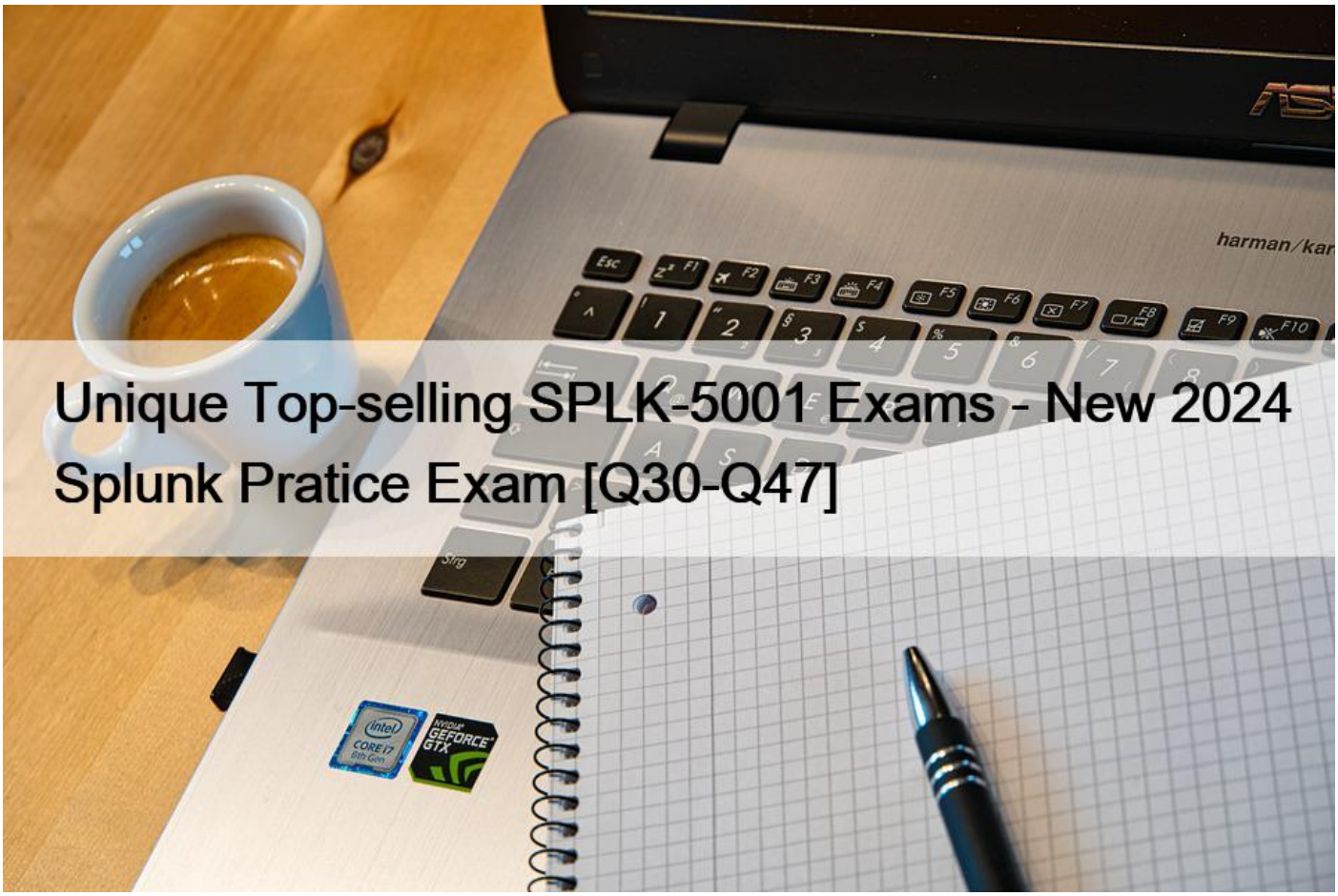
Unique Top-selling SPLK-5001 Exams - New 2024 Splunk Pratice Exam [Q30-Q47



Unique Top-selling SPLK-5001 Exams - New 2024 Splunk Pratice Exam
Cybersecurity Defense Analyst Dumps SPLK-5001 Exam for Full Questions - Exam Study Guide

NO.30 The following list contains examples of Tactics, Techniques, and Procedures (TTPs):

1. Exploiting a remote service

2. Lateral movement

3. Use EternalBlue to exploit a remote SMB server

In which order are they listed below?
* Tactic, Technique, Procedure
* Procedure, Technique, Tactic
* Technique, Tactic, Procedure
* Tactic, Procedure, Technique

NO.31 What is the main difference between hypothesis-driven and data-driven Threat Hunting?
* Data-driven hunts always require more data to search through than hypothesis-driven hunts.
* Data-driven hunting tries to uncover activity within an existing data set, hypothesis-driven hunting begins with a potential activity that the hunter thinks may be happening.
* Hypothesis-driven hunts are typically executed on newly ingested data sources, while data-driven hunts are not.
* Hypothesis-driven hunting tries to uncover activity within an existing data set, data-driven hunting begins with an activity that the hunter thinks may be happening.

NO.32 An analyst is investigating the number of failed login attempts by IP address. Which SPL command can be used to create a temporary table containing the number of failed login attempts by IP address over a specific time period?
* index=security_logs eventtype=failed_login | eval count as failed_attempts by src_ip | sort -failed_attempts
* index=security_logs eventtype=failed_login | transaction count as failed_attempts by src_ip | sort -failed_attempts
* index=security_logs eventtype=failed_login | stats count as failed_attempts by src_ip | sort -failed_attempts
* index=security_logs eventtype=failed_login | sum count as failed_attempts by src_ip | sort -failed_attempts

NO.33 A Cyber Threat Intelligence (CTI) team delivers a briefing to the CISO detailing their view of the threat landscape the organization faces. This is an example of what type of Threat Intelligence?
* Tactical
* Strategic
* Operational
* Executive

NO.34 Upon investigating a report of a web server becoming unavailable, the security analyst finds that the web server’s access log has the same log entry millions of times:

147.186.119.200 – – [28/Jul/2023:12:04:13 -0300] “GET /login/ HTTP/1.0” 200 3733 What kind of attack is occurring?
* Denial of Service Attack
* Distributed Denial of Service Attack
* Cross-Site Scripting Attack
* Database Injection Attack

NO.35 Which of the following is not considered an Indicator of Compromise (IOC)?
* A specific domain that is utilized for phishing.
* A specific IP address used in a cyberattack.
* A specific file hash of a malicious executable.
* A specific password for a compromised account.

NO.36 Which of the Enterprise Security frameworks provides additional automatic context and correlation to fields that exist within raw data?
* Adaptive Response
* Risk
* Threat Intelligence
* Asset and Identity

NO.37 Which of the following is not a component of the Splunk Security Content library (ESCU, SSE)?
* Dashboards
* Reports
* Correlation searches
* Validated architectures

NO.38 Which of the following is a best practice when creating performant searches within Splunk?
* Utilize the transaction command to aggregate data for faster analysis.
* Utilize Aggregating commands to ensure all data is available prior to Streaming commands.
* Utilize specific fields to return only the data that is required.
* Utilize multiple wildcards across fields to ensure returned data is complete and available.

NO.39 Which of the following is a correct Splunk search that will return results in the most performant way?
* index=foo host=i-478619733 | stats range(_time) as duration by src_ip | bin duration span=5min | stats count by duration, host
* | stats range(_time) as duration by src_ip | index=foo host=i-478619733 | bin duration span=5min | stats count by duration, host
* index=foo host=i-478619733 | transaction src_ip |stats count by host
* index=foo | transaction src_ip |stats count by host | search host=i-478619733

NO.40 Splunk Enterprise Security has numerous frameworks to create correlations, integrate threat intelligence, and provide a workflow for investigations. Which framework raises the threat profile of individuals or assets to allow identification of people or devices that perform an unusual amount of suspicious activities?
* Threat Intelligence Framework
* Risk Framework
* Notable Event Framework
* Asset and Identity Framework

NO.41 Which pre-packaged app delivers security content and detections on a regular, ongoing basis for Enterprise Security and SOAR?
* SSE
* ESCU
* Threat Hunting
* InfoSec

NO.42 When searching in Splunk, which of the following SPL commands can be used to run a subsearch across every field in a wildcard field list?
* foreach
* rex
* makeresults
* transaction

NO.43 A successful Continuous Monitoring initiative involves the entire organization. When an analyst discovers the need for more context or additional information, perhaps from additional data sources or altered correlation rules, to what role would this request generally escalate?
* SOC Manager
* Security Analyst
* Security Engineer
* Security Architect

NO.44 Which of the following is the primary benefit of using the CIM in Splunk?
* It allows for easier correlation of data from different sources.
* It improves the performance of search queries on raw data.
* It enables the use of advanced machine learning algorithms.
* It automatically detects and blocks cyber threats.

NO.45 Which of the following data sources can be used to discover unusual communication within an organization’s

network?
* EDS
* Net Flow
* Email
* IAM

NO.46 According to Splunk CIM documentation, which field in the Authentication Data Model represents the user who initiated a privilege escalation?
* username
* src_user_id
* src_user
* dest_user

NO.47 An IDS signature is designed to detect and alert on logins to a certain server, but only if they occur from 6:00 PM – 6:00 AM. If no IDS alerts occur in this window, but the signature is known to be correct, this would be an example of what?
* A True Negative.
* A True Positive.
* A False Negative.
* A False Positive.