

# EC-Council

## Exam Questions 312-85

Certified Threat Intelligence Analyst



#### NEW QUESTION 1

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**

#### NEW 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

**Answer: B**

#### NEW QUESTION 3

A team of threat intelligence analysts is performing threat analysis on malware, and each of them has come up with their own theory and evidence to support their theory on a given malware.

Now, to identify the most consistent theory out of all the theories, which of the following analytic processes must threat intelligence manager use?

- A. Threat modelling
- B. Application decomposition and analysis (ADA)
- C. Analysis of competing hypotheses (ACH)
- D. Automated technical analysis

**Answer: C**

#### NEW QUESTION 4

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**

#### NEW QUESTION 5

In which of the following attacks does the attacker exploit vulnerabilities in a computer application before the software developer can release a patch for them?

- A. Active online attack
- B. Zero-day attack
- C. Distributed network attack
- D. Advanced persistent attack

**Answer: B**

#### NEW QUESTION 6

Karry, a threat analyst at an XYZ organization, is performing threat intelligence analysis. During the data collection phase, he used a data collection method that involves no participants and is purely based on analysis and observation of activities and processes going on within the local boundaries of the organization.

Identify the type data collection method used by the Karry.

- A. Active data collection
- B. Passive data collection
- C. Exploited data collection
- D. Raw data collection

**Answer: B**

#### NEW QUESTION 7

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

**Answer: C**

#### NEW QUESTION 8

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

**Answer: B**

#### NEW QUESTION 9

A network administrator working in an ABC organization collected log files generated by a traffic monitoring system, which may not seem to have useful information, but after performing proper analysis by him, the same information can be used to detect an attack in the network. Which of the following categories of threat information has he collected?

- A. Advisories
- B. Strategic reports
- C. Detection indicators
- D. Low-level data

**Answer: C**

#### NEW QUESTION 10

Mr. Bob, a threat analyst, is performing analysis of competing hypotheses (ACH). He has reached to a stage where he is required to apply his analysis skills effectively to reject as many hypotheses and select the best hypotheses from the identified bunch of hypotheses, and this is done with the help of listed evidence. Then, he prepares a matrix where all the screened hypotheses are placed on the top, and the listed evidence for the hypotheses are placed at the bottom. What stage of ACH is Bob currently in?

- A. Diagnostics
- B. Evidence
- C. Inconsistency
- D. Refinement

**Answer: A**

#### NEW QUESTION 10

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

**Answer: C**

#### NEW QUESTION 11

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.

**Answer: C**

#### NEW QUESTION 13

Alice, a threat intelligence analyst at HiTech Cyber Solutions, wants to gather information for identifying emerging threats to the organization and implement essential techniques to prevent their systems and networks from such attacks. Alice is searching for online sources to obtain information such as the method used to launch an attack, and techniques and tools used to perform an attack and the procedures followed for covering the tracks after an attack. Which of the following online sources should Alice use to gather such information?

- A. Financial services
- B. Social network settings

- C. Hacking forums
- D. Job sites

**Answer:** C

**NEW QUESTION 15**

H&P, Inc. is a small-scale organization that has decided to outsource the network security monitoring due to lack of resources in the organization. They are looking for the options where they can directly incorporate threat intelligence into their existing network defense solutions. Which of the following is the most cost-effective methods the organization can employ?

- A. Recruit the right talent
- B. Look for an individual within the organization
- C. Recruit data management solution provider
- D. Recruit managed security service providers (MSSP)

**Answer:** D

**NEW QUESTION 17**

Sarah is a security operations center (SOC) analyst working at JW Williams and Sons organization based in Chicago. As a part of security operations, she contacts information providers (sharing partners) for gathering information such as collections of validated and prioritized threat indicators along with a detailed technical analysis of malware samples, botnets, DDoS attack methods, and various other malicious tools. She further used the collected information at the tactical and operational levels.

Sarah obtained the required information from which of the following types of sharing partner?

- A. Providers of threat data feeds
- B. Providers of threat indicators
- C. Providers of comprehensive cyber-threat intelligence
- D. Providers of threat actors

**Answer:** C

**NEW QUESTION 20**

Walter and Sons Company has faced major cyber attacks and lost confidential data. The company has decided to concentrate more on the security rather than other resources. Therefore, they hired Alice, a threat analyst, to perform data analysis. Alice was asked to perform qualitative data analysis to extract useful information from collected bulk data.

Which of the following techniques will help Alice to perform qualitative data analysis?

- A. Regression analysis, variance analysis, and so on
- B. Numerical calculations, statistical modeling, measurement, research, and so on.
- C. Brainstorming, interviewing, SWOT analysis, Delphi technique, and so on
- D. Finding links between data and discover threat-related information

**Answer:** C

**NEW QUESTION 22**

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

**Answer:** D

**NEW QUESTION 23**

.....

## Thank You for Trying Our Product

### We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

### 312-85 Practice Exam Features:

- \* 312-85 Questions and Answers Updated Frequently
- \* 312-85 Practice Questions Verified by Expert Senior Certified Staff
- \* 312-85 Most Realistic Questions that Guarantee you a Pass on Your First Try
- \* 312-85 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The 312-85 Practice Test Here](#)**