Exam Questions 312-85

Certified Threat Intelligence Analyst

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

NEW QUESTION 1
Enrage Tech Company hired Enrique, a security analyst, for performing threat intelligence analysis. While performing data collection process, he used a counterintelligence mechanism where a recursive DNS server is employed to perform interserver DNS communication and when a request is generated from any name server to the recursive DNS server, the recursive DNS servers log the responses that are received. Then it replicates the logged data and stores the data in the central database. Using these logs, he analyzed the malicious attempts that took place over DNS infrastructure.
Which of the following cyber counterintelligence (CCI) gathering technique has Enrique used for data collection?

A. Data collection through passive DNS monitoring
B. Data collection through DNS interrogation
C. Data collection through DNS zone transfer
D. Data collection through dynamic DNS (DDNS)

Answer: B

NEW QUESTION 2
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 3
A team of threat intelligence analysts is performing threat analysis on malware, and each of them has come up with their own theory and evidence to support their theory on a given malware.
Now, to identify the most consistent theory out of all the theories, which of the following analytic processes must threat intelligence manager use?

A. Threat modelling
B. Application decomposition and analysis (ADA)
C. Analysis of competing hypotheses (ACH)
D. Automated technical analysis

Answer: C

NEW QUESTION 4
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 5
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 6
Alice, an analyst, shared information with security operation managers and network operations center (NOC) staff for protecting the organizational resources against various threats. Information shared by Alice was highly technical and include threat actor TTPs, malware campaigns, tools used by threat actors, and so on.
Which of the following types of threat intelligence was shared by Alice?

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

Answer: C

NEW QUESTION 7
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 8
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 9
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 10
......