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.passapply.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

Alison, an analyst in an XYZ organization, wants to retrieve information about a company\\'s website from the time of its inception as well as the removed information from the target website.

What should Alison do to get the information he needs.

A. Alison should use SmartWhois to extract the required website information.

B. Alison should use https://archive.org to extract the required website information.

C. Alison should run the Web Data Extractor tool to extract the required website information.

D. Alison should recover cached pages of the website from the Google search engine cache to extract the required website information.

Correct Answer: C

QUESTION 2

In which of the following storage architecture is the data stored in a localized system, server, or storage hardware and capable of storing a limited amount of data in its database and locally available for data usage?

A. Distributed storage

B. Object-based storage

C. Centralized storage

D. Cloud storage

Correct Answer: B

QUESTION 3

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 4

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 5

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 Tam 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

Latest 312-85 Dumps	312-85 Practice Test	312-85 Study Guide