



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.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

Identify the HTTP status codes that represents the server error.

- A. 2XX
- B. 4XX
- C. 1XX
- D. 5XX

Correct Answer: D

Reference: https://www.tutorialspoint.com/http/http_status_codes.htm

QUESTION 2

Which of the following data source can be used to detect the traffic associated with Bad Bot User-Agents?

- A. Windows Event Log
- B. Web Server Logs
- C. Router Logs
- D. Switch Logs

Correct Answer: B

QUESTION 3

Which of the following attack can be eradicated by disabling of "allow_url_fopen and allow_url_include" in the php.ini file?

- A. File Injection Attacks
- B. URL Injection Attacks
- C. LDAP Injection Attacks
- D. Command Injection Attacks

Correct Answer: B

QUESTION 4

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



- A. EPS = average number of correlated events / time in seconds
- B. EPS = number of normalized events / time in seconds
- C. EPS = number of security events / time in seconds
- D. EPS = number of correlated events / time in seconds

Correct Answer: A

QUESTION 5

Which of the following tool can be used to filter web requests associated with the SQL Injection attack?

- A. Nmap
- B. UrlScan
- C. ZAP proxy
- D. Hydra

Correct Answer: B

Reference: <https://aip.scitation.org/doi/pdf/10.1063/1.4982570>

[Latest 312-39 Dumps](#)

[312-39 PDF Dumps](#)

[312-39 Braindumps](#)