



# 312-39<sup>Q&As</sup>

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

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





### QUESTION 1

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 2

Which of the following formula is used to calculate the EPS of the organization?

- A.  $EPS = \text{average number of correlated events} / \text{time in seconds}$
- B.  $EPS = \text{number of normalized events} / \text{time in seconds}$
- C.  $EPS = \text{number of security events} / \text{time in seconds}$
- D.  $EPS = \text{number of correlated events} / \text{time in seconds}$

Correct Answer: A

---

### QUESTION 3

Which of the following attack inundates DHCP servers with fake DHCP requests to exhaust all available IP addresses?

- A. DHCP Starvation Attacks
- B. DHCP Spoofing Attack
- C. DHCP Port Stealing
- D. DHCP Cache Poisoning

Correct Answer: A

Reference: <https://www.cbtnuggets.com/blog/technology/networking/what-is-a-dhcp-starvation-attack>

---

**QUESTION 4**

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

---

**QUESTION 5**

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

Correct Answer: B

[Latest 312-39 Dumps](#)

[312-39 PDF Dumps](#)

[312-39 VCE Dumps](#)