312-39Q&As

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 can help you eliminate the burden of investigating false positives?

A. Keeping default rules

B. Not trusting the security devices

C. Treating every alert as high level

D. Ingesting the context data

Correct Answer: A

Reference: https://stratozen.com/9-ways-eliminate-siem-false-positives/

QUESTION 2

What does Windows event ID 4740 indicate?

A. A user account was locked out.

B. A user account was disabled.

C. A user account was enabled.

D. A user account was created.

Correct Answer: A

Reference: https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4740#:~:text=For%204740(S)%3A%20A,Security%20ID"%20is%20not%20SYSTEM.

QUESTION 3

Which of the following contains the performance measures, and proper project and time management details?

A. Incident Response Policy

B. Incident Response Tactics

C. Incident Response Process

D. Incident Response Procedures

Correct Answer: D

QUESTION 4

Which of the following fields in Windows logs defines the type of event occurred, such as Correlation Hint, Response Time, SQM, WDI Context, and so on?

A. Keywords

B. Task Category

C. Level

D. Source

Correct Answer: A

QUESTION 5

According to the Risk Matrix table, what will be the risk level when the probability of an attack is very high, and the impact of that attack is major?

NOTE: It is mandatory to answer the question before proceeding to the next one.

A. High

B. Extreme

C. Low

D. Medium

Correct Answer: A

Reference: https://onlinelibrary.wiley.com/page/journal/15396924/homepage/special_issue__simple_characterisations_and_communication_of_risks.htm