ECCouncil.312-85.v2023-02-09.q15

Exam Code:	312-85
Exam Name:	Certified Threat Intelligence Analyst
Certification Provider:	ECCouncil
Free Question Number:	15
Version:	v2023-02-09
# of views:	458
# of Questions views:	150
https://www.freepdfdumps.com/ECCouncil.312-85.v2023-02-09.q15.html	

NEW QUESTION: 1
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. Campaign attribution
B. Nation-state attribution
C. Intrusion-set attribution
D. True attribution
Answer: D (LEAVE A REPLY)

NEW QUESTION: 2
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. Known unknowns
C. Known knowns
D. Unknowns unknown
Answer: B (LEAVE A REPLY)

NEW QUESTION: 3
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. cache: www.infothech.org
C. link: www.infothech.org
D. info: www.infothech.org
Answer: A (LEAVE A REPLY)

NEW QUESTION: 4
During the process of threat intelligence analysis, John, a threat analyst, successfully extracted an indication of adversary's information, such as Modus operandi, tools, communication channels, and forensics evasion strategies used by adversaries.
Identify the type of threat intelligence analysis is performed by John.
A. Strategic threat intelligence analysis
B. Technical threat intelligence analysis
C. Tactical threat intelligence analysis
D. Operational threat intelligence analysis
Answer: (SHOW ANSWER)

NEW QUESTION: 5
Walter and Sons Company has faced major cyber attacks and lost confidential dat a. 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. Brainstorming, interviewing, SWOT analysis, Delphi technique, and so on
B. Regression analysis, variance analysis, and so on
C. Finding links between data and discover threat-related information
D. Numerical calculations, statistical modeling, measurement, research, and so on.
Answer: (SHOW ANSWER)

NEW QUESTION: 6
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 extracted latest attacks analysis on similar organizations, which includes details about latest threats and TTPs
B. Intelligence related to increased attacks targeting a particular software or operating system vulnerability
C. Intelligence that reveals risks related to various strategic business decisions
D. Intelligence on latest vulnerabilities, threat actors, and their tactics, techniques, and procedures (TTPs)

Answer: D (LEAVE A REPLY)

NEW QUESTION: 7
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 (LEAVE A REPLY)

NEW QUESTION: 8
Which of the following components refers to a node in the network that routes the traffic from a workstation to external command and control server and helps in identification of installed malware in the network?
A. Hub
B. Network interface card (NIC)
C. Repeater
D. Gateway
Answer: D (LEAVE A REPLY)

NEW QUESTION: 9
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. Scoring
B. Open
C. Workflow
D. Search
Answer: A (LEAVE A REPLY)

NEW QUESTION: 10
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 dat a. 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 web shell running in the network by analyzing server access, error logs, suspicious strings indicating encoding, user agent strings, and so on.
B. Jim should identify the attack at an initial stage by checking the content of the user agent field.
C. Jim should monitor network traffic for malicious file transfers, file integrity monitoring, and event logs.
D. Jim should analyze malicious DNS requests, DNS payload, unspecified domains, and destination of DNS requests.
Answer: (SHOW ANSWER)

NEW QUESTION: 11
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. Production form
B. Structured form
C. Unstructured form
D. Hybrid form
Answer: (SHOW ANSWER)

NEW QUESTION: 12
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. CSV data feeds
B. External intelligence feeds
C. Proactive surveillance feeds
D. Internal intelligence feeds
Answer: (SHOW ANSWER)

NEW QUESTION: 13
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. Exploitation
D. Weaponization
Answer: (SHOW ANSWER)

NEW QUESTION: 14
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. Low-level data
B. Advisories
C. Strategic reports
D. Detection indicators
Answer: A (LEAVE A REPLY)

NEW QUESTION: 15
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. Vanguard enforcer
C. AutoShun
D. Burp suite
Answer: D (LEAVE A REPLY)