



312-39^{Q&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 Windows features is used to enable Security Auditing in Windows?

- A. Bitlocker
- B. Windows Firewall
- C. Local Group Policy Editor
- D. Windows Defender

Correct Answer: C

Reference: <https://resources.infosecinstitute.com/topic/how-to-audit-windows-10-application-logs/>

QUESTION 2

John, SOC analyst wants to monitor the attempt of process creation activities from any of their Windows endpoints.

Which of following Splunk query will help him to fetch related logs associated with process creation?

- A. index=windows LogName=Security EventCode=4678 NOT (Account_Name=*\$)
- B. index=windows LogName=Security EventCode=4688 NOT (Account_Name=*\$)
- C. index=windows LogName=Security EventCode=3688 NOT (Account_Name=*\$)
- D. index=windows LogName=Security EventCode=5688 NOT (Account_Name=*\$)

Correct Answer: B

Reference: <https://static1.squarespace.com/static/552092d5e4b0661088167e5c/t/5a3187b4419202f0fb8b2dd1/1513195444728/Windows+Splunk+Logging+Cheat+Sheet+v2.2.pdf>

QUESTION 3

Which of the following security technology is used to attract and trap people who attempt unauthorized or illicit utilization of the host system?

- A. De-Militarized Zone (DMZ)
- B. Firewall
- C. Honeypot
- D. Intrusion Detection System

Correct Answer: C

Reference: <https://www.kaspersky.com/resource-center/threats/what-is-a-honeypot>



QUESTION 4

Robin, a SOC engineer in a multinational company, is planning to implement a SIEM. He realized that his organization is capable of performing only Correlation, Analytics, Reporting, Retention, Alerting, and Visualization required for the SIEM implementation and has to take collection and aggregation services from a Managed Security Services Provider (MSSP).

What kind of SIEM is Robin planning to implement?

- A. Self-hosted, Self-Managed
- B. Self-hosted, MSSP Managed
- C. Hybrid Model, Jointly Managed
- D. Cloud, Self-Managed

Correct Answer: B

QUESTION 5

An organization wants to implement a SIEM deployment architecture. However, they have the capability to do only log collection and the rest of the SIEM functions must be managed by an MSSP.

Which SIEM deployment architecture will the organization adopt?

- A. Cloud, MSSP Managed
- B. Self-hosted, Jointly Managed
- C. Self-hosted, MSSP Managed
- D. Self-hosted, Self-Managed

Correct Answer: C

[312-39 Practice Test](#)

[312-39 Exam Questions](#)

[312-39 Braindumps](#)