312-39$^{Q\&As}$

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 of the following attack can be eradicated by converting all non-alphanumeric characters to HTML character entities before displaying the user input in search engines and forums?

A. Broken Access Control Attacks

B. Web Services Attacks

C. XSS Attacks

D. Session Management Attacks

Correct Answer: C

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

QUESTION 2

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 3

Juliea a SOC analyst, while monitoring logs, noticed large TXT, NULL payloads. What does this indicate?

A. Concurrent VPN Connections Attempt

B. DNS Exfiltration Attempt

C. Covering Tracks Attempt

D. DHCP Starvation Attempt

Correct Answer: B

Reference: https://www.google.com/url?sa=tandrct=jandq=andesrc=sandsource=webandcd=andved=2ahUKEwj8gZaKq_PuAhWGi1wKHfQTC0oQFjAAegQIARADandurl=https%3A%2F%2Fconf.splunk.com%2Fsession%2F2014%

2Fconf2014_FredWilmotSanfordOwings_Splunk_Security.pdfandusg=AOvVaw3ZLfzGqM-VUG7xKtze67ac

QUESTION 4

Which of the following formula represents the risk levels?

A. Level of risk = Consequence x Severity

B. Level of risk = Consequence x Impact

C. Level of risk = Consequence x Likelihood

D. Level of risk = Consequence x Asset Value

Correct Answer: B

QUESTION 5

Shawn is a security manager working at Lee Inc Solution. His organization wants to develop threat intelligent strategy plan. As a part of threat intelligent strategy plan, he suggested various components, such as threat intelligence requirement analysis, intelligence and collection planning, asset identification, threat reports, and intelligence buy-in.

Which one of the following components he should include in the above threat intelligent strategy plan to make it effective?

A. Threat pivoting

B. Threat trending

C. Threat buy-in

D. Threat boosting

Correct Answer: C