EC-Council

Exam Questions 312-85

Certified Threat Intelligence Analyst

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
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
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 4
John, a professional hacker, is trying to perform APT attack on the target organization network. He gains access to a single system of a target organization and tries to obtain administrative login credentials to gain further access to the systems in the network using various techniques.
What phase of the advanced persistent threat lifecycle is John currently in?

A. Initial intrusion
B. Search and exfiltration
C. Expansion
D. Persistence

Answer: C

NEW QUESTION 5
Which of the following types of threat attribution deals with the identification of the specific person, society, or a country sponsoring a well-planned and executed intrusion or attack over its target?

A. Nation-state attribution
B. True attribution
C. Campaign attribution
D. Intrusion-set attribution

Answer: B

NEW QUESTION 6
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 treat 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 7
Cybersol Technologies initiated a cyber-threat intelligence program with a team of threat intelligence analysts.
During the process, the analysts started converting the raw data into useful information by applying various techniques, such as machine-based techniques, and statistical methods.
In which of the following phases of the threat intelligence lifecycle is the threat intelligence team currently working?

A. Dissemination and integration
B. Planning and direction
C. Processing and exploitation
D. Analysis and production

Answer: A

NEW QUESTION 8
Which of the following characteristics of APT refers to numerous attempts done by the attacker to gain entry to the target's network?

A. Risk tolerance
B. Timeliness
C. Attack origination points
D. Multiphased

Answer: C

NEW QUESTION 9
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 10
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 10
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 11
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 13
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 14
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 16
.....

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