DUMPSARENA

Certified SOC Analyst (CSA)

ECCouncil 312-39

Version Demo

Total Demo Questions: 10

Total Premium Questions: 100

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

Which of the following tool is used to recover from web application incident?

A. CrowdStrike FalconTM Orchestrator

B. Symantec Secure Web Gateway

C. Smoothwall SWG

D. Proxy Workbench

ANSWER: B

QUESTION NO: 2

Robin, a SOC engineer in a multinational company, is planning to implement a SIEM. He realized that his organization is capable of performing only Correlation, Analytics, Reporting, Retention, Alerting, and Visualization required for the SIEM implementation and has to take collection and aggregation services from a Managed Security Services Provider (MSSP).

What kind of SIEM is Robin planning to implement?

A. Self-hosted, Self-Managed

B. Self-hosted, MSSP Managed

C. Hybrid Model, Jointly Managed

D. Cloud, Self-Managed

ANSWER: B

QUESTION NO: 3

Which of the following technique protects from flooding attacks originated from the valid prefixes (IP addresses) so that they can be traced to its true source?

A. Rate Limiting

B. Egress Filtering

C. Ingress Filtering

D. Throttling

ANSWER: C

Explanation:

Reference: http://www.mecs-press.org/ijcnis/ijcnis-v5-n5/IJCNIS-V5-N5-6.pdf (3)

QUESTION NO: 4

Which of the following is a set of standard guidelines for ongoing development, enhancement, storage, dissemination and implementation of security standards for account data protection?

A. FISMA

B. HIPAA

C. PCI-DSS

D. DARPA

ANSWER: C

Explanation:

Reference: https://library.educause.edu/topics/policy-and-law/pci-dss

QUESTION NO: 5

Which attack works like a dictionary attack, but adds some numbers and symbols to the words from the dictionary and tries to crack the password?

A. Hybrid Attack

B. Bruteforce Attack

C. Rainbow Table Attack

D. Birthday Attack

ANSWER: B

Explanation:

Reference: https://www.techrepublic.com/article/brute-force-and-dictionary-attacks-a-cheat-sheet/

QUESTION NO: 6

Daniel is a member of an IRT, which was started recently in a company named Mesh Tech. He wanted to find the purpose and scope of the planned incident response capabilities.

What is he looking for?

A. Incident Response Intelligence

B. Incident Response Mission

C. Incident Response Vision

D. Incident Response Resources

ANSWER: D

Explanation:

Reference: https://blog.eccouncil.org/phases-of-an-incident-response-plan/

QUESTION NO: 7

According to the Risk Matrix table, what will be the risk level when the probability of an attack is very low and the impact of that attack is major?

A. High

B. Extreme

C. Low

D. Medium

ANSWER: C

Explanation:

Reference: https://www.moheri.gov.om/userupload/Policy/IT%20Risk%20Management%20Framework.pdf (17)

QUESTION NO: 8

What does [-n] in the following checkpoint firewall log syntax represents?

fw log [-f [-t]] [-n] [-l] [-o] [-c action] [-h host] [-s starttime] [-e endtime] [-b starttime endtime] [-u unification_scheme_file] [-m unification_mode(initial|semi|raw)] [-a] [-k (alert name|all)] [-g] [logfile]

A. Speed up the process by not performing IP addresses DNS resolution in the Log files

B. Display both the date and the time for each log record

C. Display account log records only

D. Display detailed log chains (all the log segments a log record consists of)

ANSWER: A

Explanation:

Reference:
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk25532

QUESTION NO: 9

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

ANSWER: D

Explanation:

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

QUESTION NO: 10

Which of the following steps of incident handling and response process focus on limiting the scope and extent of an incident?

A. Containment

B. Data Collection

C. Eradication

D. Identification

ANSWER: A