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

Which of the following attacks causes sudden changes in file extensions or increase in file renames at rapid speed?

A. Ransomware Attack

B. DoS Attack

C. DHCP starvation Attack

D. File Injection Attack

Correct Answer: A

Reference: https://www.netfort.com/category/ransomware-detection/

QUESTION 2

Which of the following Windows Event Id will help you monitors file sharing across the network?

A. 7045

B. 4625

C. 5140

D. 4624

Correct Answer: C

Reference: https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=5140

QUESTION 3

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 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

The Syslog message severity levels are labelled from level 0 to level 7. What does level 0 indicate?

A. Alert

B. Notification

C. Emergency

D. Debugging

Correct Answer: B