

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.pass4itsure.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



https://www.pass4itsure.com/312-39.html

2024 Latest pass4itsure 312-39 PDF and VCE dumps Download

QUESTION 1

Which of the following can help you eliminate the burden of investigating false positives?

- A. Keeping default rules
- B. Not trusting the security devices
- C. Treating every alert as high level
- D. Ingesting the context data

Correct Answer: A

Reference: https://stratozen.com/9-ways-eliminate-siem-false-positives/

QUESTION 2

In which log collection mechanism, the system or application sends log records either on the local disk or over the network.

- A. rule-based
- B. pull-based
- C. push-based
- D. signature-based

Correct Answer: A

QUESTION 3

Which one of the following is the correct flow for Setting Up a Computer Forensics Lab?

A. Planning and budgeting

Correct Answer: A

Reference: https://info-savvy.com/setting-up-a-computer-forensics-lab/

QUESTION 4

Identify the attack in which the attacker exploits a target system through publicly known but still unpatched vulnerabilities.

A. Slow DoS Attack



https://www.pass4itsure.com/312-39.html

2024 Latest pass4itsure 312-39 PDF and VCE dumps Download

- B. DHCP Starvation
- C. Zero-Day Attack
- D. DNS Poisoning Attack

Correct Answer: C

Reference: https://www.bullguard.com/bullguard-security-center/pc-security/computer-threats/what-are-zero-day-attacks.aspx

QUESTION 5

Sam, a security analyst with INFOSOL INC., while monitoring and analyzing IIS logs, detected an event matching regex $(\w^*((\w27)|(\w))((\w6F)|o|(\w4F))((\w72)|r|(\w52))/ix$. What does this event log indicate?

- A. SQL Injection Attack
- B. Parameter Tampering Attack
- C. XSS Attack
- D. Directory Traversal Attack

Correct Answer: A

Reference: https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/view document?DocumentKey=001f5e09-88b4-4a9a-

b310-4c20578eecf9andCommunityKey=1ecf5f55-9545-44d6-b0f44e4a7f5f5e68andtab=librarydocuments

312-39 PDF Dumps

312-39 VCE Dumps

312-39 Practice Test