Splunk SPLK-5003 Dumps

Shared by Rasmussen on 11-11-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Review the output shown below.

```
Host is up (0.00013s latency)
Not shown 995 closed ports
PORT        STATE   SERVICE
22/tcp      open    ssh
23/tcp      open    telnet
80/tcp      open    http
3128/tcp    open    squid-http
3389/tcp    open    ms-term-serv

Nmap done: 1 IP address (1 host up) scanned in 0.05 seconds
```

What should be the first action taken to harden this host?

Options:

A- Verify if running services are necessary.
B- Implement two-factor authentication for telnet.
C- Turn off host based file integrity checking.
D- Turn on modsecurity for the http service.

Answer:

A

Explanation:

The exhibit shows an Nmap scan identifying five open TCP ports: 22 (SSH), 23 (Telnet), 80 (HTTP), 3128 (Squid HTTP proxy), and 3389 (Microsoft Terminal Services).

These open ports represent potentially accessible services that must be evaluated against the system's intended operational purpose.

The first hardening action should be to verify whether each running service is necessary.

This follows the principle of least functionality, which requires systems to provide only essential capabilities and restrict unnecessary services, ports, and protocols.

NIST SP 800-53 control CM-7 establishes this principle as part of secure configuration

management.

Telnet is particularly concerning because conventional Telnet does not provide encryption for authentication credentials or session contents. If remote administration is required, SSH or another appropriately secured alternative should normally be preferred.

The Squid proxy service and remote desktop access should also be examined to determine whether they are authorized and appropriately restricted.

Implementing multifactor authentication for Telnet does not resolve the underlying insecure transport protocol.

Disabling file-integrity checking would remove a potentially valuable defensive control.

ModSecurity may provide additional HTTP protection, but implementing it before evaluating service necessity would be premature.

The correct initial process is to establish the required service baseline, disable unnecessary functionality, and then harden the remaining services.

Question 2

Question Type: MultipleChoice

Patrick leads a security operations team of six analysts that must provide 24-hour-per-day coverage. The team is continually overwhelmed by the number of security events they must triage, analyze, and respond to each day. Patrick wants the team to focus on the most critical incidents rather than be distracted by low-priority events. His leadership team agrees to increase the budget to hire one additional person.

What is the best way for Patrick to allocate the budget?

Options:

A- Hire a third party incident response firm to supplement the team during major incidents.
B- Hire a detection engineer to create detection content for more security tools.
C- Hire one more full-time analyst to float between a different shift each day.
D- Hire a SOAR engineer to develop new playbooks for automating responses.

Answer:

D

Explanation:

The SOC's primary constraint is excessive manual triage and response activity rather than a lack of detection content.

Hiring a SOAR engineer can provide organization-wide productivity benefits by automating repetitive workflows that currently consume analysts' time.

Splunk SOAR supports playbooks for enrichment, investigation, containment, and response activities across integrated security technologies.

For example, automated workflows can retrieve endpoint details, enrich suspicious IP addresses, correlate related identity activity, and prepare findings for analyst review.

This enables analysts to concentrate on high-priority incidents requiring judgment, contextual assessment, and complex investigation.

A properly designed automation program should also incorporate safeguards, approval requirements, exception handling, and performance monitoring.

Hiring another detection engineer may increase the number of alerts without resolving the existing processing bottleneck.

Adding one analyst provides additional capacity but may not significantly improve efficiency across all shifts.

External incident-response services can assist during major incidents but do not directly reduce routine daily alert-handling work.

However, one additional SOAR engineer does not solve the organization's 24-hour staffing problem. Six analysts may already be insufficient for sustainable round-the-clock coverage once leave, breaks, and training are considered.

Patrick should separately evaluate minimum staffing requirements and workload distribution.

Among the listed options, SOAR engineering offers the strongest potential to reduce repetitive work at scale.

Official reference / study topic: Splunk SOAR, Use Playbooks to Automate Analyst Workflows and Create Playbooks.

==========

Question 3

Question Type: MultipleChoice

Which of the following describes the benefits of modern cybersecurity-defense data architectures that use technologies such as data fabric, data lakes, message bus, and federated search?

Options:

A- They use local storage on each security appliance to reduce network traffic and eliminate the need for search capabilities.
B- They protect and isolate security data ensuring safe data sharing.
C- They distribute data storage and processing, enabling different teams to manage and consume data as needed to meet their use cases.
D- They centralize all security data into a single repository to reduce complexity and improve access speed.

Answer:

C

Explanation:

Modern cybersecurity data architectures increasingly separate data collection, processing, storage, and consumption to support diverse operational requirements without forcing every workload into one centralized platform.

A data lake provides scalable storage for large volumes of structured and unstructured information.

A message bus enables event producers to distribute telemetry to multiple consumers through decoupled communication mechanisms.

A data fabric provides architectural capabilities for integrating, governing, and accessing data across heterogeneous systems.

Federated search enables authorized users to query supported remote datasets through a common search interface without necessarily migrating the underlying information.

Splunk Federated Search supports querying remote datasets through documented federation options, enabling organizations to obtain insights across distributed information environments.

These technologies can support security operations, threat hunting, forensic investigations, compliance reporting, and analytical workloads with different performance and retention requirements.

For example, high-priority alerts may remain in a fast-search environment while large historical telemetry datasets are retained in more economical storage.

Option A eliminates search functionality, which contradicts investigative requirements.

Option B describes a possible security objective but does not capture the principal architectural advantage.

Option D incorrectly assumes that modern architectures require centralizing every dataset.

The defining benefit is flexible, governed, and scalable data distribution and consumption.

Official reference / study topic: Splunk, Overview of Federated Search Options for the Splunk Platform.

==========

Question 4

Question Type: MultipleChoice

The increasing rate of cyberattacks has caused many countries to enact laws and regulations concerning the collection, handling, and protection of their citizens' private information, regardless of where it is stored.

Which term best describes these laws?

Options:

A- Data residency
B- Data sovereignty
C- Data shielding
D- Data providence

Answer:

B

Explanation:

Data sovereignty concerns the application of legal and regulatory authority to data, including requirements governing its collection, processing, access, protection, storage, and transfer.

The concept is particularly important for multinational organizations because information may be subject to legal obligations arising from the location of individuals, processing activities, service providers, or applicable jurisdictions.

For example, GDPR can apply to organizations outside the European Union when their activities meet specified territorial-scope conditions.

An organization cannot assume that relocating personal information to infrastructure in another country automatically removes applicable privacy obligations.

Data sovereignty considerations therefore influence cloud architecture, contractual arrangements, cross-border transfers, government-access requirements, and the selection of service providers.

Data residency, option A, refers more specifically to the geographic location where information is stored or processed.

Residency requirements may be one mechanism used to satisfy applicable legal obligations, but physical location and legal jurisdiction are not identical concepts.

Data shielding is not the standard term for the complete set of laws described.

Data providence is not the recognized legal concept in this context.

It is also important to distinguish data sovereignty from an unrestricted claim that every country's laws automatically apply to all information concerning its citizens everywhere. Legal applicability depends on the relevant statute and its jurisdictional provisions.

Official reference / study topic: Splunk Cybersecurity Defense Architect: Governance Risk and Compliance, Data Sovereignty and Residency.

==========

Question 5

Question Type: MultipleChoice

Which option best explains how data science, machine learning, behavioral analysis, and AI enhance threat detection over traditional detection methods?

Options:

A- They rely on defined rules and signatures to identify threats.
B- They rapidly integrate with legacy SIEM infrastructure to identify threats.
C- They escalate anomalies based on static thresholds to identify threats.
D- They highlight anomalies, relationships, and unique patterns to identify threats.

Answer:

D

Explanation:

Data science, machine learning, behavioral analysis, and artificial intelligence extend traditional security detection by identifying complex relationships and deviations that predefined signatures may not recognize.

Traditional signature-based approaches are effective when suspicious activity matches known indicators, established rules, or explicitly configured conditions.

However, sophisticated attackers may use previously unseen tools, legitimate administrative utilities, and low-frequency activity that does not match existing detection signatures.

Machine-learning techniques can analyze large datasets to identify unusual authentication patterns, abnormal network traffic, unexpected process behavior, and statistically significant deviations from established baselines.

Behavioral analysis can compare current activity with historical patterns associated with users, devices, applications, or other entities.

For example, an account that suddenly accesses unfamiliar infrastructure, performs unusual administrative operations, and transfers significantly more data than normal may require investigation even when no individual event matches a known malicious signature.

Splunk Machine Learning Toolkit supports statistical analysis and machine-learning workflows that can complement conventional correlation searches.

These capabilities are not inherently reliable without appropriate training data, validation, and ongoing tuning.

Option A describes traditional rule-based detection. Option B concerns platform integration, while option C emphasizes fixed thresholds rather than adaptive analysis.

Option D accurately captures the primary analytical advantage.

Official reference / study topic: Splunk Machine Learning Toolkit, Advanced Security Analytics and Behavioral Detection.

==========

Question 6

Question Type: MultipleChoice

What is a Software Bill of Materials (SBOM)?

Options:

A- A contract for purchasing software licenses annually
B- A list of dependencies a user must download in addition to a piece of software
C- A list of third-party components contained within a piece of software
D- An invoice for commercial software license renewal

Answer:

C

Explanation:

A Software Bill of Materials (SBOM) is a structured inventory identifying the software components and dependencies incorporated into a particular software product.

Its primary objective is to improve transparency into software composition, supporting vulnerability management, software supply-chain assurance, procurement evaluation, and license governance.

An SBOM may identify open-source packages, third-party libraries, commercial components, dependency relationships, component versions, and relevant producer information.

CISA's software transparency guidance establishes expectations for component identification and structured information exchange.

For example, when a vulnerability is disclosed in a widely used software library, organizations can examine available SBOM records to identify applications containing potentially affected versions.

This enables more targeted vulnerability assessment and remediation.

Option C is the closest definition because third-party software components are central to SBOM transparency.

However, an SBOM is not necessarily limited to third-party components. Depending on the format and generation method, it may also represent first-party components and additional software relationships.

Option B is too narrow because an SBOM describes components incorporated into the software, not merely files users must download separately.

Options A and D concern commercial licensing documents rather than software composition.

An SBOM does not independently demonstrate that software is secure; its usefulness depends on

accuracy, completeness, freshness, and integration with security processes.

Official reference / study topic: CISA, Software Bill of Materials FAQ and Framing Software Component Transparency.

==========

Question 7

Question Type: MultipleChoice

Which of the following should be the initial step when developing an effective integration strategy for diverse security data sources in a security operations center (SOC)?

Options:

A- Begin collecting available logs from all systems.
B- Evaluate security information and event management (SIEM) systems.
C- Hire a team of data engineers to manage the integrations.
D- Define the security use cases and operational requirements that the data will support.

Answer:

D

Explanation:

An effective security data-integration strategy begins with identifying the security outcomes the organization needs to achieve.

These requirements should be expressed through documented detection, investigation, compliance, operational monitoring, and threat-hunting use cases.

For example, detecting suspicious privileged account activity may require authentication events, identity-management records, administrative changes, and asset context.

Once the use case is defined, the architect can determine which data sources, fields, collection mechanisms, retention periods, and normalization requirements are necessary.

This approach prevents indiscriminate ingestion and reduces the risk of investing in expensive data pipelines that do not deliver meaningful security value.

Splunk's Common Information Model supports standardized analytics across diverse data

sources, but the necessary field mappings and integrations should be selected according to specific analytical requirements.

The strategy should also address event latency, source reliability, data quality, access restrictions, and operational ownership.

Beginning by collecting every available log can introduce unnecessary ingestion costs and excessive data-management complexity.

Selecting SIEM products before defining requirements risks choosing technology that does not adequately support intended workflows.

Hiring engineering personnel may eventually be necessary, but staffing decisions should follow an understanding of the integration scope.

A requirements-driven approach therefore provides the strongest foundation for scalable and effective SOC data integration.

Official reference / study topic: Splunk Common Information Model, Security Data Integration and Use-Case-Driven Planning.

==========

Question 8

Question Type: MultipleChoice

Which of the following are standard capabilities of a Threat Intelligence Platform (TIP)?

Choose three

Options:

A- Automated report correlation
B- Stores forensic images
C- Capability of high-volume indicator storage
D- Built-in sharing functionality

Answer:

A, C, D

Explanation:

A Threat Intelligence Platform (TIP) provides centralized capabilities for collecting, organizing, correlating, enriching, and distributing cyber threat intelligence.

Automated report correlation enables intelligence records from different sources to be associated through shared indicators, adversary identities, campaigns, malware families, and other relevant attributes.

This helps analysts identify relationships that might otherwise require extensive manual research.

High-volume indicator storage is an important TIP capability because intelligence feeds may contain large numbers of IP addresses, domains, URLs, file hashes, and other indicators.

The platform must support efficient indicator management, deduplication, confidence assessment, and lifecycle handling.

Built-in sharing functionality enables approved intelligence to be distributed to internal security platforms, operational teams, and authorized external partners.

Standards such as STIX and TAXII can support structured intelligence exchange between compatible systems.

Splunk Intelligence Management provides intelligence aggregation, normalization, enrichment, prioritization, and operational distribution capabilities.

Forensic image storage, option B, is not a standard TIP function.

Disk images and memory captures require appropriate digital-evidence storage, integrity protection, access controls, and chain-of-custody procedures.

A TIP may reference forensic evidence or consume indicators extracted from it, but it is not principally designed to function as a forensic evidence repository.

Therefore, A, C, and D identify the relevant platform capabilities.

Official reference / study topic: Splunk Intelligence Management, Threat Indicator Storage, Correlation, Enrichment and Sharing.

==========

Question 9

Question Type: MultipleChoice

During a SOC process and workflow review, the SOC manager notes that analysts spend considerable time moving among the EDR, remote access, and IAM consoles to add context to a

finding.

Which of the following would reduce the time to resolution with these concerns in mind?

Options:

A- Automate the vulnerability scanning for the entity in the related finding.
B- Automate the initial triage and present results in the related finding.
C- Automate the quarantine of the entity in the related finding.
D- Automate the incident reporting in the related finding.

Answer:

B

Explanation:

The scenario identifies inefficient manual enrichment and investigation workflows as the primary operational problem.

Analysts must repeatedly access Endpoint Detection and Response (EDR), remote-access, and Identity and Access Management (IAM) platforms to collect contextual information about security findings.

Automating initial triage directly addresses this inefficiency by gathering relevant evidence and presenting it within the associated finding.

A SOAR playbook can query integrated security platforms to retrieve endpoint details, account information, authentication activity, network context, and relevant threat-intelligence attributes.

These results can then support faster incident classification, prioritization, and investigation.

Splunk SOAR playbooks are designed to automate analyst workflows through integrated applications and predefined actions.

Splunk Enterprise Security also supports enrichment of findings using asset and identity information.

For example, an analyst investigating a suspicious login could receive the affected user's identity attributes, recent authentication history, endpoint status, and associated network observations without manually querying multiple consoles.

Option A introduces vulnerability scanning, which does not directly address the identified workflow bottleneck.

Option C may provide containment but is premature when the primary requirement is gathering

context.

Option D improves reporting efficiency rather than initial investigation.

Therefore, automated triage with results presented in the relevant finding is the most effective solution.

Official reference / study topic: Splunk SOAR, Playbooks and Automation Rules for Enterprise Security Findings.

==========

Question 10

Question Type: MultipleChoice

Which categories of SOAR playbooks are commonly used in a security operations center?

Choose three

Options:

A- Attack
B- Endpoint
C- Phishing
D- Enrichment

Answer:

B, C, D

Explanation:

Security Orchestration, Automation, and Response (SOAR) platforms organize automation workflows around common investigation, enrichment, and response use cases.

Endpoint playbooks automate activities involving workstations, servers, and endpoint security platforms. Examples include retrieving endpoint information, examining suspicious processes, collecting relevant artifacts, and isolating compromised devices.

Phishing playbooks support the investigation and containment of suspicious email messages. They may extract message artifacts, analyze attachments, inspect URLs, retrieve reputation information, and coordinate approved email-remediation actions.

Enrichment playbooks add contextual information to security observations. This may include IP reputation, domain intelligence, file-hash analysis, identity attributes, asset information, and related historical activity.

Splunk Security Content explicitly organizes published SOAR playbooks into use-case categories including Endpoint, Phishing, and Enrichment.

These categories provide reusable automation capabilities that can be integrated into larger security investigation and remediation workflows.

Although SOAR may automate responses to attacks, Attack is not one of the standard playbook categories in the relevant Splunk Security Content taxonomy.

The distinction is important because playbooks describe specific workflows and actions rather than merely naming the presence of hostile activity.

A mature SOAR implementation should combine these categories according to incident type, integration availability, operational requirements, and approved response procedures.

Official reference / study topic: Splunk Security Content, SOAR Use Cases: Endpoint, Phishing and Enrichment.

==========

To Get Premium Files for SPLK-5003 Visit
https://www.p2pexams.com/products/splk-5003

For More Free Questions Visit
https://www.p2pexams.com/splunk/pdf/splk-5003

