EC-Council

Exam Questions 312-85

Certified Threat Intelligence Analyst

NEW QUESTION 1
Jim works as a security analyst in a large multinational company. Recently, a group of hackers penetrated into their organizational network and used a data staging technique to collect sensitive data. They collected all sorts of sensitive data about the employees and customers, business tactics of the organization, financial information, network infrastructure information and so on.
What should Jim do to detect the data staging before the hackers exfiltrate from the network?

A. Jim should identify the attack at an initial stage by checking the content of the user agent field.
B. Jim should analyze malicious DNS requests, DNS payload, unspecified domains, and destination of DNS requests.
C. Jim should monitor network traffic for malicious file transfers, file integrity monitoring, and event logs.
D. Jim should identify the web shell running in the network by analyzing server access, error logs, suspicious strings indicating encoding, user agent strings, and so on.

Answer: C

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
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 5
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 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
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 8
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 9
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 Tam 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
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 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 15
Mr. Bob, a threat analyst, is performing analysis of competing hypotheses (ACH). He has reached to a stage where he is required to apply his analysis skills effectively to reject as many hypotheses and select the best hypotheses from the identified bunch of hypotheses, and this is done with the help of listed evidence. Then, he prepares a matrix where all the screened hypotheses are placed on the top, and the listed evidence for the hypotheses are placed at the bottom.
What stage of ACH is Bob currently in?

A. Diagnostics
B. Evidence
C. Inconsistency
D. Refinement

Answer: A

NEW QUESTION 20
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 21
Jame, a professional hacker, is trying to hack the confidential information of a target organization. He identified the vulnerabilities in the target system and created a tailored deliverable malicious payload using an exploit and a backdoor to send it to the victim.
Which of the following phases of cyber kill chain methodology is Jame executing?

A. Reconnaissance
B. Installation
C. Weaponization
D. Exploitation

Answer: C

NEW QUESTION 22
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 23
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 24
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 26
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 27
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 29
An attacker instructs bots to use camouflage mechanism to hide his phishing and malware delivery locations in the rapidly changing network of compromised bots. In this particular technique, a single domain name consists of multiple IP addresses.
Which of the following technique is used by the attacker?

A. DNS zone transfer
B. Dynamic DNS
C. DNS interrogation
D. Fast-Flux DNS

Answer: D

NEW QUESTION 33
......

Relate Links

100% Pass Your 312-85 Exam with Exambible Prep Materials

https://www.exambible.com/312-85-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/