



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

Certified SOC Analyst (CSA)

## Pass Pegasystems 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 Pegasystems Official Exam Center

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





### QUESTION 1

Which of the following threat intelligence helps cyber security professionals such as security operations managers, network operations center and incident responders to understand how the adversaries are expected to perform the attack on the organization, and the technical capabilities and goals of the attackers along with the attack vectors?

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

Correct Answer: D

Reference: <https://info-savvy.com/types-of-threat-intelligence/>

---

### QUESTION 2

Ray is a SOC analyst in a company named Queens Tech. One Day, Queens Tech is affected by a DoS/ DDoS attack. For the containment of this incident, Ray and his team are trying to provide additional bandwidth to the network devices and increasing the capacity of the servers.

What is Ray and his team doing?

- A. Blocking the Attacks
- B. Diverting the Traffic
- C. Degrading the services
- D. Absorbing the Attack

Correct Answer: D

---

### QUESTION 3

What is the correct sequence of SOC Workflow?

- A. Collect, Ingest, Validate, Document, Report, Respond
- B. Collect, Ingest, Document, Validate, Report, Respond
- C. Collect, Respond, Validate, Ingest, Report, Document
- D. Collect, Ingest, Validate, Report, Respond, Document

Correct Answer: A

---



#### QUESTION 4

Properly applied cyber threat intelligence to the SOC team help them in discovering TTPs.

What does these TTPs refer to?

- A. Tactics, Techniques, and Procedures
- B. Tactics, Threats, and Procedures
- C. Targets, Threats, and Process
- D. Tactics, Targets, and Process

Correct Answer: A

Reference: <https://www.crest-approved.org/wp-content/uploads/CREST-Cyber-Threat-Intelligence.pdf>

---

#### QUESTION 5

John as a SOC analyst is worried about the amount of Tor traffic hitting the network. He wants to prepare a dashboard in the SIEM to get a graph to identify the locations from where the TOR traffic is coming.

Which of the following data source will he use to prepare the dashboard?

- A. DHCP/Logs capable of maintaining IP addresses or hostnames with IPtoName resolution.
- B. IIS/Web Server logs with IP addresses and user agent IPtouseragent resolution.
- C. DNS/ Web Server logs with IP addresses.
- D. Apache/ Web Server logs with IP addresses and Host Name.

Correct Answer: D

[312-39 VCE Dumps](#)

[312-39 Practice Test](#)

[312-39 Braindumps](#)