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.leads4pass.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

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 2

Identify the attack, where an attacker tries to discover all the possible information about a target network before launching a further attack.

A. DoS Attack

B. Man-In-Middle Attack

C. Ransomware Attack

D. Reconnaissance Attack

Correct Answer: D

Reference: https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-cyber-101july2017.pdf

QUESTION 3

Daniel is a member of an IRT, which was started recently in a company named Mesh Tech. He wanted to

find the purpose and scope of the planned incident response capabilities.

What is he looking for?

A. Incident Response Intelligence

B. Incident Response Mission

C. Incident Response Vision

D. Incident Response Resources

Correct Answer: D

Reference: https://blog.eccouncil.org/phases-of-an-incident-response-plan/

QUESTION 4

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 5

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/