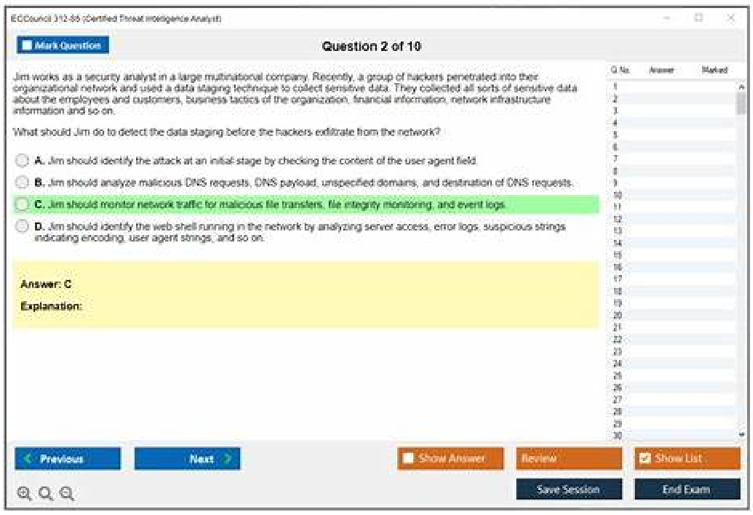
ECCouncil 312-85 Test Passing Score - 312-85 Test Dumps Demo



Question 2 of 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 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

Explanation:

What's more, part of that Getcertkey 312-85 dumps now are free: https://drive.google.com/open?id=1HYSYpNEo5d0IBN0GQsvZP27UAh_YWiFk

Certified Threat Intelligence Analyst exam tests hired dedicated staffs to update the contents of the data on a daily basis. Our industry experts will always help you keep an eye on changes in the exam syllabus, and constantly supplement the contents of 312-85 test guide. Therefore, with our study materials, you no longer need to worry about whether the content of the exam has changed. You can calm down and concentrate on learning. At the same time, the researchers hired by 312-85 Test Guide is all those who passed the 312-85 exam, and they all have been engaged in teaching or research in this industry for more than a decade. They have a keen sense of smell on the trend of changes in the exam questions. Therefore, with the help of these experts, the contents of 312-85 exam questions must be the most advanced and close to the real exam.

ECCouncil 312-85 (Certified Threat Intelligence Analyst) Certification Exam is a professional certification program designed for individuals who want to specialize in threat intelligence and analysis. Certified Threat Intelligence Analyst certification exam measures the knowledge and skills required to identify and mitigate different types of security threats. Certified Threat Intelligence Analyst certification exam covers topics such as threat intelligence, cybercrime investigations, threat hunting, and incident response. Individuals who pass this certification exam are recognized as experts in the field of threat intelligence and analysis.

ECCouncil 312-85, also known as the Certified Threat Intelligence Analyst (CTIA) certification exam, is an internationally recognized certification that validates an individual's expertise in identifying and analyzing cyber threats. 312-85 Exam is designed for professionals who are responsible for protecting sensitive information and critical infrastructure from cyber threats. The CTIA certification exam is a testament to the individual's ability to provide effective threat intelligence solutions to organizations worldwide.

>> ECCouncil 312-85 Test Passing Score <<

312-85 Test Dumps Demo - Reliable 312-85 Study Plan

To be the best global supplier of electronic 312-85 study materials for our customers through innovation and enhancement of our customers' satisfaction has always been our common pursuit. The advantages of our 312-85 study guide are more than you can count. As the most important factor that our worthy customers will consider-the pass rate, we are proud to tell you that we have a pass rate high as 98% to 100% on our 312-85 training engine, which is also unique in the market. And our price of the 312-85 practice guide is also reasonable.

The CTIA certification is an excellent choice for individuals who are looking to validate their skills and knowledge in the field of threat intelligence analysis. Certified Threat Intelligence Analyst certification covers a wide range of topics related to threat intelligence, and it is recognized globally. If you are interested in pursuing a career in cybersecurity and are looking to specialize in threat intelligence analysis, then the CTIA certification is definitely worth considering.

ECCouncil Certified Threat Intelligence Analyst Sample Questions (Q23-Q28):

NEW QUESTION # 23
Henry. a threat intelligence analyst at ABC Inc., is working on a threat intelligence program. He was assigned to work on establishing criteria for prioritization of intelligence needs and requirements.
Which of the following considerations must be employed by Henry to prioritize intelligence requirements?

- A. Understand frequency and impact of a threat
- B. Produce actionable data
- C. Understand data reliability
- D. Develop a collection plan

Answer: A

Explanation:
When prioritizing intelligence requirements, it is crucial to understand the frequency and impact of various threats. This approach helps in allocating resources effectively, focusing on threats that are both likely to occur and that would have significant consequences if they did. By assessing threats based on these criteria, Henry can ensure that the threat intelligence program addresses the most pressing and potentially damaging threats first, thereby enhancing the organization's security posture. This prioritization is essential for effective threat management and for ensuring that the most critical threats are addressed promptly.
References:
"Cyber Threat Intelligence: Prioritizing and Using CTI Effectively," by SANS Institute
"Threat Intelligence: What It Is, and How to Use It Effectively," by Gartner

NEW QUESTION # 24
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

Explanation:
The "related:" Google search operator is used to find websites that are similar or related to a specified URL.
In the context provided, Moses wants to identify fake websites that may be posing as or are similar to his organization's official site.
By using the "related:" operator followed by his organization's URL, Google will return a list of websites that Google considers to be similar to the specified site. This can help Moses identify potential impersonating websites that could be used for phishing or other malicious activities. The "info:",
"link:", and "cache:" operators serve different purposes; "info:" provides information about the specified webpage, "link:" used to be used to find pages linking to a specific URL (but is now deprecated), and "cache:" shows the cached version of the specified webpage.
References:
Google Search Operators Guide by Moz
Google Advanced Search Help Documentation

NEW QUESTION # 25
James, a senior threat intelligence officer, was tasked with assessing the success and failure of the threat intelligence program established by the organization. As part of the assessment, James reviewed the outcome of the intelligence program, determined if any improvements were required, and identified the past learnings that can be applied to future programs.
Identify the activity performed by James in the above scenario.

- A. Determine the costs and benefits associated with the program

- B. Conduct a gap analysis
- C. Report findings and recommendations
- D. Determine the fulfillment of stakeholders

Answer: C

Explanation:
The activity described involves reviewing outcomes, identifying improvements, and documenting lessons learned, which corresponds to Reporting Findings and Recommendations.
This activity takes place in the evaluation and feedback phase of the threat intelligence lifecycle. It ensures the program remains effective and continuously improves based on real-world results and organizational feedback.
Why the Other Options Are Incorrect:
* B. Determine the fulfillment of stakeholders: Focuses on verifying if stakeholder requirements are met, not overall program performance.
* C. Conduct a gap analysis: Identifies missing capabilities or processes, but does not encompass reviewing program success.
* D. Determine the costs and benefits: Involves financial evaluation, not operational assessment.
Conclusion:
James was engaged in the Report Findings and Recommendations phase of program evaluation.
Final Answer: A. Report findings and recommendations
Explanation Reference (Based on CTIA Study Concepts):
CTIA highlights reporting findings and recommendations as a crucial feedback mechanism to enhance the effectiveness of intelligence programs.

NEW QUESTION # 26
Two cybersecurity teams from different organizations joined forces to combat a rapidly evolving malware campaign targeting their industry. They exchange real-time information about the attackers' techniques, compromised systems, and immediate defensive actions. What type of threat intelligence sharing characterizes this collaboration?

- A. Sharing strategic threat intelligence
- B. Sharing operational threat intelligence
- C. Sharing tactical threat intelligence
- D. Sharing technical threat intelligence

Answer: C

Explanation:
The exchange of attack techniques, compromised systems, and immediate defensive actions represents Tactical Threat Intelligence sharing.
Tactical Threat Intelligence focuses on adversary Tactics, Techniques, and Procedures (TTPs) and helps defenders understand and counter ongoing attacks in real time.
Why the Other Options Are Incorrect:
* B. Operational: Focuses on broader attack campaigns and contextual analysis.
* C. Strategic: Provides high-level, long-term insights for executives.
* D. Technical: Concerns low-level indicators like IPs and file hashes, not methodologies or immediate actions.
Conclusion:
The collaboration involves Tactical Threat Intelligence, which centers on sharing actionable TTPs and response techniques.
Final Answer: A. Sharing tactical threat intelligence
Explanation Reference (Based on CTIA Study Concepts):
CTIA defines tactical threat intelligence as intelligence describing attacker behaviors and techniques that can be acted upon immediately by defenders.

NEW QUESTION # 27
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. Human, social media, chat rooms
- B. Active campaigns, attacks on other organizations, data feeds from external third parties

- C. Campaign reports, malware, incident reports, attack group reports, human intelligence
- D. OSINT, CTI vendors, ISAO/ISACs

Answer: D

Explanation:
For gathering strategic threat intelligence that provides a high-level overview of the current cybersecurity posture, potential financial impacts of cyber activities, and overarching threats, sources such as Open Source Intelligence (OSINT), Cyber Threat Intelligence (CTI) vendors, and Information Sharing and Analysis Organizations (ISAOs)/Information Sharing and Analysis Centers (ISACs) are invaluable. OSINT involves collecting data from publicly available sources, CTI vendors specialize in providing detailed threat intelligence services, and ISAOs/ISACs facilitate the sharing of threat data within specific industries or communities. These sources can provide broad insights into threat landscapes, helping organizations understand how to align their cybersecurity strategies with current trends and threats.
References:
"Cyber Threat Intelligence: Sources and Methods," by Max Kilger, Ph.D., SANS Institute Reading Room
"Open Source Intelligence (OSINT): An Introduction to the Basic Concepts and the Potential Benefits for Information Security," by Kevin Cardwell, IEEE Xplore

NEW QUESTION # 28
......