312-39Q&As

Certified SOC Analyst (CSA)

Pass EC-COUNCIL 312-39 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/312-39.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

QUESTION 1

Which encoding replaces unusual ASCII characters with "%" followed by the character\\'s two-digit ASCII code expressed in hexadecimal?

A. Unicode Encoding

B. UTF Encoding

C. Base64 Encoding

D. URL Encoding

Correct Answer: D

Reference: https://ktflash.gitbooks.io/ceh_v9/content/125_countermeasures.html

QUESTION 2

Properly applied cyber threat intelligence to the SOC team help them in discovering TTPs. What does these TTPs refer to?

A. Tactics, Techniques, and Procedures

B. Tactics, Threats, and Procedures

C. Targets, Threats, and Process

D. Tactics, Targets, and Process

Correct Answer: A

Reference: https://www.crest-approved.org/wp-content/uploads/CREST-Cyber-Threat-Intelligence.pdf

QUESTION 3

Which of the following threat intelligence is used by a SIEM for supplying the analysts with context and "situational awareness" by using threat actor TTPs, malware campaigns, tools used by threat actors.

1.

Strategic threat intelligence

2.

Tactical threat intelligence

3.

Operational threat intelligence

4.

Technical threat intelligence

A. 2 and 3

B. 1 and 3

C. 3 and 4

D. 1 and 2

Correct Answer: A

Reference: https://hodigital.blog.gov.uk/wp-content/uploads/sites/161/2020/03/Cyber-Threat-Intelligence-A-Guide-For-Decision-Makers-and-Analysts-v2.0.pdf (38)

QUESTION 4

Which of the following service provides phishing protection and content filtering to manage the Internet experience on and off your network with the acceptable use or compliance policies?

A. Apility.io

B. Malstrom

C. OpenDNS

D. I-Blocklist

Correct Answer: C

Reference: https://www.spamtitan.com/web-filtering/category/cybersecurity-advice/

QUESTION 5

Bonney\\'s system has been compromised by a gruesome malware.

What is the primary step that is advisable to Bonney in order to contain the malware incident from spreading?

A. Complaint to police in a formal way regarding the incident

B. Turn off the infected machine

C. Leave it to the network administrators to handle

D. Call the legal department in the organization and inform about the incident

Correct Answer: B