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

KILL EXAMS

SPLK-5003 MCQs
SPLK-5003 Exam Questions
SPLK-5003 Practice Test
SPLK-5003 TestPrep
SPLK-5003 Study Guide

PASS

killexams.com

Splunk

SPLK-5003

Splunk Certified Cybersecurity Defense Architect

ORDER FULL VERSION

https://killexams.com/pass4sure/exam-detail/SPLK-5003

Question: 1158

A defense contractor must comply with CMMC 2.0 requirements while developing a threat intelligence strategy that leverages open source providers for emerging TTPs and commercial providers for classified threat actor attribution. The Splunk Cybersecurity Defense Architect needs to ensure the strategy includes rigorous evaluation criteria and maintenance automation. Which combined approach best meets CMMC-aligned customization?

A. Establish manual CSV uploads for all intelligence feeds without automation to maintain full control over curation processes in high-security environments
B. Configure native connectors in the Splunk Threat Intelligence Marketplace exclusively for commercial Recorded Future feeds supplemented by scheduled Splunk Add-on for MISP ingestion with custom KV store lookups for OTX data and automated deduplication rules
C. Rely exclusively on open source MISP instances hosted internally without integrating commercial providers to minimize costs and external dependencies
D. Deploy the Threat Intelligence Management module in Splunk Enterprise Security with TAXII 2.1 client configured for MISP open source feeds and API-based ingestion for CrowdStrike commercial data including automated confidence scoring adjustments based on source reliability

Answer: D
Explanation: Deploy the Threat Intelligence Management module in Splunk Enterprise Security with TAXII 2.1 client configured for MISP open source feeds and API-based ingestion for CrowdStrike commercial data including automated confidence scoring adjustments based on source reliability best meets CMMC-aligned customization by embedding evaluation criteria into the ingestion pipeline and providing maintenance automation that supports classified attribution while preserving open source TTP velocity for defense contractor environments.

Question: 1159

What role does "Benchmarking" play in assessing security program effectiveness?

A. Measuring the physical weight of the servers used in the security architecture to ensure they meet floor loading limits.
B. Comparing the organization's security metrics against industry peers to identify relative strengths and weaknesses.
C. Identifying the maximum number of heavy search jobs that can be run on a single Splunk indexer before it crashes.
D. Testing the typing speed of the security analysts to ensure they can enter commands into the terminal quickly.

Answer: B
Explanation: Benchmarking provides external context. If an organization's MTTR is 4 hours, is that good? If the industry average is 24 hours, the program is very effective. If the industry average is 30 minutes, it is not. Benchmarking helps the architect and the business understand their performance in the broader competitive and threat landscape.

Question: 1160

A defense architect overseeing a legacy-heavy power generation facility designs strategies for nonstandard instrumentation to integrate OT data into Splunk Enterprise Security for risk-aligned operations. Which strategy aligns best with architectural requirements?

A. Enable direct index-time parsing on Splunk indexers receiving raw serial data streams from OT devices
B. Install universal forwarders on every legacy RTU device to forward logs over dedicated fiber links
C. Rely on daily batch exports from SCADA master stations ingested via file monitoring inputs on deployment servers

D. Utilize passive optical taps and out-of-band sensor gateways with Splunk Industrial Security add-ons to parse proprietary protocols and enforce CIM compliance at the collection layer

Answer: D
Explanation: Utilizing passive optical taps and out-of-band sensor gateways with Splunk Industrial Security add-ons to parse proprietary protocols and enforce CIM compliance at the collection layer is the most robust strategy for nonstandard legacy environments as it eliminates any risk to critical infrastructure while delivering normalized data essential for effective security operations and threat detection use cases.

Question: 1161

Which of the following is a key benefit of integrating open-source threat intelligence with commercial providers?

A. Simplified processes for intelligence evaluation
B. Reduced costs associated with intelligence acquisition
C. Increased diversity of intelligence sources and perspectives
D. Elimination of the need for internal threat analysis

Answer: C
Explanation: Integrating open-source threat intelligence with commercial providers increases the diversity of intelligence sources and perspectives. This broader view enhances the organization's ability to detect and respond to threats more effectively.

Question: 1162

Within a government agency's Splunk Enterprise Security setup continual testing of security controls reveals gaps in zero-trust implementation. How are these gaps remediated most effectively alongside sustained testing? (Select one.)

A. By conducting standalone Splunk control evaluations disconnected from iterative remediation processes.
B. By maintaining predefined Splunk control parameters independent of testing-derived gap analysis.
C. By using one-time Splunk configuration checks without continuous testing linkage for ongoing gap remediation.
D. By leveraging Splunk risk framework outputs in continuous control tests to detect zero-trust gaps and remediate through iterative policy updates and enhanced identity data model accelerations.

Answer: D
Explanation: By leveraging Splunk risk framework outputs in continuous control tests to detect zero-trust gaps and remediate through iterative policy updates and enhanced identity data model accelerations the gaps are addressed in alignment with testing results ensuring zero-trust controls evolve continuously and remain validated through repeated assessments.

Question: 1163

During the architecture phase for a defense contractor handling classified systems the Splunk Cybersecurity Defense Architect must incorporate governmental directives from NIST publications to influence the design of defense capabilities that support RMF continuous monitoring. Which element of the NIST CSF most directly drives the requirement for Splunk platform features such as adaptive risk dashboards and automated control assessment workflows in this high-stakes

environment?

A. By prioritizing the Respond function using SOAR playbooks exclusively without linking to overarching governmental risk governance directives
B. By establishing the Govern function as the core driver requiring Splunk architectures to include policy-driven risk management oversight and efficacy measurement mechanisms
C. By emphasizing only the Detect function through custom correlation searches without embedding governance structures for risk measurement
D. By restricting design to the Protect function via access control lists while excluding integration with NIST RMF authorization processes

Answer: B
Explanation: By establishing the Govern function as the core driver requiring Splunk architectures to include policy-driven risk management oversight and efficacy measurement mechanisms most directly drives the requirement for Splunk platform features such as adaptive risk dashboards and automated control assessment workflows in this high-stakes environment because NIST CSF guidance publications and related governmental directives mandate that defense capabilities be designed around governance to ensure risk is measured continuously and aligned with organizational objectives across the entire Splunk deployment.

Question: 1164

In the context of cybersecurity incident management, what does the term "playbook" refer to?

A. A collection of training materials for employees
B. A predefined set of procedures for responding to specific incidents
C. A report summarizing recent security incidents
D. A document outlining best practices for security policies

Answer: B
Explanation: A "playbook" in cybersecurity incident management refers to a predefined set of procedures for responding to specific incidents. This helps ensure a consistent and effective response to various types of incidents. The other options describe different aspects of security management but do not specifically refer to response procedures.

Question: 1165

In a network design utilizing east-west microsegmentation with NSX and east-west traffic inspection, Splunk SOAR playbooks for incident response must integrate with VMware tools for VM quarantine and Palo Alto for network blocking. What factor most enables development of these complex automations? (Select all that apply)

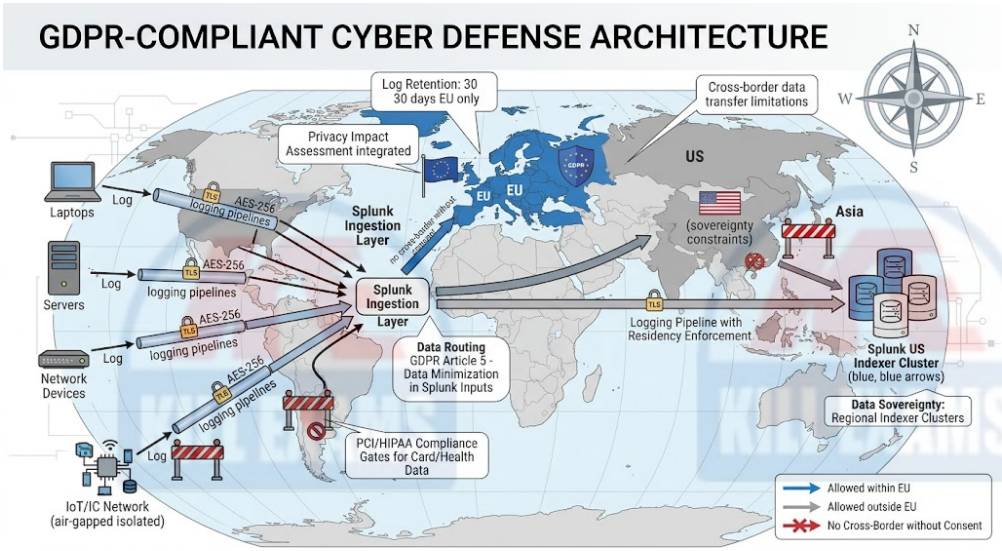
A. Service mesh integration providing observability and retry logic for microsegmented tool communications
B. Flat network without microsegmentation allowing unrestricted calls but compromising zero-trust principles
C. Custom action development using NSX and Palo Alto app APIs with error handling for inspection delays
D. NSX distributed firewall rules explicitly permitting SOAR Automation Broker traffic for quarantine and blocking actions

Answer: A,C,D
Explanation: NSX distributed firewall rules explicitly permitting SOAR Automation Broker traffic for quarantine and blocking actions support the integration without violating microsegmentation. Service mesh integration provides observability and

retry logic for microsegmented tool communications improving reliability. Custom action development using NSX and Palo Alto app APIs with error handling for inspection delays ensures robust playbook execution.

Question: 1166

How regulations like GDPR affect cyber defense architecture in relation to data privacy impact on logging, data sovereignty, and data residency, and how industry standards like PCI, HIPAA, and OT/IC affect it.



A. Allowing unrestricted global data logging to maximize detection coverage regardless of residency.
B. Requiring data residency controls and privacy-preserving logging configurations in Splunk deployments to ensure sovereignty while integrating with industry standards for controls that balance risk and compliance costs.
C. Eliminating logging of sensitive data entirely to comply with privacy laws.
D. Centralizing all data in a single non-compliant region for simplified management.

Answer: B
Explanation: Requiring data residency controls and privacy-preserving logging configurations in Splunk deployments to ensure sovereignty while integrating with industry standards for controls that balance risk and compliance costs is the primary architectural impact of GDPR and similar regulations like PCI/HIPAA because it mandates regional indexers, PII redaction/anonymization in inputs, 30-day EU retention policies, and compliance gates (e.g., for cardholder or health data) that enforce data minimization and sovereignty without eliminating logging—directly influencing Splunk architecture design to support OT/IC isolation and overall risk-offsetting controls within the GRC program, unlike unrestricted global flows, single-region centralization, or total elimination of sensitive data logging which would compromise detection efficacy or violate regulations.

Question: 1167

Risk tolerance caps breach cost at $1M. In Splunk ES, which metric measures program effectiveness?

A. Percentage of logs forwarded with compression enabled
B. Number of Splunk forwarders deployed on endpoints firm-wide
C. Analyst certification completion rates yearly

D. Potential loss avoidance = (breaches prevented * avg breach cost) annually

Answer: D
Explanation: Potential loss avoidance calculates saved value against $1M cap, directly tying metrics to financial risk tolerance for effectiveness reporting. Forwarders, compression, and certifications support but do not measure loss prevention.

Question: 1168

In a scenario where a federal agency is modernizing its Splunk Cybersecurity Defense Architecture to comply with updated governmental risk management directives the architect evaluates how NIST CSF 2.0 influences the inclusion of governance elements. Which specific design principle derived from NIST guidance ensures that defense capabilities incorporate ongoing risk assessment and measurement throughout the Splunk platform lifecycle?

A. By prioritizing multi-site clustering solely for the Recover function while excluding integration with broader governmental directives on risk
B. By applying the Govern function to require Splunk architectures to embed enterprise risk management strategies oversight bodies and continuous monitoring dashboards for defense efficacy
C. By limiting the architecture to Protect function controls using encryption at rest without governance oversight mechanisms
D. By restricting implementation to the Detect function via anomaly detection models in isolation from NIST governance requirements

Answer: B
Explanation: By applying the Govern function to require Splunk architectures to embed enterprise risk management strategies oversight bodies and continuous monitoring dashboards for defense efficacy ensures that defense capabilities incorporate ongoing risk assessment and measurement throughout the Splunk platform lifecycle because NIST CSF guidance publications explicitly influence design by positioning governance as the overarching driver that aligns all defense capabilities with organizational risk tolerance and regulatory expectations.

Question: 1169

Legacy AS/400 monitoring: Nonstandard sensors?

A. Tail /QIBM/UserData logs via UF with props.conf
B. REST API to cloud mirror
C. SNMP only for CPU metrics
D. Vendor dashboard screenshots

Answer: A
Explanation: UF tails QIBM logs with custom props/transforms for fields like user,command, enabling | search command=rm on AS/400, more comprehensive than SNMP or unreliable alternatives.

Question: 1170

A pharmaceutical company audit uncovers prevention gaps in lab system access controls detection incomplete from partial

acceleration response siloed across teams and recovery with short retention windows. Select the mitigation using targeted changes to close gaps while prioritizing R&D innovation budgets. (Select one.)

A. Add access control integrations via SOAR architecture accelerate remaining lab models through ES config unify response via cross-team process matrices and extend retention configs for full recovery coverage.
B. Rely on process documentation updates alone for all gaps perform no architecture or config modifications since lab systems require specialized non-Splunk tools for prevention and detection.
C. Use config changes exclusively for data models ignore process for response and limit architecture to prevention since recovery short windows pose minimal risk to pharmaceutical operations.
D. Implement architecture replacement of ES with open-source alternatives focusing config on response only and deferring prevention recovery as innovation priorities outweigh security gaps.

Answer: A
Explanation: Add access control integrations via SOAR architecture accelerate remaining lab models through ES config unify response via cross-team process matrices and extend retention configs for full recovery coverage because access integrations close prevention acceleration addresses detection unification enhances response and retention extension completes recovery allowing budget preservation for R&D innovation.

Question: 1171

A cybersecurity architect is implementing a threat intelligence strategy that uses both open-source (OSINT) and commercial feeds. The objective is to calculate a "Source Reliability Score" for each provider. If a provider's indicators consistently result in notable events that are marked as "False Positive" by analysts, the system should automatically lower the weight of that provider. How should this be designed in Splunk ES?

A. By configuring the Threat Intelligence Management module to automatically delete any feed that produces more than ten false positives in a single 24-hour window.
B. By creating a search that analyzes the 'incident_review' KV store for 'false_positive' tags and maps them back to the 'threat_group' field in the threat intelligence collection.
C. By manually reviewing the analyst notes on every notable event and typing a new reliability score into a text file that the Splunk search head reads every morning.
D. By assigning the same "Default Weight" to all providers and ignoring the analyst feedback, as technical indicators are more objective than human analyst interpretations.

Answer: B
Explanation: A mature intelligence lifecycle includes a feedback loop from the "Curation" and "Operations" stages back to the "Evaluation" stage. By programmatically linking the outcome of security investigations (Notable Events in ES) back to the sources of the intelligence that triggered them, an architect can objectively measure the quality of each feed. This allows for the automated or semi-automated adjustment of source weights, ensuring that the most reliable intelligence drives the most critical alerts.

Question: 1172

(Select all that apply)
For coordinating a DDoS attack response impacting e-commerce, which processes in Splunk integrate with ITIL continual service improvement for post-incident lessons learned?

A. Correlation search tuning linked to service improvement plans
B. Manual AAR reports uploaded to Splunk content library
C. SOAR retrospective playbooks with CSI register updates
D. ES metrics exported to ITSM CSI dashboards automatically

Answer: A,C,D
Explanation: Splunk SOAR retrospective playbooks feed CSI registers, ES metrics auto-export to ITSM CSI dashboards, and tuned correlation searches link to SIPs, embedding IR into ITIL CS**I.** Manual AAR uploads lack automation, hindering scalable DDoS coordination.

Question: 1173

How can an organization ensure that its cybersecurity policies remain effective and relevant over time?

A. By maintaining static policies that do not change.
B. By relying solely on external audits for policy updates.
C. By reviewing and updating policies only when a breach occurs.
D. By conducting regular assessments and incorporating feedback.

Answer: D
Explanation: Conducting regular assessments and incorporating feedback are essential for ensuring that cybersecurity policies remain effective and relevant over time. Policies should be dynamic and adaptable to changing threats and business conditions, rather than being static or only reviewed after incidents.

Question: 1174

An architect is comparing NetFlow data with full packet capture (PCAP) for a high-volume network link. The primary goal is to identify a long-term trend of data staging prior to exfiltration. Which source is more appropriate for this specific goal?

A. PCAP, because the architect needs to see the actual content of the files being moved between servers.
B. PCAP, because it has lower storage requirements than NetFlow for the same duration of time.
C. NetFlow, because it includes the full payload of the packets allowing for deep content inspection.
D. NetFlow, because it provides a compact summary of traffic volumes and durations over long periods.

Answer: D
Explanation: NetFlow is a high-signal, low-volume source that is perfect for long-term trend analysis. While it doesn't show the "what" (payload), it shows the "how much" and "how long," which is sufficient to identify the staging of large amounts of data without the massive storage costs of PCAP.

Question: 1175

Continuous testing flags SIEM coverage gaps. Effectiveness metric?

A. Total GB of logs ingested per Splunk indexer daily
B. Number of custom TA apps installed

C. Coverage remediation cycle time from gap ID to full ingest
D. Search concurrency limits configured

Answer: C
Explanation: Cycle time quantifies testing-to-remediation speed, measuring program effectiveness. Ingest volume, TAs, and limits are infrastructural.

Question: 1176

For a company operating in the Energy sector, the OT/IC security frameworks (like NERC CIP) often require "Access Recovery" capabilities. How does a clustered Splunk architecture support this requirement?

A. By requiring that all passwords be written on a physical piece of paper and stored in a locked safe that only the CEO can access.
B. By disabling all network connections to the Splunk cluster during an incident to ensure that the data cannot be corrupted by external hackers.
C. By providing a single point of failure where all data is stored on one disk, making it easier to find the data during a recovery operation.
D. By using indexer clustering and search head clustering to provide high availability and data redundancy, ensuring the SOC can always access data.

Answer: D
Explanation: High availability and disaster recovery are essential for critical infrastructure. Frameworks like NERC CIP mandate that security monitoring must be resilient. In Splunk, clustering ensures that if one server (or even a whole site) fails, the data remains available for searching and alerting. This redundancy ensures that the defense architecture can continue to operate and support "Access Recovery" of security events even during a significant system failure or cyberattack.

Question: 1177

A security architect is building a workflow to automate the investigation of suspected data exfiltration. The process involves querying Splunk Enterprise for traffic logs, checking an external Threat Intelligence Platform (TIP), and then querying an EDR tool to check for unusual process activity on the source host. Which factor represents a technical architecture constraint on the "investigation" phase of this workflow?

A. The use of different data formats (JSON vs XML) between the EDR and the TIP, requiring complex transformation.
B. The total number of analysts currently logged into the Splunk SOAR web interface during the automated execution.
C. The requirement for the SOAR platform to have a specific license level to enable the multi-threading of API calls.
D. The presence of SSL inspection middleboxes that might block the SOAR platform's API calls to external cloud TIPs.

Answer: D
Explanation: Network design elements like SSL/TLS inspection proxies are significant constraints for security orchestration. If the technical architecture intercepts and inspects outbound traffic, it may break the certificate chain or block the API requests that the SOAR platform sends to external services like Threat Intelligence Platforms. The architect must ensure that the orchestration platform’s traffic is either bypassed or that the proper certificates are installed to enable seamless cross-platform communication.

Question: 1178

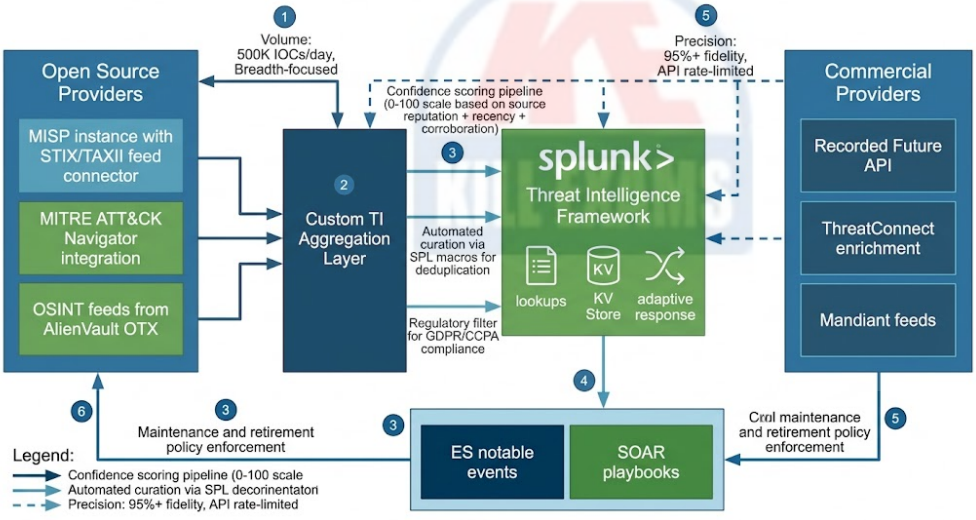
For a banking institution with complex regulatory and business needs the Splunk Cybersecurity Defense Architect evaluates methodologies for selecting technologies that integrate with existing identity management systems. Which methodology ensures comprehensive alignment?

A. Focus selection exclusively on cost reduction metrics disregarding regulatory and integration requirements
B. Select technologies using only technical specifications without business stakeholder input or landscape assessment
C. Recommend immediate full deployment of all modules without prior methodology-driven evaluation
D. Apply a capability selection framework that assesses business needs technology landscape and security controls through workshops and Splunk Security Essentials assessments before finalizing Enterprise Security and SOAR selections

Answer: D
Explanation: Apply a capability selection framework that assesses business needs technology landscape and security controls through workshops and Splunk Security Essentials assessments before finalizing Enterprise Security and SOAR selections is the correct methodology for selecting security technologies aligned to business need organizational technology landscape and security controls.

Question: 1179

In a global financial institution with hybrid cloud infrastructure and stringent data sovereignty regulations, the security architect must develop a customized threat intelligence strategy that leverages both open source providers for broad coverage of emerging TTPs and commercial providers for high-fidelity IOCs on nation-state actors. The strategy requires automated ingestion, deduplication, and confidence-based prioritization to feed directly into Splunk Enterprise Security correlation searches.



A. Implement standalone commercial feeds only via direct API to Splunk lookups without open source integration, relying solely on vendor-provided scoring to minimize custom development overhead in high-volume environments.
B. Deploy a federated TI platform using MISP for open source STIX/TAXII ingestion combined with commercial API connectors in Splunk ES, applying weighted confidence scoring (70% commercial + 30% OSINT) and automated SPL-based curation macros for regulatory-compliant prioritization before enrichment in threat objects.
C. Use a third-party aggregator service for all feeds without direct Splunk integration, exporting aggregated IOCs weekly via

scheduled exports instead of real-time streaming for simplicity.
D. Rely exclusively on open source MISP with manual CSV uploads to Splunk, bypassing commercial providers to reduce costs while using basic field extractions for IOC matching without confidence weighting.

Answer: B
Explanation: The optimal implementation approach deploys a federated TI platform using MISP for open source STIX/TAXII ingestion combined with commercial API connectors in Splunk ES, applying weighted confidence scoring (70% commercial + 30% OSINT) and automated SPL-based curation macros for regulatory-compliant prioritization before enrichment in threat objects because it directly addresses the need for balanced customization across provider types while embedding intelligence lifecycle elements like scoring and curation into Splunk-native workflows for real-time operational use.