

EC-Council

Exam Questions 312-85

Certified Threat Intelligence Analyst



NEW QUESTION 1

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)

Answer: B

NEW QUESTION 2

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 3

Lizzy, an analyst, wants to recognize the level of risks to the organization so as to plan countermeasures against cyber attacks. She used a threat modelling methodology where she performed the following stages:

Stage 1: Build asset-based threat profiles

Stage 2: Identify infrastructure vulnerabilities

Stage 3: Develop security strategy and plans

Which of the following threat modelling methodologies was used by Lizzy in the aforementioned scenario?

- A. TRIKE
- B. VAST
- C. OCTAVE
- D. DREAD

Answer: C

NEW QUESTION 4

An organization suffered many major attacks and lost critical information, such as employee records, and financial information. Therefore, the management decides to hire a threat analyst to extract the strategic threat intelligence that provides high-level information regarding current cyber-security posture, threats, details on the financial impact of various cyber-activities, and so on.

Which of the following sources will help the analyst to collect the required intelligence?

- A. Active campaigns, attacks on other organizations, data feeds from external third parties
- B. OSINT, CTI vendors, ISAO/ISACs
- C. Campaign reports, malware, incident reports, attack group reports, human intelligence
- D. Human, social media, chat rooms

Answer: B

NEW QUESTION 5

Daniel is a professional hacker whose aim is to attack a system to steal data and money for profit. He performs hacking to obtain confidential data such as social security numbers, personally identifiable information (PII) of an employee, and credit card information. After obtaining confidential data, he further sells the information on the black market to make money.

Daniel comes under which of the following types of threat actor.

- A. Industrial spies
- B. State-sponsored hackers
- C. Insider threat
- D. Organized hackers

Answer: D

NEW QUESTION 6

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 7

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 8

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 9

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 10

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 10

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
- B. info: www.infothech.org
- C. link: www.infothech.org
- D. cache: www.infothech.org

Answer: A

NEW QUESTION 14

.....

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](#)