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

KILL EXAMS

SPLK-5001 MCQs
SPLK-5001 Exam Questions
SPLK-5001 Practice Test
SPLK-5001 TestPrep
SPLK-5001 Study Guide

PASS

killexams.com

Splunk

SPLK-5001

Splunk Certified Cybersecurity Defense Analyst

ORDER FULL VERSION

https://killexams.com/pass4sure/exam-detail/SPLK-5001

Question: 1117

When performing "Outlier Detection" on file execution events, why is it important to normalize process paths?

A. To make the Splunk search run 50% faster.
B. To ensure that `C:\Windows\System32\cmd.exe` and `c:\windows\system32\cmd.exe` are treated as the same entity by the `stats` command.
C. To prevent Splunk from indexing the data.
D. To hide the process names from the end user.

Answer: B
Explanation: Outlier detection relies on accurate counts. If paths are not normalized (e.g., converted to lowercase), Splunk's case-sensitive nature might treat the same process as multiple different entities, skewing the frequency distribution and making it harder to identify true rare events.

Question: 1118

Which Splunk ES commands leverage accelerated CIM for sourcetype assessment?

A. | inputlookup es_content.csv | search recommended_sourcetype
B. | tstats values(sourcetype) from datamodel=Authentication where nodename=* by datamodel
C. Splunk ES Content dashboard > Sourcetype Coverage widget
D. | datamodel Authentication search | stats values(sourcetype) by All_Times.earliest

Answer: B
Explanation: Tstats from accelerated Authentication reveals contributing sourcetypes efficiently. Datamodel search slower sans acceleration, others non-standard or UI-based not command.

Question: 1119

A complex security search involves multiple subsearches to find commonalities between different datasets. The analyst notices that the subsearch is being automatically truncated. What is the default maximum number of results a subsearch can return in Splunk, and what is the best practice if more results are needed?

A. 50,000; use the TRANSACTION command.
B. 10,000; increase the limit in the subsearch using "maxresults".
C. 100; use the APPEND command to combine results.
D. 1,000; use a LOOKUP or JOIN instead if the dataset is large.

Answer: D
Explanation: By default, Splunk subsearches are limited to 1,000 results and a 60-second execution time. If an analyst needs to correlate data across larger sets, subsearches are not the best practice. Instead, they should

look at using the LOOKUP command, Data Model-based TSTATS, or potentially a STATS command that combines multiple sourcetypes and uses conditional logic to correlate.

Question: 1120

SOAR from ES: Triggers incl. (Select all that apply)

A. Manual notable
B. Drilldown
C. Adaptive auto
D. All above but D
E. Risk search

Answer: A,C,E
Explanation: Adaptive, manual, risk; drilldown links not triggers.

Question: 1121

In Splunk ES, an analyst investigating a risk notable notices the Risk Event Timeline visualization shows contributing events with varying calculated_risk_score values, some modified by custom risk factors based on MITRE ATT&CK annotations. The notable originated from the "ATT&CK Tactic Threshold Exceeded for Object Over Previous 7 days" correlation search. Which of the following accurately describes the role of risk factors and how they influence the final risk notable in this scenario?

A. Risk factors replace the need for the Risk Analysis adaptive response action entirely in correlation searches.
B. Risk factors dynamically multiply or adjust the base risk_score of intermediate findings based on conditions like annotations or entity metadata before threshold evaluation, directly impacting whether the risk notable is generated and its displayed score.
C. Risk factors are applied post-notable creation via manual ad-hoc risk entries only and do not affect the initial aggregation in risk incident rules.
D. All risk factors are disabled by default in risk notables, requiring manual override in the Incident Review dashboard for each event.

Answer: B
Explanation: Risk factors dynamically multiply or adjust the base risk_score of intermediate findings based on conditions like annotations or entity metadata before threshold evaluation, directly impacting whether the risk notable is generated and its displayed score because the risk framework uses risk factors (configured via the Risk factor editor) to modify scores at search time using metadata such as MITRE ATT&CK tactics from correlation search annotations, ensuring the aggregated risk for the object in the risk index accurately reflects contextual threat severity before a risk incident rule creates the notable.

Question: 1122

Which of the following best describes the concept of threat hunting?

A. Proactively searching for hidden threats in the environment
B. Implementing security patches to prevent attacks
C. Monitoring network traffic for anomalies
D. Automating responses to detected threats

Answer: A
Explanation: Threat hunting involves proactively searching for hidden threats within an organization's environment. Unlike traditional security measures that react to alerts, threat hunting is a proactive approach to identifying and mitigating threats before they can cause harm.

Question: 1123

A scenario-based question on SIEM best practices: After ingesting new endpoint data that fails to accelerate properly due to missing tags, what corrective actions align with Splunk Enterprise Security operation concepts? (Select all that apply)

A. Rebuild the data model after verifying sourcetype compliance with CIM.
B. Disable acceleration entirely to avoid summary indexing overhead.
C. Use Splunk Security Essentials to assess and recommend content gaps.
D. Add required CIM tags and fields via props.conf and transforms.conf.

Answer: A,C,D
Explanation: Adding required CIM tags and fields via props.conf and transforms.conf, rebuilding the data model after verifying sourcetype compliance with CIM, and using Splunk Security Essentials to assess and recommend content gaps are the corrective actions that align with best practices for CIM, Data Models, acceleration, and threat analysis.

Question: 1124

During a hypothesis-driven hunt for lateral movement, an analyst uses Splunk to model anomalies in SMB traffic. Which SPL commands are most effective for this configuration-based and modeling technique? (Select two)

A. | inputlookup smb_baseline.csv | stats count by src_ip,dest_ip | where count > threshold
B. | from datamodel:Authentication | eval anomaly_score=if(login_time > avg_login_time + 3*stdev,1,0)
C. | search sourcetype=stream:smb | cluster t=smb_command | where cluster_count<5
D. | tstats count from datamodel=Network_Traffic where nodename::action=smb by src,dest | anomaly(mean(count) by src)

Answer: C,D
Explanation: For modeling anomalies in SMB traffic, tstats leverages accelerated data models for efficient time-series anomaly detection on network traffic counts by source and destination, while the cluster command performs behavioral clustering on SMB commands to identify rare configurations indicative of tool usage like Cobalt Strike beacons. Inputlookup is for static IOC matching not dynamic modeling, and the authentication datamodel with eval is unrelated to SMB lateral movement hunting.

Question: 1125

In industry practice, TTPs from a known threat actor are mapped in Splunk ES annotations to help correlate events involving lateral movement via remote service exploitation using a specific tool like EternalBlue. What is the correct hierarchical order of these TTP examples, and their regard in cybersecurity?

A. Tactic only, with techniques and procedures de-emphasized in modern analysis.
B. All treated as equivalent IOCs without hierarchy or industry regard.
C. Procedure first for exact steps, ignoring tactic and technique levels.
D. Lateral movement as tactic, exploitation of remote services as technique, and EternalBlue usage as procedure, regarded as critical for structured threat modeling in frameworks like MITRE ATT&CK.

Answer: D
Explanation: Lateral movement as tactic, exploitation of remote services as technique, and EternalBlue usage as procedure, regarded as critical for structured threat modeling in frameworks like MITRE ATT&CK is the correct order because TTPs follow a hierarchy where tactics are broad goals, techniques are methods to achieve them, and procedures are detailed implementations, and they are highly regarded industry-wide for enabling precise adversary emulation and defensive gap analysis.

Question: 1126

SIEM scale: Best practice for 100 sourcetypes CIM compliance? (Select two)

A. Use Security Essentials audits pre-ingestion
B. Deploy universal TAs per vendor at forwarders/UF
C. Machine learning on raw events pre-CIM
D. Centralize acceleration on 10 core data models only

Answer: A,B
Explanation: TAs ensure vendor sourcetype normalization at edge. Security Essentials validates compliance iteratively. Acceleration post-compliance, ML post-normalization.

Question: 1127

In a scenario involving a state-sponsored adversary targeting critical infrastructure, the attack begins with phishing for credentials (social engineering), progresses to supply chain injection for malware delivery, and culminates in data exfiltration over C2 channels with botnet support for redundancy. The overarching motivation is geopolitical disruption. Select the elements that define the attack types, motivations, and tactics here. (Select all that apply.)

A. Botnet redundancy for C2 and exfiltration as tactics in a supply chain attack motivated by geopolitical objectives
B. Pure DDoS flooding without exfiltration or supply chain as the primary motivation and vector
C. Zero-day exploitation exclusively through email compromise without bot or C2 components
D. Phishing-driven social engineering combined with registry persistence to support account takeover and ransomware

Answer: A,D
Explanation: Botnet redundancy for C2 and exfiltration as tactics in a supply chain attack motivated by geopolitical objectives captures the resilient command infrastructure and data theft in state-sponsored operations. Phishing-driven social engineering combined with registry persistence to support account takeover and ransomware correctly incorporates the initial credential harvesting and endpoint persistence common in such hybrid threats. Pure DDoS flooding without exfiltration or supply chain as the primary motivation and vector does not align with the described exfiltration and supply chain elements. Zero-day exploitation exclusively through email compromise without bot or C2 components overlooks the botnet and broader supply chain aspects.

Question: 1128

An enterprise SOC is benchmarking against common standards and discovers its detections do not leverage Splunk's full framework capabilities for APT detection. A complex scenario requires updating multiple correlation searches. Who owns the task of ensuring annotations cover TTPs from MITRE ATT&CK while aligning with CIS Controls, and what is the benefit to the cyber landscape understanding?

A. No single role owns it; it is automated.
B. The Security Analyst owns it for daily use only.
C. The Security Architect owns only policy writing.
D. The Security Engineer owns the configuration of annotations in savedsearches.conf and security_framework_annotations.csv to map TTPs and controls, benefiting Analysts' understanding of attack vectors in the broader cyber landscape.

Answer: D
Explanation: The Security Engineer owns the configuration of annotations in savedsearches.conf and security_framework_annotations.csv to map TTPs and controls, benefiting Analysts' understanding of attack vectors in the broader cyber landscape because Engineers maintain the technical incorporation of frameworks like MITRE ATT&CK and CIS into Splunk ES, enhancing overall SOC awareness of the cyber landscape, standards, and TTPs.

Question: 1129

A security analyst needs to identify brute-force attempts where a single user logs in from multiple distinct source IPs within a 5-minute window. Which SPL command structure is most efficient for grouping these related events into a single conceptual entity for analysis while maintaining the original event context?

A. `... | bin _time span=5m | stats values(src_ip) as ips by user | where mvcount(ips) > 1`
B. `... | tstats dc(src_ip) where index=auth by user _time span=5m | where 'dc(src_ip)' > 1`
C. `... | transaction user maxspan=5m | search dc(src_ip) > 1`
D. `... | streamstats window=5m dc(src_ip) as ip_count by user | search ip_count > 1`

Answer: C
Explanation: The transaction command is specifically designed to group events that share common characteristics into a single transaction based on constraints like maxspan. While stats is often more performant for counting, transaction is the correct term for creating a single conceptual entity that keeps the raw data of all related events together, which is essential for certain security forensics where the chronological relationship between events in a session matters.

Question: 1130

In the context of continuous monitoring within Splunk Enterprise Security, the five basic stages of investigation according to Splunk emphasize structured progression from initial collection to final remediation. For a scenario involving a Risk Notable from anomalous DNS queries (correlation: | tstats count from datamodel=Network_Resolution where DNS.query=*malicious* by src_ip), the analyst has completed collection and examination but finds the activity benign upon analysis. Which metric would best quantify the efficiency of completing these stages, and how does disposition assignment factor in?

A. Risk score accumulation is the key metric, independent of disposition.
B. MTTA is the primary metric improved by quick disposition regardless of stage completion.
C. MTTD is directly lowered by faster correlation search execution in early stages.
D. Dwell time, calculated as MTTD plus MTTR, is reduced when Benign Positive is assigned promptly.

Answer: D
Explanation: Dwell time, calculated as MTTD plus MTTR, is reduced when Benign Positive is assigned promptly is correct because completing the five basic stages efficiently, including proper disposition assignment for benign activity, minimizes the overall time an alert remains open, directly impacting the breach detection gap metric in analyst performance tracking.

Question: 1131

Which common sourcetypes are recommended for on-prem deployments in Splunk Security Essentials for endpoint threat detection? (Select all that apply)

A. Sysmon:Event for process creation (ID 1)
B. XmlWinEventLog:Security/4663 for object access
C. WinEventLog:Security for auth events
D. aws:cloudtrail for IAM anomalies

Answer: A,B,C
Explanation: WinEventLog:Security captures 4624/4625 logons essential for brute-force and privilege escalation baselines. XmlWinEventLog:Security/4663 detects sensitive object (e.g., registry) access, key for DCSync. Sysmon ID 1 provides rich process lineage (parent/cmdline/hash) for living-off-the-land hunting; aws:cloudtrail is cloud-native, not on-prem.

Question: 1132

In the context of Splunk Enterprise Security, what is the primary purpose of "Identity Correlation"?

A. To encrypt user passwords before they are stored in the index.
B. To synchronize Splunk user roles with Active Directory groups.
C. To prevent users from logging into Splunk with more than one device simultaneously.
D. To link multiple account names (e.g., ssmith, admin_ssmith, ssmith@corp.com) to a single human entity.

Answer: D
Explanation: Identity Correlation within the Asset and Identity framework allows the SIEM to map various usernames and identifiers used across different systems back to one specific person. This is crucial for investigations to see the full scope of an individual's activity across the enterprise.

Question: 1133

ES dashboard for notable | search index=notable | stats sum(risk_score) by rule_name?

A. Incident Review; rule breakdowns
B. Risk Analysis; total scores
C. Both A and B
D. Session Intelligence; only

Answer: C
Explanation: Incident Review stats rule-level noteworthables; Risk Analysis aggregates scores—both display this SPL output.

Question: 1134

When analyzing an incident involving insider threats, which adaptive response actions are most appropriate? (Select All that Apply)

A. Monitor the user's network activity
B. Lock the user's account
C. Allow the user to continue working
D. Inform HR about the incident

Answer: A,B,D
Explanation: Locking the user's account prevents further potential harm, monitoring their network activity provides insights into their actions, and informing HR is essential for addressing the human resources aspect of the incident. Allowing the user to continue working poses a risk to the organization.

Question: 1135

A detection engineer incorporates intelligence on specific adversary procedures, such as custom PowerShell scripts for lateral movement (mapped to MITRE T1021), into custom correlation searches and risk scoring in Splunk ES to improve anomaly detection for upcoming threat hunts. This medium-term intelligence focuses on attack methods rather than active campaigns or board trends. Which tier is applied, and how?

A. Operational threat intelligence solely for immediate campaign response playbooks
B. Strategic threat intelligence limited to geopolitical forecasting
C. Basic IOC feeds without MITRE or procedure details
D. Tactical threat intelligence, enhancing threat analysis by mapping procedures to detections and hunts

Answer: D
Explanation: Tactical threat intelligence, enhancing threat analysis by mapping procedures to detections and hunts is the tier here as it provides technique/procedure details for proactive detection engineering and hunting in Splunk.

Question: 1136

A security team wants to assess their "Data Readiness" for a new set of ransomware detections. Which Splunk tool provides a "Data Source Assessment" specifically to identify gaps in log ingestion for these detections?

A. Splunk Add-on for Microsoft Windows
B. Splunk Enterprise Security
C. Splunk Machine Learning Toolkit
D. Splunk Security Essentials

Answer: D
Explanation: Splunk Security Essentials (SSE) includes a "Data Source Assessment" tool. It allows organizations to see which data sources they currently have, which ones are needed for specific security use cases (like ransomware), and provides guidance on how to onboard the missing data.

Question: 1137

A scenario unfolds with an adversary taking over a user account through phishing, modifying registry for persistence, and then exfiltrating data while maintaining C2. Identify all applicable common terms that define this multi-stage threat actor activity. (Select all that apply)

A. Account takeover via social engineering, registry for persistence, exfiltration, and C2 usage by a threat actor or APT.
B. Pure botnet DDoS without persistence or data theft elements.
C. Isolated email compromise ignoring account and registry aspects.
D. Zero trust model fully preventing supply chain ransomware.

Answer: A
Explanation: Account takeover via social engineering, registry for persistence, exfiltration, and C2 usage by a threat actor or APT define the activity because account takeover uses unauthorized access (often via phishing/social engineering), registry enables persistence, exfiltration steals data, C2 provides control, and threat actor/APT describes the sophisticated entity; this encompasses more than botnet DDoS alone, zero trust preventing ransomware/supply chain, or isolated email compromise.

Question: 1138

You are looking for "Lateral Movement" using WM**I.** You search for events where `process_name=wmiprvse.exe`. Which CIM field would typically contain the "Command Line" arguments used by the WMI process to help you identify the specific malicious script?

A. `command`
B. `args`
C. `process`
D. `cmd_line`

Answer: D
Explanation: In the "Endpoint" CIM model, the standardized field for the full command string executed by a process is `process` (for the name/path) and `process_exec` or `process` again, but most commonly in ES, the field `process` or a custom `cmd_line` is used. However, per Splunk CIM documentation for the "Processes" dataset, the field is specifically `process`. (Correction: In many TAs, it is mapped to `process`, which includes arguments).

Question: 1139

In Splunk Enterprise Security, an analyst is reviewing a notable event triggered by a correlation search for suspicious registry modifications. The event displays mapped annotations including MITRE ATT&CK technique T1547 (Boot or Logon Autostart Execution) and Kill Chain phase for persistence. How do these annotations primarily function within the platform to support investigations?

A. They solely serve as decorative labels without any investigative or enrichment value
B. They limit visibility to only managed annotations and exclude custom analyst inputs
C. They enrich the notable event with framework mappings to facilitate root cause analysis and phase-based threat progression tracking
D. They replace the need for correlation searches by automatically generating risk scores

Answer: C
Explanation: They enrich the notable event with framework mappings to facilitate root cause analysis and phase-based threat progression tracking accurately outlines the core purpose of annotations in Splunk ES, which add context from frameworks like MITRE and Kill Chain to detections for better investigation management.

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.