



# **EC-Council**

## **Exam Questions 312-85**

Certified Threat Intelligence Analyst

## About ExamBible

### *Your Partner of IT Exam*

## Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

## Our Advances

### \* 99.9% Uptime

All examinations will be up to date.

### \* 24/7 Quality Support

We will provide service round the clock.

### \* 100% Pass Rate

Our guarantee that you will pass the exam.

### \* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

#### NEW QUESTION 1

Andrews and Sons Corp. has decided to share threat information among sharing partners. Garry, a threat analyst, working in Andrews and Sons Corp., has asked to follow a trust model necessary to establish trust between sharing partners. In the trust model used by him, the first organization makes use of a body of evidence in a second organization, and the level of trust between two organizations depends on the degree and quality of evidence provided by the first organization.

Which of the following types of trust model is used by Garry to establish the trust?

- A. Mediated trust
- B. Mandated trust
- C. Direct historical trust
- D. Validated trust

**Answer: D**

#### NEW QUESTION 2

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 3

Sam works as an analyst in an organization named InfoTech Security. He was asked to collect information from various threat intelligence sources. In meeting the deadline, he forgot to verify the threat intelligence sources and used data from an open-source data provider, who offered it at a very low cost. Through it was beneficial at the initial stage but relying on such data providers can produce unreliable data and noise putting the organization network into risk.

What mistake Sam did that led to this situation?

- A. Sam used unreliable intelligence sources.
- B. Sam used data without context.
- C. Sam did not use the proper standardization formats for representing threat data.
- D. Sam did not use the proper technology to use or consume the information.

**Answer: D**

#### NEW QUESTION 4

Jim works as a security analyst in a large multinational company. Recently, a group of hackers penetrated into their organizational network and used a data staging technique to collect sensitive data. They collected all sorts of sensitive data about the employees and customers, business tactics of the organization, financial information, network infrastructure information and so on.

What should Jim do to detect the data staging before the hackers exfiltrate from the network?

- A. Jim should identify the attack at an initial stage by checking the content of the user agent field.
- B. Jim should analyze malicious DNS requests, DNS payload, unspecified domains, and destination of DNS requests.
- C. Jim should monitor network traffic for malicious file transfers, file integrity monitoring, and event logs.
- D. Jim should identify the web shell running in the network by analyzing server access, error logs, suspicious strings indicating encoding, user agent strings, and so on.

**Answer: C**

#### NEW QUESTION 5

Tim is working as an analyst in an ABC organization. His organization had been facing many challenges in converting the raw threat intelligence data into meaningful contextual information. After inspection, he found that it was due to noise obtained from misrepresentation of data from huge data collections. Hence, it is important to clean the data before performing data analysis using techniques such as data reduction. He needs to choose an appropriate threat intelligence framework that automatically performs data collection, filtering, and analysis for his organization.

Which of the following threat intelligence frameworks should he choose to perform such task?

- A. HighCharts
- B. SIGVERIF
- C. Threat grid
- D. TC complete

**Answer: D**

#### NEW QUESTION 6

Kim, an analyst, is looking for an intelligence-sharing platform to gather and share threat information from a variety of sources. He wants to use this information to develop security policies to enhance the overall security posture of his organization.

Which of the following sharing platforms should be used by Kim?

- A. Cuckoo sandbox
- B. OmniPeek
- C. PortDroid network analysis
- D. Blueliv threat exchange network

**Answer:** D

#### NEW QUESTION 7

What is the correct sequence of steps involved in scheduling a threat intelligence program?

- \* 1. Review the project charter
- \* 2. Identify all deliverables
- \* 3. Identify the sequence of activities
- \* 4. Identify task dependencies
- \* 5. Develop the final schedule
- \* 6. Estimate duration of each activity
- \* 7. Identify and estimate resources for all activities
- \* 8. Define all activities
- \* 9. Build a work breakdown structure (WBS)

- A. 1-->9-->2-->8-->3-->7-->4-->6-->5
- B. 3-->4-->5-->2-->1-->9-->8-->7-->6
- C. 1-->2-->3-->4-->5-->6-->9-->8-->7
- D. 1-->2-->3-->4-->5-->6-->7-->8-->9

**Answer:** A

#### NEW QUESTION 8

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

#### NEW QUESTION 9

During the process of threat intelligence analysis, John, a threat analyst, successfully extracted an indication of adversary's information, such as Modus operandi, tools, communication channels, and forensics evasion strategies used by adversaries.

Identify the type of threat intelligence analysis is performed by John.

- A. Operational threat intelligence analysis
- B. Technical threat intelligence analysis
- C. Strategic threat intelligence analysis
- D. Tactical threat intelligence analysis

**Answer:** D

#### NEW QUESTION 10

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 10

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 15

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:** C

#### NEW QUESTION 18

In which of the following forms of bulk data collection are large amounts of data first collected from multiple sources in multiple formats and then processed to achieve threat intelligence?

- A. Structured form
- B. Hybrid form
- C. Production form
- D. Unstructured form

**Answer:** D

#### NEW QUESTION 20

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 21

Michael, a threat analyst, works in an organization named TechTop, was asked to conduct a cyber-threat intelligence analysis. After obtaining information regarding threats, he has started analyzing the information and understanding the nature of the threats.

What stage of the cyber-threat intelligence is Michael currently in?

- A. Unknown unknowns
- B. Unknowns unknown
- C. Known unknowns
- D. Known knowns

**Answer:** C

#### NEW QUESTION 25

Moses, a threat intelligence analyst at InfoTec Inc., wants to find crucial information about the potential threats the organization is facing by using advanced Google search operators. He wants to identify whether any fake websites are hosted at the similar to the organization's URL.

Which of the following Google search queries should Moses use?

- A. related: [www.infothech.org](http://www.infothech.org)
- B. info: [www.infothech.org](http://www.infothech.org)
- C. link: [www.infothech.org](http://www.infothech.org)
- D. cache: [www.infothech.org](http://www.infothech.org)

**Answer:** A

#### NEW QUESTION 27

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 28

Jian is a member of the security team at Trinity, Inc. He was conducting a real-time assessment of system activities in order to acquire threat intelligence feeds. He acquired feeds from sources like honeynets, P2P monitoring, infrastructure, and application logs.

Which of the following categories of threat intelligence feed was acquired by Jian?

- A. Internal intelligence feeds
- B. External intelligence feeds
- C. CSV data feeds
- D. Proactive surveillance feeds

**Answer:** A

#### NEW QUESTION 31

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 33

.....

## Relate Links

**100% Pass Your 312-85 Exam with ExamBible Prep Materials**

<https://www.exambible.com/312-85-exam/>

## Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>