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 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

An attacker, in an attempt to exploit the vulnerability in the dynamically generated welcome page, inserted

code at the end of the company\\'s URL as follows:

http://technosoft.com.com/alert("WARNING: The application has encountered an error");.

Identify the attack demonstrated in the above scenario.

A. Cross-site Scripting Attack

B. SQL Injection Attack

C. Denial-of-Service Attack

D. Session Attack

Correct Answer: D

QUESTION 3

Emmanuel is working as a SOC analyst in a company named Tobey Tech. The manager of Tobey Tech recently recruited an Incident Response Team (IRT) for his company. In the process of collaboration with the IRT, Emmanuel just escalated an incident to the IRT.

What is the first step that the IRT will do to the incident escalated by Emmanuel?

A. Incident Analysis and Validation

B. Incident Recording

C. Incident Classification

D. Incident Prioritization

Correct Answer: C

QUESTION 4

Which of the log storage method arranges event logs in the form of a circular buffer?

A. FIFO

B. LIFO

C. non-wrapping

D. wrapping

Correct Answer: A

Reference: https://en.wikipedia.org/wiki/Circular_buffer

QUESTION 5

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/