B. Timeliness
- C. Attack origination points
- D. Multiphased

Answer: C

QUESTION 2

Lizzy, an analyst, wants to recognize the level of risks to the organization so as to plan countermeasures against cyber attacks. She used a threat modelling methodology where she performed the following stages:

Stage 1: Build asset-based threat profiles
Stage 2: Identify infrastructure vulnerabilities
Stage 3: Develop security strategy and plans

Which of the following threat modelling methodologies was used by Lizzy in the aforementioned scenario?

- A. TRIKE
- B. VAST
- C. OCTAVE
- D. DREAD

Answer: C

QUESTION 3

Which of the following types of threat attribution deals with the identification of the specific person, society, or a country sponsoring a well-planned and executed intrusion or attack over its target?

- A. Nation-state attribution
- B. True attribution
- C. Campaign attribution
- D. Intrusion-set attribution

Answer: B

QUESTION 4

In a team of threat analysts, two individuals were competing over projecting their own hypotheses on a given malware. However, to find logical proofs to confirm their hypotheses, the threat intelligence manager used a de-biasing strategy that involves learning strategic decision making in the circumstances comprising multistep interactions with numerous representatives, either having or without any perfect relevant information.

Which of the following de-biasing strategies the threat intelligence manager used to confirm their hypotheses?

- A. Game theory
- B. Machine learning
- C. Decision theory
- D. Cognitive psychology

Answer: A

QUESTION 5

Cybersol Technologies initiated a cyber-threat intelligence program with a team of threat intelligence analysts. During the process, the analysts started converting the raw data into useful information by applying various techniques, such as machine-based techniques, and statistical methods. In which of the following phases of the threat intelligence lifecycle is the threat intelligence team currently working?

- A. Dissemination and integration
- B. Planning and direction
- C. Processing and exploitation
- D. Analysis and production

Answer: C

QUESTION 6

Joe works as a threat intelligence analyst with Xsecurity Inc. He is assessing the TI program by comparing the project results with the original objectives by reviewing project charter. He is also reviewing the list of expected deliverables to ensure that each of those is delivered to an acceptable level of quality.

Identify the activity that Joe is performing to assess a TI program's success or failure.

- A. Determining the fulfillment of stakeholders
- B. Identifying areas of further improvement
- C. Determining the costs and benefits associated with the program
- D. Conducting a gap analysis

Answer: D

QUESTION 7

An analyst wants to disseminate the information effectively so that the consumers can acquire and benefit out of the intelligence.

Which of the following criteria must an analyst consider in order to make the intelligence concise, to the point, accurate, and easily understandable and must consist of a right balance between tables, narrative, numbers, graphics, and multimedia?

- A. The right time
- B. The right presentation
- C. The right order
- D. The right content

Answer: B

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

- ★ More than **99,900** Satisfied Customers Worldwide.
- ★ Average **99.9%** Success Rate.
- ★ **Free Update** to match latest and real exam scenarios.
- ★ **Instant Download** Access! No Setup required.
- ★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.
- ★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.
- ★ **100%** Guaranteed Success or **100%** Money Back Guarantee.
- ★ **Fast**, helpful support **24x7**.



View list of all certification exams: <http://www.lead2pass.com/all-products.html>



Microsoft



ORACLE



CITRIX



JUNIPER
NETWORKS



EMC²
where information lives

10% Discount Coupon Code: ASTR14