



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

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 2

An XYZ organization hired Mr. Andrews, a threat analyst. In order to identify the threats and mitigate the effect of such threats, Mr. Andrews was asked to perform threat modeling. During the process of threat modeling, he collected important information about the threat actor and characterized the analytic behavior of the adversary that includes technological details, goals, and motives that can be useful in building a strong countermeasure.

What stage of the threat modeling is Mr. Andrews currently in?

- A. System modeling
- B. Threat determination and identification
- C. Threat profiling and attribution
- D. Threat ranking

Answer: C

NEW QUESTION 3

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 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

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 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

Answer: C

NEW 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

Answer: B

NEW QUESTION 8

Kathy wants to ensure that she shares threat intelligence containing sensitive information with the appropriate audience. Hence, she used traffic light protocol (TLP).

Which TLP color would you signify that information should be shared only within a particular community?

- A. Red
- B. White
- C. Green
- D. Amber

Answer: D

NEW QUESTION 9

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

Answer: B

NEW QUESTION 10

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

Tyrion, a professional hacker, is targeting an organization to steal confidential information. He wants to perform website footprinting to obtain the following information, which is hidden in the web page header.

Connection status and content type
Accept-ranges and last-modified information
X-powered-by information
Web server in use and its version

Which of the following tools should the Tyrion use to view header content?

- A. Hydra
- B. AutoShun
- C. Vanguard enforcer
- D. Burp suite

Answer: D

NEW QUESTION 13

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 18

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 23

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 25

.....

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/>