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.pass2lead.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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Which of the following formula represents the risk?

A. Risk = Likelihood × Severity × Asset Value

B. Risk = Likelihood × Consequence × Severity

C. Risk = Likelihood × Impact × Severity

D. Risk = Likelihood × Impact × Asset Value

Correct Answer: B

QUESTION 2

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)

Correct Answer: A

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

QUESTION 3

An organization wants to implement a SIEM deployment architecture. However, they have the capability to do only log collection and the rest of the SIEM functions must be managed by an MSSP.

Which SIEM deployment architecture will the organization adopt?

A. Cloud, MSSP Managed

B. Self-hosted, Jointly Managed

C. Self-hosted, MSSP Managed

D. Self-hosted, Self-Managed

Correct Answer: C

QUESTION 4

Harley is working as a SOC analyst with Powell Tech. Powell Inc. is using Internet Information Service (IIS) version 7.0 to host their website.

Where will Harley find the web server logs, if he wants to investigate them for any anomalies?

A. SystemDrive%\inetpub\logs\LogFiles\W3SVCN

B. SystemDrive%\LogFiles\inetpub\logs\W3SVCN

C. %SystemDrive%\LogFiles\logs\W3SVCN

D. SystemDrive%\ inetpub\LogFiles\logs\W3SVCN

Correct Answer: B

Reference: https://docs.microsoft.com/en-us/iis/configuration/system.applicationhost/sites/sitedefaults/ logfile/

QUESTION 5

Which of the following is a correct flow of the stages in an incident handling and response (IHandR) process?

A. Containment –andgt; Incident Recording –andgt; Incident Triage –andgt; Preparation –andgt; Recovery –andgt; Eradication –andgt; Post-Incident Activities

B. Preparation –andgt; Incident Recording –andgt; Incident Triage –andgt; Containment –andgt; Eradication –andgt; Recovery –andgt; Post-Incident Activities

C. Incident Triage –andgt; Eradication –andgt; Containment –andgt; Incident Recording –andgt; Preparation –andgt; Recovery –andgt; Post-Incident Activities

D. Incident Recording –andgt; Preparation –andgt; Containment –andgt; Incident Triage –andgt; Recovery –andgt; Eradication –andgt; Post-Incident Activities

Correct Answer: B

Reference: https://blog.elearnsecurity.com/the-4-steps-of-incident-handling-response.html

312-39 PDF Dumps 312-39 Practice Test 312-39 Study Guide