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

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 2

Which of the following attack inundates DHCP servers with fake DHCP requests to exhaust all available IP addresses?

A. DHCP Starvation Attacks

B. DHCP Spoofing Attack

C. DHCP Port Stealing

D. DHCP Cache Poisoning

Correct Answer: A

Reference: https://www.cbtnuggets.com/blog/technology/networking/what-is-a-dhcp-starvation-attack

QUESTION 3

Which of the following framework describes the essential characteristics of an organization\\'s security engineering process that must exist to ensure good security engineering?

A. COBIT

B. ITIL

C. SSE-CMM

D. SOC-CMM

Correct Answer: C

Reference: https://www.iso.org/standard/44716.html

QUESTION 4

If the SIEM generates the following four alerts at the same time:

I. Firewall blocking traffic from getting into the network alerts

II. SQL injection attempt alerts

III. Data deletion attempt alerts

IV. Brute-force attempt alerts

Which alert should be given least priority as per effective alert triaging?

A. III

B. IV

C. II

D. I

Correct Answer: D

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