# 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

**QUESTION 1**

Where will you find the reputation IP database, if you want to monitor traffic from known bad IP reputation using OSSIM SIEM?

A. /etc/ossim/reputation

B. /etc/ossim/siem/server/reputation/data

C. /etc/siem/ossim/server/reputation.data

D. /etc/ossim/server/reputation.data

Correct Answer: A

**QUESTION 2**

An attacker, in an attempt to exploit the vulnerability in the dynamically generated welcome page, inserted code at the end of the company\\'s URL as follows:

http://technosoft.com.com/alert("WARNING: The application has encountered an error");.

Identify the attack demonstrated in the above scenario.

A. Cross-site Scripting Attack

B. SQL Injection Attack

C. Denial-of-Service Attack

D. Session Attack

Correct Answer: D

**QUESTION 3**

What does the Security Log Event ID 4624 of Windows 10 indicate?

A. Service added to the endpoint

B. A share was assessed

C. An account was successfully logged on

D. New process executed

Correct Answer: C

Reference: https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4624

**QUESTION 4**

Which of the following event detection techniques uses User and Entity Behavior Analytics (UEBA)?

A. Rule-based detection

B. Heuristic-based detection

C. Anomaly-based detection

D. Signature-based detection

Correct Answer: C

**QUESTION 5**

InfoSystem LLC, a US-based company, is establishing an in-house SOC. John has been given the responsibility to finalize strategy, policies, and procedures for the SOC. Identify the job role of John.

A. Security Analyst

Correct Answer: B

Reference: https://www.exabeam.com/security-operations-center/security-operations-center-roles-and-responsibilities/