



312-85^{Q&As}

Certified Threat Intelligence Analyst

Pass EC-COUNCIL 312-85 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.pass4itsure.com/312-85.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers



**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

Correct Answer: C

QUESTION 2

ABC is a well-established cyber-security company in the United States. The organization implemented the automation of tasks such as data enrichment and indicator aggregation. They also joined various communities to increase their knowledge about the emerging threats. However, the security teams can only detect and prevent identified threats in a reactive approach.

Based on threat intelligence maturity model, identify the level of ABC to know the stage at which the organization stands with its security and vulnerabilities.

- A. Level 2: increasing CTI capabilities
- B. Level 3: CTI program in place
- C. Level 1: preparing for CTI
- D. Level 0: vague where to start

Correct Answer: A

QUESTION 3

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



Correct Answer: C

QUESTION 4

Bob, a threat analyst, works in an organization named TechTop. He was asked to collect intelligence to fulfil the needs and requirements of the Red Team present within the organization. Which of the following are the needs of a RedTeam?

- A. Intelligence related to increased attacks targeting a particular software or operating system vulnerability
- B. Intelligence on latest vulnerabilities, threat actors, and their tactics, techniques, and procedures (TTPs)
- C. Intelligence extracted latest attacks analysis on similar organizations, which includes details about latest threats and TTPs
- D. Intelligence that reveals risks related to various strategic business decisions

Correct Answer: B

QUESTION 5

An attacker instructs bots to use camouflage mechanism to hide his phishing and malware delivery locations in the rapidly changing network of compromised bots. In this particular technique, a single domain name consists of multiple IP addresses.

Which of the following technique is used by the attacker?

- A. DNS zone transfer
- B. Dynamic DNS
- C. DNS interrogation
- D. Fast-Flux DNS

Correct Answer: D

QUESTION 6

An analyst is conducting threat intelligence analysis in a client organization, and during the information gathering process, he gathered information from the publicly available sources and analyzed to obtain a rich useful form of intelligence. The information source that he used is primarily used for national security, law enforcement, and for collecting intelligence required for business or strategic decision making.

Which of the following sources of intelligence did the analyst use to collect information?

- A. OPSEC
- B. ISAC



C. OSINT

D. SIGINT

Correct Answer: C

QUESTION 7

Tracy works as a CISO in a large multinational company. She consumes threat intelligence to understand the changing trends of cyber security. She requires intelligence to understand the current business trends and make appropriate decisions regarding new technologies, security budget, improvement of processes, and staff. The intelligence helps her in minimizing business risks and protecting the new technology and business initiatives.

Identify the type of threat intelligence consumer is Tracy.

A. Tactical users

B. Strategic users

C. Operational users

D. Technical users

Correct Answer: B

QUESTION 8

Which of the following components refers to a node in the network that routes the traffic from a workstation to external command and control server and helps in identification of installed malware in the network?

A. Repeater

B. Gateway

C. Hub

D. Network interface card (NIC)

Correct Answer: B

QUESTION 9

Jame, a professional hacker, is trying to hack the confidential information of a target organization. He identified the vulnerabilities in the target system and created a tailored deliverable malicious payload using an exploit and a backdoor to send it to the victim.

Which of the following phases of cyber kill chain methodology is Jame executing?

A. Reconnaissance

B. Installation



C. Weaponization

D. Exploitation

Correct Answer: C

QUESTION 10

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

Correct Answer: B

[Latest 312-85 Dumps](#)

[312-85 Exam Questions](#)

[312-85 Braindumps](#)