Splunk SPLK-5001 Practice Questions

Shared by Bishop on 18-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

The United States Department of Defense (DoD) requires all government contractors to provide adequate security safeguards referenced in National Institute of Standards and Technology (NIST) 800-171. All DoD contractors must continually reassess, monitor, and track compliance to be able to do business with the US government.

Which feature of Splunk Enterprise Security provides an analyst context for the correlation search mapping to the specific NIST guidelines?

Options:

A- Comments
B- Moles
C- Annotations
D- Framework mapping

Answer:

D

Question 2

Question Type: MultipleChoice

What is the first phase of the Continuous Monitoring cycle?

Options:

A- Monitor and Protect
B- Define and Predict
C- Assess and Evaluate
D- Respond and Recover

Answer:

B

Question 3

Question Type: MultipleChoice

An analyst is looking at Web Server logs, and sees the following entry as the last web request that a server processed before unexpectedly shutting down:

[51.125.121.100 - [28/01/2006:10:27:10 -0300] "POST /cgi-bin/shurdown/ HTTP/1.0" 200 3304]

What kind of attack is most likely occurring?

Options:

A- Distributed denial of service attack.
B- Database injection attack.
C- Denial of service attack.
D- Cross-Site scripting attack.

Answer:

C

Question 4

Question Type: MultipleChoice

There are different metrics that can be used to provide insights into SOC operations. If Mean Time to Respond is defined as the total time it takes for an Analyst to disposition an event, what is the typical starting point for calculating this metric for a particular event?

Options:

A- When the malicious event occurs.
B- When the SOC Manager is informed of the issue.
C- When a Notable Event is triggered.
D- When the end users are notified about the issue.

Answer:

C

Question 5

Question Type: MultipleChoice

An adversary uses "LoudWiner" to hijack resources for crypto mining. What does this represent in a TTP framework?

Options:

A- Procedure
B- Tactic
C- Problem
D- Technique

Answer:

A

Question 6

Question Type: MultipleChoice

Which option best roles is commonly responsible for selecting and designing the infrastructure and tools that a security analyst utilizes to effectively complete their job duties?

Options:

A- Threat Intelligence Analyst
B- SOC Manager
C- Security Engineer
D- Security Architect

Answer:

D

Question 7

Question Type: MultipleChoice

An analyst is attempting to investigate a Notable Event within Enterprise Security. Through the course of their investigation they determined that the logs and artifacts needed to investigate the alert are not available.

What event disposition should the analyst assign to the Notable Event?

Options:

A- Benign Positive, since there was no evidence that the event actually occurred.
B- False Negative, since there are no logs to prove the activity actually occurred.
C- True Positive, since there are no logs to prove that the event did not occur.
D- Other, since a security engineer needs to ingest the required logs.

Answer:

D