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.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

Wesley is an incident handler in a company named Maddison Tech. One day, he was learning techniques for eradicating the insecure deserialization attacks.

What among the following should Wesley avoid from considering?

A. Deserialization of trusted data must cross a trust boundary

B. Understand the security permissions given to serialization and deserialization

C. Allow serialization for security-sensitive classes

D. Validate untrusted input, which is to be serialized to ensure that serialized data contain only trusted classes

Correct Answer: C

QUESTION 2

If the SIEM generates the following four alerts at the same time:

I. Firewall blocking traffic from getting into the network alerts

II. SQL injection attempt alerts

III. Data deletion attempt alerts

IV. Brute-force attempt alerts

Which alert should be given least priority as per effective alert triaging?

A. III

B. IV

C. II

D. I

Correct Answer: D

QUESTION 3

Which encoding replaces unusual ASCII characters with "%" followed by the character\\'s two-digit ASCII code expressed in hexadecimal?

A. Unicode Encoding

B. UTF Encoding

C. Base64 Encoding

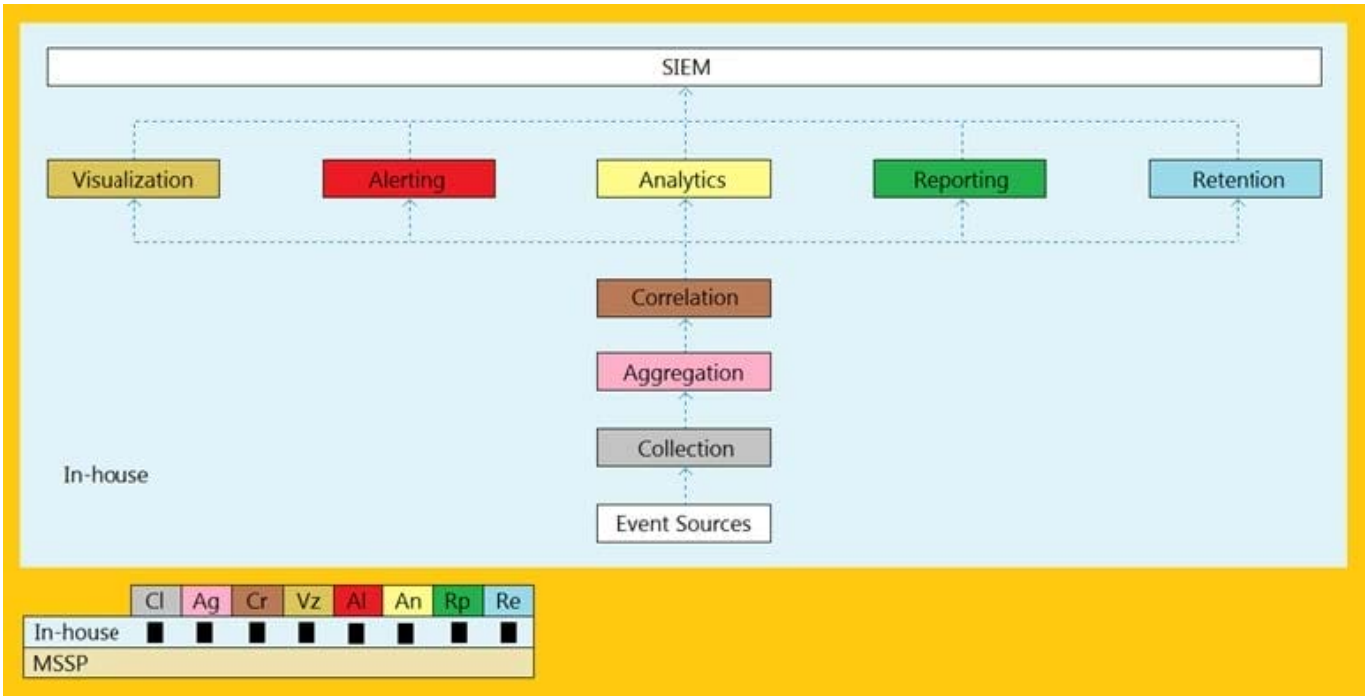
D. URL Encoding

Correct Answer: D

Reference: https://ktflash.gitbooks.io/ceh_v9/content/125_countermeasures.html

QUESTION 4

An organization is implementing and deploying the SIEM with following capabilities.



What kind of SIEM deployment architecture the organization is planning to implement?

A. Cloud, MSSP Managed

B. Self-hosted, Jointly Managed

C. Self-hosted, Self-Managed

D. Self-hosted, MSSP Managed

Correct Answer: A

QUESTION 5

Jane, a security analyst, while analyzing IDS logs, detected an event matching Regex /((\%3C)|)/|.

What does this event log indicate?

A. Directory Traversal Attack

B. Parameter Tampering Attack

C. XSS Attack

D. SQL Injection Attack

Correct Answer: C

Reference: https://books.google.com.pk/books?id=PDR4nOAP8qUCandpg=PA87andlpg=PA87anddq=regex+/((%5C%253C)%7C)/%7Candsource=blandots=kOBHNfJmtqandsig=ACfU3U2CG_hELc1HMb1chdc9OS4ooXPlMgandhl=enandsa=Xandved=2ahUKEwjYwJmlt_buAhUFShUIHTBNAs8Q6AEwBXoECAUQAw#v=onepageandqandf=false