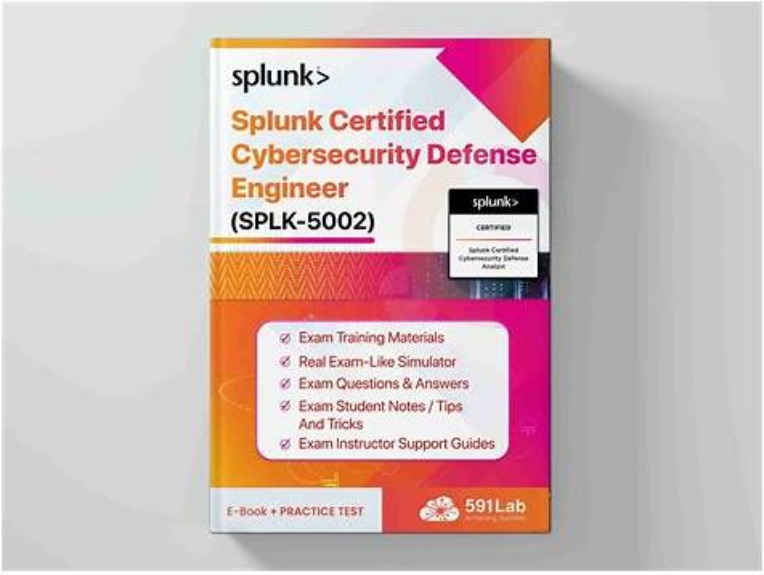
SPLK-5002認證考試 - SPLK-5002學習資料



2026 NewDumps最新的SPLK-5002 PDF版考試題庫和SPLK-5002考試問題和答案免費分享：https://drive.google.com/open?id=1pJBRNdb-ASJLBjV6vj5KMjG2TT6sh3sH

NewDumps的SPLK-5002考古題的命中率很高，可以幫助大家一次通過考試。這是經過很多考生證明過的事實。所以不用擔心這個考古題的品質，這絕對是最值得你信賴的考試資料。如果你還是不相信的話，那就趕快自己來體驗一下吧。你绝对会相信我的话的。

選擇NewDumps可以100%幫助你通過考試。我們根據Splunk SPLK-5002的考試科目的不斷變化，也會不斷的更新我們的培訓資料，會提供最新的考試內容。NewDumps可以為你免費提供24小時線上客戶服務，如果你沒有通過Splunk SPLK-5002的認證考試，我們會全額退款給您。

>> SPLK-5002認證考試 <<

SPLK-5002認證考試的學習資料

我們NewDumps網站的Splunk培訓資料是沒有網站可以與之比較的。它是空前絕後的真實，準確，為了幫助每位考生順利通過考試，我們的SPLK-5002精英團隊不斷探索。我可以毫不猶豫的說這絕對是一份具有針對性的培訓資料。我們NewDumps網站不僅產品真實，而且價格也很合理，當你選擇我們的產品，我們還提供一年的免費更新，讓你更在充裕的時間裏準備SPLK-5002考試，這樣也可以消除你對考試緊張的心理，達到一個兩全其美的辦法了。

Splunk SPLK-5002 考試大綱：

主題	簡介
主題 1	• Automation and Efficiency: This section assesses Automation Engineers and SOAR Specialists in streamlining security operations. It covers developing automation for SOPs, optimizing case management workflows, utilizing REST APIs, designing SOAR playbooks for response automation, and evaluating integrations between Splunk Enterprise Security and SOAR tools.
主題 2	• Building Effective Security Processes and Programs: This section targets Security Program Managers and Compliance Officers, focusing on operationalizing security workflows. It involves researching and integrating threat intelligence, applying risk and detection prioritization methodologies, and developing documentation or standard operating procedures (SOPs) to maintain robust security practices.

主題 3	• Detection Engineering: This section evaluates the expertise of Threat Hunters and SOC Engineers in developing and refining security detections. Topics include creating and tuning correlation searches, integrating contextual data into detections, applying risk-based modifiers, generating actionable Notable Events, and managing the lifecycle of detection rules to adapt to evolving threats.
主題 4	• Data Engineering: This section of the exam measures the skills of Security Analysts and Cybersecurity Engineers and covers foundational data management tasks. It includes performing data review and analysis, creating and maintaining efficient data indexing, and applying Splunk methods for data normalization to ensure structured and usable datasets for security operations.
主題 5	• Auditing and Reporting on Security Programs: This section tests Auditors and Security Architects on validating and communicating program effectiveness. It includes designing security metrics, generating compliance reports, and building dashboards to visualize program performance and vulnerabilities for stakeholders.

最新的 Cybersecurity Defense Analyst SPLK-5002 免費考試真題 (Q65-Q70):

問題 #65
Which practices strengthen the development of Standard Operating Procedures (SOPs)?(Choosethree)

- A. Excluding historical incident data
- B. Regular updates based on feedback
- C. Focusing solely on high-risk scenarios
- D. Including detailed step-by-step instructions
- E. Collaborating with cross-functional teams

答案： B,D,E

解題說明：
Why Are These Practices Essential for SOP Development?
Standard Operating Procedures (SOPs)are crucial for ensuring consistent, repeatable, and effective security operations in aSecurity Operations Center (SOC). Strengthening SOP development ensuresefficiency, clarity, and adaptabilityin responding to incidents.
1##Regular Updates Based on Feedback (Answer A)
Security threats evolve, andSOPs must be updatedbased onreal-world incidents, analyst feedback, and lessons learned.
Example: Anew ransomware variantis detected; theSOP is updatedto include aspecific containment playbookin Splunk SOAR.
2##Collaborating with Cross-Functional Teams (Answer C)
Effective SOPs requireinput from SOC analysts, threat hunters, IT, compliance teams, and DevSecOps.
Ensures thatall relevant security and business perspectivesare covered.
Example: ASOC team collaborates with DevOpsto ensure that acloud security response SOPaligns with AWS security controls.
3##Including Detailed Step-by-Step Instructions (Answer D)
SOPs should provideclear, actionable, and standardizedsteps for security analysts.
Example: ASplunk ES incident response SOPshould include:
How to investigate a security alertusing correlation searches.
How to escalate incidentsbased on risk levels.
How to trigger a Splunk SOAR playbookfor automated remediation.
Why Not the Other Options?
#B. Focusing solely on high-risk scenarios-All security events matter, not just high-risk ones.Low-level alertscan be early indicators of larger threats.#E. Excluding historical incident data- Past incidents providevaluable lessonsto improveSOPs and incident response workflows.
References & Learning Resources
#Best Practices for SOPs in Cybersecurity:https://www.nist.gov/cybersecurity-framework#Splunk SOAR Playbook SOP Development: https://docs.splunk.com/Documentation/SOAR#Incident Response SOPs with Splunk: https://splunkbase.splunk.com

問題 #66
Which features are crucial for validating integrations in Splunk SOAR? (Choose three)

- A. Increasing indexer capacity
- B. Testing API connectivity
- C. Monitoring data ingestion rates
- D. Verifying authentication methods
- E. Evaluating automated action performance

答案： B,D,E

解題說明：
Validating Integrations in Splunk SOAR
Splunk SOAR (Security Orchestration, Automation, and Response) integrates with various security tools to automate security workflows. Proper validation of integrations ensures that playbooks, threat intelligence feeds, and incident response actions function as expected.
#Key Features for Validating Integrations
1##Testing API Connectivity (A)
Ensures Splunk SOAR can communicate with external security tools (firewalls, EDR, SIEM, etc.).
Uses API testing tools like Postman or Splunk SOAR's built-in Test Connectivity feature.
2##Verifying Authentication Methods (C)
Confirms that integrations use the correct authentication type (OAuth, API Key, Username/Password, etc.).
Prevents failed automations due to expired or incorrect credentials.
3##Evaluating Automated Action Performance (D)
Monitors how well automated security actions (e.g., blocking IPs, isolating endpoints) perform.
Helps optimize playbook execution time and response accuracy.
#Incorrect Answers & Explanations
B: Monitoring data ingestion rates # Data ingestion is crucial for Splunk Enterprise, but not a core integration validation step for SOAR.
E: Increasing indexer capacity # This is related to Splunk Enterprise data indexing, not Splunk SOAR integration validation.
#Additional Resources:
Splunk SOAR Administration Guide
Splunk SOAR Playbook Validation
Splunk SOAR API Integrations

問題 #67
What is Enterprise Security's default way of determining the urgency of a finding (notable event)?

- A. Add risk scores for associated objects within a network.
- B. Take into account the priority assigned to the asset/identity as well as the severity value assigned to the finding.
- C. Leverage the scheduling priority of the detection to know what's most critical.
- D. Multiply the risk score of a detection by how many times it has run.

答案： B

解題說明：
In Splunk Enterprise Security, the default method for determining the urgency of a notable event considers both the priority of the asset or identity involved and the severity value assigned to the finding. This ensures that critical assets with high-severity events are prioritized appropriately for analyst attention.

問題 #68
If a correlation search cannot be run at the configured time, which scheduling option should an engineer use to ensure there are no backfill gaps in data?

- A. Default
- B. Continuous
- C. Real-time
- D. Auto

答案： B

解題說明：

The Continuous scheduling option ensures that if a correlation search is delayed or cannot run at its scheduled time, Splunk will still execute it later and cover the missed time range. This prevents backfill gaps in data and ensures no events are overlooked.

問題 #69
What are key elements of a well-constructed notable event?(Choosethree)

- A. Proper categorization
- B. Meaningful descriptions
- C. Relevant field extractions
- D. Minimal use of contextual data

答案：A,B,C

解題說明：
A notable event in Splunk Enterprise Security (ES) represents a significant security detection that requires investigation.
#Key Elements of a Good Notable Event#Meaningful Descriptions (Answer A) Helps analysts understand the event at a glance.
Example: Instead of "Possible attack detected," use "Multiple failed admin logins from foreign IP address".
#Proper Categorization (Answer C)
Ensures events are classified correctly (e.g., Brute Force, Insider Threat, Malware Activity).
Example: A malicious file download alert should be categorized as "Malware Infection", not just "General Alert".
#Relevant Field Extractions (Answer D)
Ensures that critical details (IP, user, timestamp) are present for SOC analysis.
Example: If an alert reports failed logins, extracted fields should include username, source IP, and login method.
Why Not the Other Options?
#B. Minimal use of contextual data - More context helps SOC analysts investigate faster.
References & Learning Resources
#Building Effective Notable Events in Splunk ES: https://docs.splunk.com/Documentation/ES#SOC Best Practices for Security Alerts: https://splunkbase.splunk.com#How to Categorize Security Alerts Properly: https://www.splunk.com/en_us/blog/security

問題 #70
.....

入□ SPLK-5002 □並獲取免費下載最新SPLK-5002試題

- 優秀的SPLK-5002認證考試和資格考試中的領先供應商和快速下載Splunk Splunk Certified Cybersecurity Defense Engineer □ 在☀ www.pdfexamdumps.com □☀□網站上查找✔ SPLK-5002 □✔□的最新題庫SPLK-5002認證指南
- jeanbdsu225522.thelateblog.com, tiannagfvr978830.mappywiki.com, hamzahawpw013637.tdlwiki.com, monicaczer227104.blogrelation.com, socialmediatotal.com, craigcnts886376.angelinsblog.com, www.stes.tyc.edu.tw, kianajhnr665265.blognody.com, jayasgfn182545.national-wiki.com, www.stes.tyc.edu.tw, Disposable vapes

2026 NewDumps最新的SPLK-5002 PDF版考試題庫和SPLK-5002考試問題和答案免費分享：https://drive.google.com/open?id=1pJBRNdb-ASJLBjV6vj5KMjG2TT6sh3sH