EC-Council

Exam Questions 312-85

Certified Threat Intelligence Analyst

NEW QUESTION 1
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 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
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 4
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 5
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 6
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 7
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 8
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 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
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 10
SecurityTech Inc. is developing a TI plan where it can drive more advantages in less funds. In the process of selecting a TI platform, it wants to incorporate a feature that ranks elements such as intelligence sources, threat actors, attacks, and digital assets of the organization, so that it can put in more funds toward the resources which are critical for the organization's security.
Which of the following key features should SecurityTech Inc. consider in their TI plan for selecting the TI platform?

A. Search
B. Open
C. Workflow
D. Scoring

Answer: D

NEW QUESTION 14
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 19
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 24
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 26
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 31
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 32
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons 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 FirstTry

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