Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ----- Guaranteed.

SPLK-3001 MCQs
SPLK-3001 Exam Questions
SPLK-3001 Practice Test
SPLK-3001 TestPrep
SPLK-3001 Study Guide

killexams.com

Splunk

SPLK-3001

Splunk Enterprise Security Certified Admin

ORDER FULL VERSION

https://killexams.com/pass4sure/exam-detail/SPLK-3001

Question: 1066

During an incident response, an analyst finds notable events indicating that a system has been communicating with a known malicious IP address. What should the analyst do first?

A. Notify the incident response team
B. Conduct a full system scan for malware
C. Block the IP address on the firewall
D. Investigate the system's recent activity

Answer: D
Explanation: Investigating the system's recent activity should be the first step to understand the context of the communication with the malicious IP address. This will help determine if the system is compromised and inform the appropriate response actions.

Question: 1067

In a scenario with high availability requirements, what is the optimal prep topology for ES install?

A. Install on indexer
B. Single dedicated search head
C. Cloud auto-scaling
D. Dedicated SHC for ES with deployer and load-balanced search heads

Answer: D
Explanation: For HA, use a dedicated search head cluster for ES, with deployer for consistency and load balancing for analyst access; this is the enterprise-grade prep for critical security operations.

Question: 1068

A glass table is used to monitor user behavior analytics. During a review, an analyst notices a user accessing the system from an unusual location. What should be the next step in the investigation?

A. Ignore it as it may be a legitimate access
B. Confirm the user's identity through additional verification

C. Block the user's access immediately
D. Notify the user's manager for further action

Answer: B
Explanation: The next step should be to confirm the user's identity through additional verification. This approach helps ensure that the access is legitimate before taking further action, such as blocking access or notifying management.

Question: 1069

A Lead Architect wants to create a "Glass Table" that displays a real-time "Security Posture" score alongside a specific "Business Service" health score from ITS**I.** When attempting to add the metric, the architect cannot find the ITSI service. What is the reason for this?

A. Glass Tables cannot cross-reference ITSI data
B. The Glass Table editor only supports ES-native "Security Metrics"
C. The ES and ITSI search heads are not peered
D. The user lacks the "itsi_admin" role

Answer: B
Explanation: While Glass Tables are available in both ES and ITSI, the version within Splunk Enterprise Security is specifically designed to work with "Security Metrics" (notable event counts, risk scores, etc.). To pull ITSI health scores, the dashboard would need to be built in ITSI or use an ad-hoc SPL search to query the ITSI summary index.

Question: 1070

An organization is planning to ingest data from multiple sources into Splunk ES but is concerned about data quality. What is the most effective strategy to ensure high-quality data ingestion?

A. Increase the indexing performance settings
B. Use a single data input for all sources
C. Rely on Splunk's default parsing settings
D. Implement data validation checks at the source

Answer: D
Explanation: Implementing data validation checks at the source is the most effective strategy to ensure high-quality data ingestion. This proactive approach helps identify and rectify data quality issues before they enter the Splunk environment, enhancing overall data integrity.

Question: 1071

Admin sees slow install on virtualized search head. Likely prep miss?

A. Network latency
B. All contribute
C. Insufficient vCPU allocation or no CPU pinning
D. Storage thin provisioning

Answer: B
Explanation: Virtual environments need proper vCPU/RAM/storage prep to avoid install timeouts or slow extraction.

Question: 1072

You are tasked with configuring a local threat intelligence file upload. The file is a CSV containing three columns: `ip`, `description`, and `date`. Which of the following is a strict requirement for Splunk ES to process this file correctly as "Threat Intelligence"?

A. The file must contain a header row that matches CIM threat fields
B. The file must be uploaded via the "Lookup Editor" app first
C. The file must be renamed to `threat_intel.csv` before upload
D. The file must be zipped in a .gz format to be accepted by the parser

Answer: A
Explanation: For the Threat Intelligence Parser to correctly map data from a CSV file into the KV Store collections, the column headers must match the expected field names used by the framework (e.g., `ip`, `domain`, `file_hash`). If the headers are missing or non-standard, the parser will fail to extract the indicators.

Question: 1073

In a large enterprise deployment of Splunk Enterprise Security 8.0, the SOC team observes that the Threat Intelligence Download Manager has failed to ingest a critical STIX 2.1 feed containing 50,000 new malware IOCs due to a misconfigured authentication token. After correcting the token in the Threat Intelligence Framework settings, which tool should the admin immediately use to verify successful ingestion and index the observables into the threat_intel framework while ensuring no duplicate entries are created?

A. Asset and Identity Manager
B. Lookup Editor

C. Threat Download Dashboard
D. Threat Intelligence Audit Dashboard

Answer: C
Explanation: The Threat Download Dashboard provides real-time visibility into the status of all configured intelligence feeds, including authentication errors, download success rates, and parsing outcomes for formats like STIX 2.1. It allows admins to trigger manual downloads, monitor ingestion pipelines, and confirm that new IOCs such as malware hashes or IPs are normalized and stored in the principal threat lookup without duplicates via automatic deduplication rules in the framework. This tool is essential for Security Intelligence as it directly manages the ingestion process before enrichment occurs in correlation searches or investigations.

Question: 1074

A security analyst is tasked with reviewing the current data model configurations in Splunk Enterprise Security. They notice that some models have not been updated in a while. What should be their primary concern regarding these outdated data models?

A. They will automatically update when new data sources are added
B. They cannot be accelerated once they are created
C. They are likely to consume more resources without being useful
D. They may not include the latest security threats and events

Answer: D
Explanation: The primary concern with outdated data models is that they may not include the latest security threats and events, which can hinder the organization's ability to respond effectively to emerging risks. Regular updates are necessary to ensure that data models reflect current security landscapes.

Question: 1075

In a scenario with 100+ glass tables for forensics, performance degrades when loading the navigation menu. What optimization reduces load time?

A. Increase search head resources
B. Categorize menus with sub-menus and limit top-level entries
C. Use static HTML menus instead
D. Disable unused glass tables via ACL

Answer: B
Explanation: Large navigation menus slow loading; categorizing into hierarchical sub-menus for forensics topics optimizes performance while maintaining access.

Question: 1076

Create "Supply Chain Compromise" search: unusual repo clones >5/min from src_ip. Export/import for air-gapped env, with AR email alert. Method?

A. Content pack upload
B. CLI splunk add oneshot, export JSON
C. UI: search, cron=1m, AR "Send Email", export ZIP
D. YAML manifest with action.email.to=secops@

Answer: C
Explanation: Content Management UI: define search | stats dc(repo) as clones by src_ip | where clones>5, 1m schedule, add "Send Email" AR with dynamic fields, export as ZIP for import into air-gapped via Manage Apps > Install.

Question: 1077

In a scenario where multiple detections contribute risk to the same entity simultaneously in ES 8.x, how does the system prevent duplicate findings while preserving all contributing metadata?

A. Manual analyst merging is required
B. All detections generate separate findings regardless of overlap
C. Risk events are discarded if a finding already exists
D. Findings deduplicate based on shared key attributes but aggregate metadata like sources and techniques

Answer: D
Explanation: ES 8.x findings aggregate metadata from multiple contributing detections or intermediate findings, deduplicating where appropriate based on entity and time windows while retaining comprehensive details such as ATT&CK techniques, sources, and scores for full context in investigations.

Question: 1078

An organization has multiple data sources feeding into Splunk ES, but the data from one source is not appearing in the expected dashboards. After validating the data input configuration, the administrator discovers that the data is being indexed but not being tagged correctly. What is the most likely cause of this tagging issue?

A. The indexer is misconfigured
B. The event types are not defined correctly

C. The technology add-on is not properly installed
D. The data source is not configured to send tags

Answer: B
Explanation: The most likely cause of the tagging issue is that the event types are not defined correctly. Event types determine how events are categorized and tagged within Splunk, and if they are improperly defined, events may not appear in dashboards as expected.

Question: 1079

An analyst is reviewing a glass table that shows user activity over the past month. They notice an account that has a high volume of changes to critical configurations. What is the most appropriate action to take?

A. Investigate the user's activity for potential malicious actions
B. Ignore the activity as it may be normal
C. Revoke the user's access immediately
D. Notify the user about the changes

Answer: A
Explanation: Investigating the user's activity for potential malicious actions is the most appropriate action. High volumes of changes to critical configurations can indicate unauthorized or harmful behavior that needs to be addressed promptly.

Question: 1080

During a forensic investigation in Splunk ES, an analyst uses the Intrusion Center dashboard to pivot from a notable event involving a suspicious IP. The swim lanes show endpoint process executions but lack identity information. The admin verifies that the identity lookup is populated correctly via LDAP integration. What is the probable reason for missing identity context in the forensics workflow?

A. The forensics dashboard macros do not include identity enrichment by default for intrusion domains
B. The data model acceleration for Identity Management is incomplete or outdated
C. The asset/identity correlation is disabled in the investigation workflow settings
D. The notable event urgency calculation excludes identity priority in this scenario

Answer: B
Explanation: Forensics dashboards in Splunk ES rely on accelerated data models for efficient pivoting and enrichment; if the Identity Management data model acceleration is incomplete or stale, identity information will not populate in swim lanes or context views even when lookups are correct.

Question: 1081

A security team has configured a correlation search to detect unauthorized access to sensitive files. However, the search is generating too many alerts from users who have legitimate access. What is the most effective way to tune this search?

A. Increase the threshold for alerting
B. Decrease the sensitivity of the correlation search
C. Change the search to focus on specific file types only
D. Implement role-based access controls and adjust the search accordingly

Answer: D
Explanation: Implementing role-based access controls and adjusting the correlation search accordingly ensures that alerts are only generated for users who do not have legitimate access. This tuning method effectively reduces false positives while maintaining the ability to detect unauthorized access.

Question: 1082

In a new ES deployment, the admin is preparing a search head cluster. The deployer and SHC nodes are on Splunk Enterprise 9.2, but app versions differ slightly on some nodes. What must be ensured before staging ES on the deployer?

A. Revert SHC to a clean state by removing all custom apps
B. Only ES version compatibility matters; other apps can differ
C. All other apps on deployer and SHC nodes must have identical versions to avoid bundle push failures
D. Disable app updates on SHC members temporarily

Answer: C
Explanation: SHC requires identical app versions across deployer and members for successful bundle push. Version mismatches cause validation errors or incomplete deployments. This is a critical pre-install preparation step for ES in clustered environments.

Question: 1083

A security analyst in Splunk Enterprise Security 7.3 encounters issues where asset lookups fail to match on 'nt_host' due to domain qualifiers in event data like 'host.domain.com'. To normalize this, you need to configure the lookup to strip domains. What transform configuration achieves this by using a calculated field in the asset_lookup_by_nt_host?

A. Configure FIELDALIAS-nt_host = replace(nt_host,".*\\.","") in props.conf
B. Use REX field=nt_host mode=sed "s/\\..*//g" in automatic lookup

C. Add EVAL-nt_host = mvindex(split(nt_host,"."),0) in transforms.conf
D. Set CALC-nt_host = substr(nt_host,1,index(nt_host,".")) in lookups.conf

Answer: C
Explanation: To normalize hostnames in asset lookups within Splunk Enterprise Security, an EVAL expression in transforms.conf like EVAL-nt_host = mvindex(split(nt_host,"."),0) strips domain qualifiers, ensuring accurate matching and enrichment without domain interference.

Question: 1084

Risk object type "system" accumulates risk slowly. Accelerate?

A. Lower threshold
B. Ignore
C. Apply positive risk factors for server category
D. Add more rules

Answer: C
Explanation: Risk factors modify scores per object type/category (e.g., critical systems) to prioritize in RBA.

Question: 1085

You are preparing to install ES in a highly regulated environment where internet access is blocked. How do you handle the "Threat Intelligence" framework preparation?

A. The ES installation will fail because it cannot reach the Splunk threat servers.
B. You must disable the `threat_intel` modular input before running the installer.
C. You must manually download the threat files and host them on an internal web server.
) You can only use the "Local File" threat source option and must disable all other defaults.

Answer: C
Explanation: Splunk ES expects to download threat intelligence. In air-gapped environments, the preparation involves setting up an internal repository (like a web server) where the files are manually placed, and then configuring ES to pull from those internal URLs.

Question: 1086

A forensics analyst reports that a glass table displaying process injection indicators (e.g., hollow process metrics) loads slowly, with some widgets timing out. The table uses multiple chained searches with | stats

and | lookup commands. What optimization is required for this complex forensics visualization?

A. Move lookups to KV Store acceleration
B. Convert chained searches to single tstats queries using accelerated data models
C. Reduce the number of widgets to under 20 per canvas
D. Increase the glass table refresh interval to 300 seconds

Answer: B
Explanation: Slow-loading glass tables in forensics scenarios with chained searches benefit from conversion to tstats on accelerated models, reducing execution time and avoiding timeouts for complex metrics like process behaviors.

Question: 1087

ES admins note the "Malware Beaconing" correlation search with extreme search enabled generates 150 notables/month unnecessarily due to intermittent network latency. Lab shows context_gen_search running every 5m but primary_search cron="*/10 * * * *". To tune scheduling sensitivity, which paired adjustment optimizes resource use?

A. Change context_gen to "/15 * * * *" and quantity_threshold=0.6
B. Disable extreme search and set urgency=medium
C. Set primary_search to "/20 * * * " and enable throttle window=1800
D. Align both to "0 */1 * * " and set match_threshold=50

Answer: C
Explanation: Scheduling primary_search less frequently at 20-minute intervals reduces overlap with context_gen, mitigating latency-induced mismatches, while a 30-minute throttle window blocks duplicates for grouped events. This tunes sensitivity by lowering execution overhead and notable duplication rates, crucial for extreme searches reliant on timely context data.

Question: 1088

You are analyzing alerts generated by Splunk ES and notice that many alerts are related to the same user account. What is a recommended approach to handle this situation effectively?

A. Conduct a thorough investigation of the user’s activity
B. Disable the user account immediately
C. Increase the alert threshold for that user account
D. Ignore the alerts if they are repetitive

Answer: A

Explanation: Conducting a thorough investigation of the user's activity is essential to determine whether the alerts indicate a legitimate security concern or if they are false positives, allowing for informed decision-making.

Question: 1089

Deployment checklist: Multi-site (SiteA 5 idx, SiteB 3 idx), "Indexing Strategy: Shared es_index across sites, Network_Resolution cross-site >200s". dest lookups fail. Fix?

A. Site-specific es_network_resolution indexes
B. Multisite RF=3 with summary search_factor=1
C. Global acceleration on Network_Resolution 30-day
D. Replicator for index metadata only

Answer: C
Explanation: Accelerating shared data models like Network_Resolution globally with 30-day summaries resolves cross-site dest lookup latency (>200s) in multi-site topologies, per checklist; site-specific fragments data, replicator content-only, RF/SF affect raw HA not summaries, optimizing ES-wide queries.

Question: 1090

A glass table is designed to monitor external threat intelligence feeds. What is the key factor to ensure the data displayed is actionable?

A. Including as many feeds as possible
B. Displaying historical data for context
C. Filtering the data to focus on relevant threats
D. Ensuring the table is updated every minute

Answer: C
Explanation: Filtering the data to focus on relevant threats is essential for ensuring that the information displayed is actionable. This targeted approach allows analysts to prioritize their responses based on the most pertinent threats.

Question: 1091

During an investigation in Splunk ES 8.x, an analyst starts an investigation from a high-risk finding generated by a finding-based detection (FBD) correlated to MITRE ATT&CK Tactic TA0008 (Lateral Movement). The finding groups multiple intermediate findings from risk rules, but the Investigation view shows incomplete artifact enrichment due to missing adaptive response actions on the original risk events.

What configuration ensures automatic enrichment during finding aggregation for faster pivot in complex lateral movement scenarios?

A. Configure adaptive response actions to run on risk rules and stamp additional fields into the risk index for FBD consumption
B. Adjust the data model acceleration to include All_Risk fields in the finding datamodel
C. Enable prompt-driven automation in SOAR to query artifacts post-finding creation
D. Manually run stream capture ARA from the finding menu for each grouped risk object

Answer: A
Explanation: In ES 8.x, finding-based detections aggregate risk events into findings, but enrichment relies on fields stamped during risk rule execution. Configuring ARAs (e.g., lookup enrichment or threat intel matching) on contributing risk rules ensures metadata like MITRE annotations or context fields are available in the risk index, automatically enriching the grouped finding for seamless investigation pivots without manual intervention.

KILLEXAMS.COM

Killexams.com is a leading online platform specializing in high-quality certification exam preparation. Offering a robust suite of tools, including MCQs, practice tests, and advanced test engines, Killexams.com empowers candidates to excel in their certification exams. Discover the key features that make Killexams.com the go-to choice for exam success.

Exam Questions Based on Current Exam Objectives

Killexams.com provides exam questions aligned with the latest official exam objectives and latest syllabus. Our content is reviewed and updated regularly to reflect recent changes announced by certification vendors. By studying these questions, candidates will become cover the structure, difficulty level, and topic coverage of the actual exam, helping them prepare more effectively and efficiently.

Comprehensive Exam MCQs (PDF Format)

Killexams.com offers multiple-choice questions (MCQs) in easy-to-read PDF format, covering all major domains of the exam. Each PDF contains a structured collection of questions and verified answers designed to support focused study. These MCQs help candidates reinforce key concepts, identify knowledge gaps, and improve exam readiness through consistent practice.

Realistic Practice Tests (Online & Desktop)

To support hands-on preparation, Killexams.com provides practice tests through both an Online Test Engine and a Desktop Exam Simulator. These tools are designed to simulate a real exam environment, allowing candidates to practice under exam-like conditions. Performance tracking, test history, and result analysis help users evaluate their progress and focus on areas that need improvement.

Risk-Free Purchase Policy

Killexams.com follows a transparent and customer-friendly purchase policy. If users are not satisfied with the study materials, they may request assistance or a refund in accordance with our published terms and conditions. This policy reflects our commitment to customer satisfaction, fairness, and confidence in our preparation resources.

Regularly Updated Content

Our question bank is reviewed and updated on an ongoing basis to stay aligned with the latest exam outlines and vendor updates. This ensures candidates are studying relevant material and preparing with content that reflects current exam expectations, helping them stay confident and well-prepared.