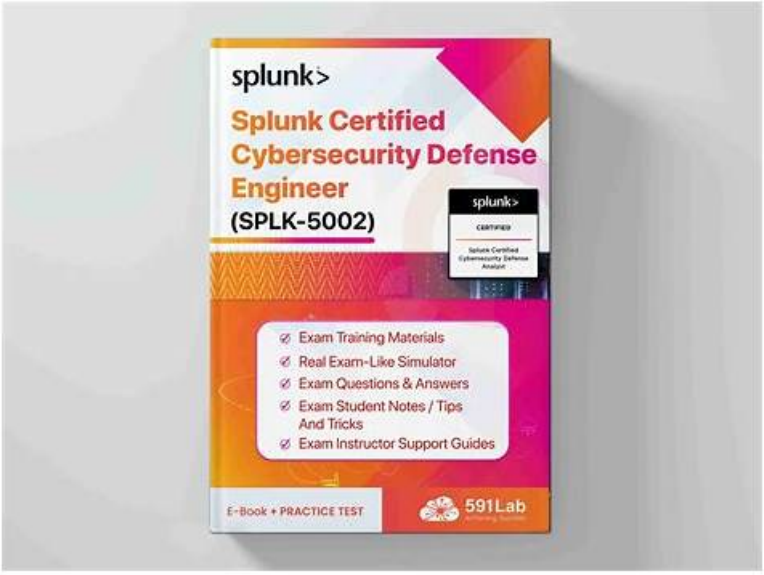
Splunk SPLK-5002試験 & SPLK-5002試験勉強過去問



ちなみに、ShikenPASS SPLK-5002の一部をクラウドストレージからダウンロードできます：https://drive.google.com/open?id=1Uqy2m2CKtd2opwmqCBjsBWkeobu3Z9Tj

急速に発展している世界のすべての人にとって、良い仕事をすることがますます重要になっていることは私たちに知られています。 SPLK-5002認定を取得することがますます困難になっていることがわかっています。仕事、賃金、およびSPLK-5002認定が心配な場合、これを変更する場合は、SPLK-5002試験トレントで高品質の問題を解決するのを手伝います。無料でダウンロードできます。 SPLK-5002ガイドトレントのウェブ上のデモ。SPLK-5002試験の質問に後悔しないことをお約束します。

Splunk SPLK-5002 認定試験の出題範囲：

トピック	出題範囲
トピック 1	• 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.
トピック 2	• 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.
トピック 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.
トピック 4	• 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.
トピック 5	• 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.

SPLK-5002試験勉強過去問、SPLK-5002受験料

あなたは弊社の商品を買ったら一年間に無料でアップサービスが提供されたSPLK-5002認定試験に合格するまで利用しても喜んでいます。もしテストの内容が変われば、すぐにお客様に伝えます。弊社はあなた１００％SPLK-5002合格率を保証いたします。

Splunk Certified Cybersecurity Defense Engineer 認定 SPLK-5002 試験問題 (Q32-Q37):

質問 # 32
A security team notices delays in responding to phishing emails due to manual investigation processes.
Howcan Splunk SOAR improve this workflow?

- A. By prioritizing phishing cases manually
- B. By assigning cases to analysts in real-time
- C. By increasing the indexing frequency of email logs
- D. By automating email triage and analysis with playbooks

正解：D

解説：
How Splunk SOAR Improves Phishing Response?
Phishing attacks require fast detection and response. Manual investigation delays can be eliminated using Splunk SOAR automation.
#Why Use Playbooks for Automated Email Triage? (Answer B)#Extracts email headers and attachments for analysis#Checks links & attachments against threat intelligence feeds#Automatically quarantines or deletes malicious emails#Escalates high-risk cases to SOC analysts
#Example Playbook Workflow in Splunk SOAR:#Scenario: A suspicious email is reported.#Splunk SOAR playbook automatically:
Extracts sender details & checks against threat intelligence
Analyzes URLs & attachments using VirusTotal/Sandboxing
Tags the email as "Malicious" or "Safe"
Quarantines the email & alerts SOC analysts
Why Not the Other Options?
#A. Prioritizing phishing cases manually - Still requires manual effort, leading to delays.#C. Assigning cases to analysts in real-time - Doesn't solve the issue of slow manual investigations.#D. Increasing the indexing frequency of email logs - Helps with log retrieval but doesn't automate phishing response.
References & Learning Resources
#Splunk SOAR Phishing Playbook Guide: https://docs.splunk.com/Documentation/SOAR#Phishing Detection Automation in Splunk: https://splunkbase.splunk.com#Email Threat Intelligence with SOAR: https://www.splunk.com/en_us/blog/security

質問 # 33
What methods can improve dashboard usability for security program analytics?(Choosethree)

- A. Using drill-down options for detailed views
- B. Limiting the number of panels on the dashboard
- C. Adding context-sensitive filters
- D. Standardizing color coding for alerts
- E. Avoiding performance optimization

正解：A、C、D

解説：
Methods to Improve Dashboard Usability in Security Analytics
A well-designed Splunk security dashboard helps SOC teams quickly identify, analyze, and respond to security threats.
#1. Using Drill-Down Options for Detailed Views (A)
Allows analysts to click on high-level metrics and drill down into event details.

Helps teams pivot from summary statistics to specific security logs.
Example:
Clicking on a failed login trend chart reveals specific failed login attempts per user.
#2. Standardizing Color Coding for Alerts (B)
Consistent color usage enhances readability and priority identification.
Example:
Red # Critical incidents
Yellow # Medium-risk alerts
Green # Resolved issues
#3. Adding Context-Sensitive Filters (D)
Filters allow users to focus on specific security events without running new searches.
Example:
A dropdown filter for "Event Severity" lets analysts view only high-risk events.
#Incorrect Answers:
C: Limiting the number of panels on the dashboard # Dashboards should be optimized, not restricted.
E: Avoiding performance optimization # Performance tuning is essential for responsive dashboards.
#Additional Resources:
Splunk Dashboard Design Best Practices
Optimizing Security Dashboards in Splunk

質問 # 34
A Splunk administrator is tasked with creating a weekly security report for executives.
Whatelements should they focus on?

- A. High-level summaries and actionable insights
- B. Excluding compliance metrics to simplify reports
- C. Avoiding visuals to focus on raw data
- D. Detailed logs of every notable event

正解：A

解説：
Why Focus on High-Level Summaries & Actionable Insights?
Executive security reports should provideconcise, strategic insightsthat help leadership teams makeinformed decisions.
#Key Elements for an Executive-Level Report:#Summarized Security Incidents- Focus onmajor threats and trends.#Actionable Recommendations- Includemitigation stepsfor ongoing risks.#Visual Dashboards- Use charts and graphs foreasy interpretation.#Compliance & Risk Metrics- Highlightcompliance status(e.g., PCI- DSS, NIST).
#Example in Splunk:#Scenario:A CISO requests aweekly security report.#Best Report Format:
Threat Summary:"Detected 15 phishing attacks this week."
Key Risks:"Increase in brute-force login attempts."
Recommended Actions:"Enhance MFA enforcement & user awareness training." Why Not the Other Options?
#B. Detailed logs of every notable event- Too technical; executives needsummaries, not raw logs.#C. Excluding compliance metrics to simplify reports- Compliance is critical forrisk assessment.#D. Avoiding visuals to focus on raw data-Visuals improve clarity; raw data is too complex for executives.
References & Learning Resources
#Splunk Security Reporting Best Practices: https://www.splunk.com/en_us/blog/security#Creating Effective Executive Dashboards in Splunk: https://splunkbase.splunk.com#Cybersecurity Metrics & Reporting for Leadership Teams:https://www.nist.gov/cyberframework

質問 # 35
What are essential steps in developing threat intelligence for a security program?(Choosethree)

- A. Creating dashboards for executives
- B. Collecting data from trusted sources
- C. Operationalizing intelligence through workflows
- D. Conducting regular penetration tests
- E. Analyzing and correlating threat data

正解：B、C、E

解説：
Threat intelligence in Splunk Enterprise Security (ES) enhances SOC capabilities by identifying known attack patterns, suspicious activity, and malicious indicators.
Essential Steps in Developing Threat Intelligence:
Collecting Data from Trusted Sources (A)
Gather data from threat intelligence feeds (e.g., STIX, TAXII, OpenCTI, VirusTotal, AbuseIPDB).
Include internal logs, honeypots, and third-party security vendors.
Analyzing and Correlating Threat Data (C)
Use correlation searches to match known threat indicators against live data.
Identify patterns in network traffic, logs, and endpoint activity.
Operationalizing Intelligence Through Workflows (E)
Automate responses using Splunk SOAR (Security Orchestration, Automation, and Response).
Enhance alert prioritization by integrating intelligence into risk-based alerting (RBA).

質問 # 36
What methods can improve Splunk's indexing performance?(Choosetwo)

- A. Use universal forwarders for data ingestion.
- B. Create multiple search heads.
- C. Enable indexer clustering.
- D. Optimize event breaking rules.

正解：C、D

解説：
Improving Splunk's indexing performance is crucial for handling large volumes of data efficiently while maintaining fast search speeds and optimized storage utilization.
Methods to Improve Indexing Performance:
Enable Indexer Clustering (A)
Distributes indexing load across multiple indexers.
Ensures high availability and fault tolerance by replicating indexed data.
Optimize Event Breaking Rules (D)
Defines clear event boundaries to reduce processing overhead.
Uses correctLINE_BREAKERandTRUNCATEsettings to improve parsing speed.

質問 # 37
.....

- SPLK-5002資格認証攻略 □ SPLK-5002日本語練習問題 □ SPLK-5002勉強時間 ◂ 今すぐ“ www.goshiken.com ”を開き、▹ SPLK-5002 ◃を検索して無料でダウンロードしてくださいSPLK-5002受験料
- 更新のSPLK-5002試験 | 素晴らしい合格率のSPLK-5002 Exam | 素晴らしいSPLK-5002: Splunk Certified Cybersecurity Defense Engineer □ 《 www.xhs1991.com 》サイトにて最新➠ SPLK-5002 □問題集をダウンロードSPLK-5002資格認証攻略
- 一番優秀なSPLK-5002試験と更新するSPLK-5002試験勉強過去問 □ □ www.goshiken.com □を開いて➤ SPLK-5002 □を検索し、試験資料を無料でダウンロードしてくださいSPLK-5002更新版
- 最新のSPLK-5002試験 - 合格スムーズSPLK-5002試験勉強過去問 | 効率的なSPLK-5002受験料 □ ✔ www.xhs1991.com □✔□から《 SPLK-5002 》を検索して、試験資料を無料でダウンロードしてくださいSPLK-5002トレーニング資料
- Splunk SPLK-5002 Exam | SPLK-5002試験 - 試す SPLK-5002試験勉強過去問 無料で簡単に購入 □ ▹ www.goshiken.com ◃で□ SPLK-5002 □を検索して、無料で簡単にダウンロードできますSPLK-5002試験問題
- SPLK-5002試験勉強攻略 □ SPLK-5002資格認証攻略 □ SPLK-5002試験勉強攻略 □ 今すぐ➤ www.topexam.jp □を開き、⇛ SPLK-5002 ⇚を検索して無料でダウンロードしてくださいSPLK-5002復習テキスト
- myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, lms.ait.edu.za, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, knowyourmeme.com, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, Disposable vapes

P.S.ShikenPASSがGoogle Driveで共有している無料の2025 Splunk SPLK-5002ダンプ：https://drive.google.com/open?id=1Uqy2m2CKtd2opwmqCBjsBWkeobu3Z9Tj