



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.passapply.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

The threat intelligence, which will help you, understand adversary intent and make informed decision to ensure appropriate security in alignment with risk. What kind of threat intelligence described above?

- A. Tactical Threat Intelligence
- B. Strategic Threat Intelligence
- C. Functional Threat Intelligence
- D. Operational Threat Intelligence

Correct Answer: B

Reference: <https://www.blueliv.com/cyber-security-and-cyber-threat-intelligence-blog-blueliv/threat-intelligence/what-is-threat-intelligence/>

QUESTION 2

Which of the following steps of incident handling and response process focus on limiting the scope and extent of an incident?

- A. Containment
- B. Data Collection
- C. Eradication
- D. Identification

Correct Answer: A

QUESTION 3

Which of the following attack can be eradicated by filtering improper XML syntax?

- A. CAPTCHA Attacks
- B. SQL Injection Attacks
- C. Insufficient Logging and Monitoring Attacks
- D. Web Services Attacks

Correct Answer: B

QUESTION 4



Charline is working as an L2 SOC Analyst. One day, an L1 SOC Analyst escalated an incident to her for further investigation and confirmation. Charline, after a thorough investigation, confirmed the incident and assigned it with an initial priority.

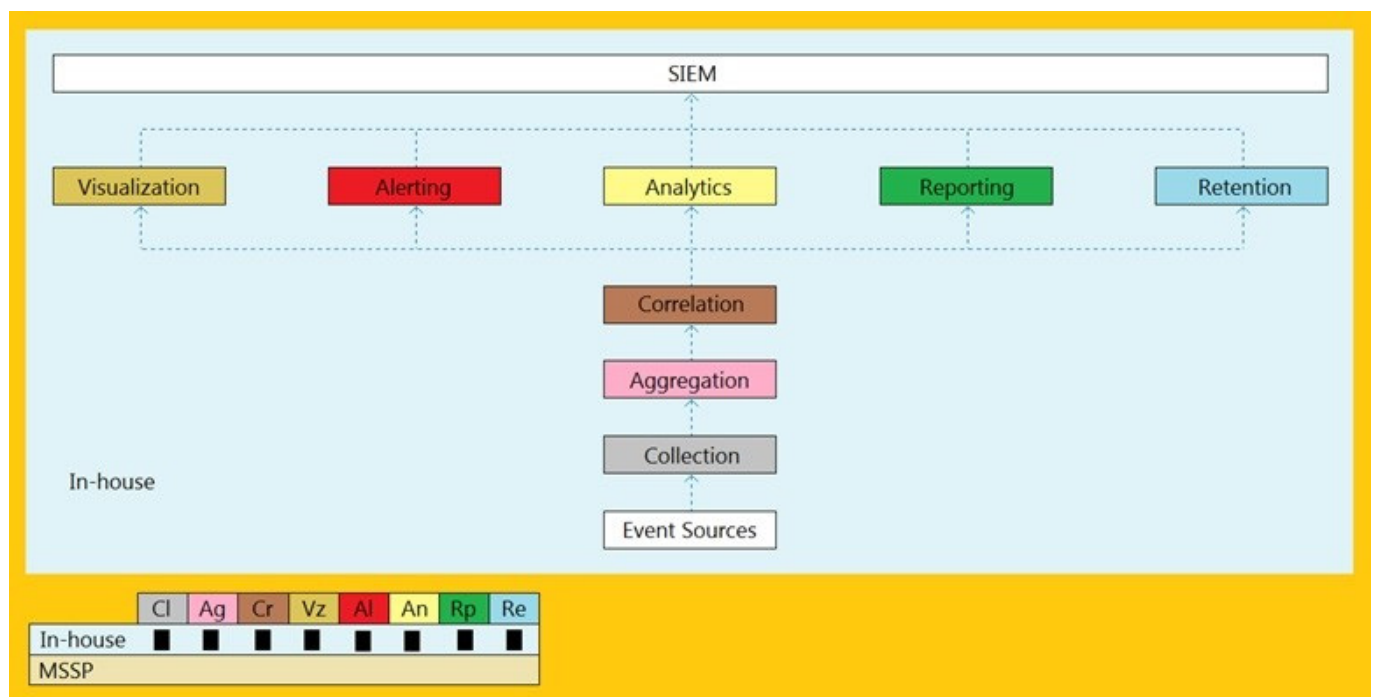
What would be her next action according to the SOC workflow?

- A. She should immediately escalate this issue to the management
- B. She should immediately contact the network administrator to solve the problem
- C. She should communicate this incident to the media immediately
- D. She should formally raise a ticket and forward it to the IRT

Correct Answer: B

QUESTION 5

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