

Exam Questions 312-85

Certified Threat Intelligence Analyst

<https://www.2passeasy.com/dumps/312-85/>



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

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 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

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 5

Steve works as an analyst in a UK-based firm. He was asked to perform network monitoring to find any evidence of compromise. During the network monitoring, he came to know that there are multiple logins from different locations in a short time span. Moreover, he also observed certain irregular log in patterns from locations where the organization does not have business relations. This resembles that somebody is trying to steal confidential information.

Which of the following key indicators of compromise does this scenario present?

- A. Unusual outbound network traffic
- B. Unexpected patching of systems
- C. Unusual activity through privileged user account
- D. Geographical anomalies

Answer: C

NEW QUESTION 6

Miley, an analyst, wants to reduce the amount of collected data and make the storing and sharing process easy. She uses filtering, tagging, and queuing technique to sort out the relevant and structured data from the large amounts of unstructured data.

Which of the following techniques was employed by Miley?

- A. Sandboxing
- B. Normalization
- C. Data visualization
- D. Convenience sampling

Answer: B

NEW QUESTION 7

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 8

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 9

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 10

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

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

A threat analyst obtains an intelligence related to a threat, where the data is sent in the form of a connection request from a remote host to the server. From this data, he obtains only the IP address of the source and destination but no contextual information. While processing this data, he obtains contextual information stating that multiple connection requests from different geo-locations are received by the server within a short time span, and as a result, the server is stressed and gradually its performance has reduced. He further performed analysis on the information based on the past and present experience and concludes the attack experienced by the client organization.

Which of the following attacks is performed on the client organization?

- A. DHCP attacks
- B. MAC spoofing attack
- C. Distributed Denial-of-Service (DDoS) attack
- D. Bandwidth attack

Answer: C

NEW QUESTION 18

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 23

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 26

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 27

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 32

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 34

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 35

Henry, a threat intelligence analyst at ABC Inc., is working on a threat intelligence program. He was assigned to work on establishing criteria for prioritization of intelligence needs and requirements.

Which of the following considerations must be employed by Henry to prioritize intelligence requirements?

- A. Understand frequency and impact of a threat
- B. Understand data reliability
- C. Develop a collection plan
- D. Produce actionable data

Answer: A

NEW QUESTION 38

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 312-85 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 312-85 Product From:

<https://www.2passeasy.com/dumps/312-85/>

Money Back Guarantee

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 FirstTry
- * 312-85 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year