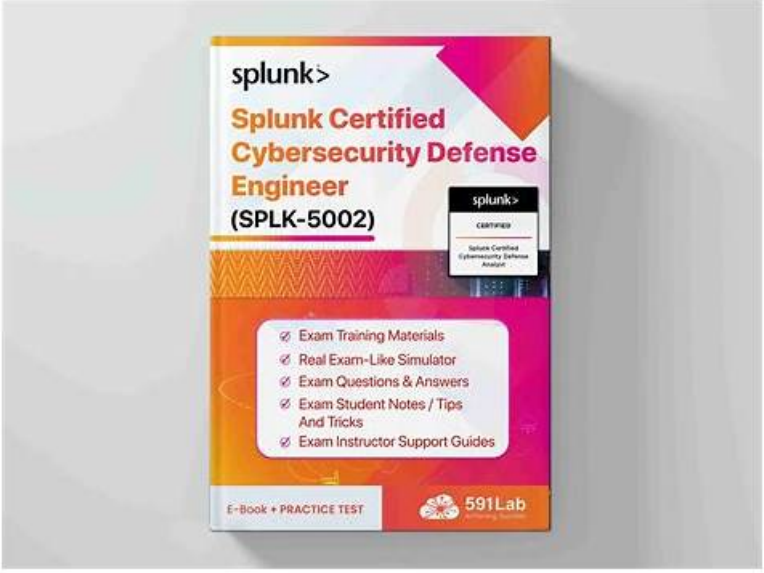
素敵なSPLK-5002関連資格試験対応 &保証するSplunk SPLK-5002専門的な試験の成功SPLK-5002最新受験攻略



P.S. PassTestがGoogle Driveで共有している無料かつ新しいSPLK-5002ダンプ：https://drive.google.com/open?id=1mRzRYzQSOk_DbuXaPo7oqiQuR9QXA-3x

多くの人々はSplunkのSPLK-5002試験に合格できるのは難しいことであると思っています。この悩みに対して、我々社PassTestはSplunkのSPLK-5002試験に準備するあなたに専門的なヘルプを与えられます。弊社のSplunkのSPLK-5002練習問題を利用したら、あなたは気楽に勉強するだけではなく、順調に試験に合格します。

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	• 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 2	• 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 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.

Splunk Certified Cybersecurity Defense Engineer 認定 SPLK-5002 試験問題 (Q42-Q47):

質問 # 42
Which components are necessary to develop a SOAR playbook in Splunk?(Choosethree)

- A. Manual approval processes
- B. Defined workflows
- C. Integration with external tools
- D. Actionable steps or tasks
- E. Threat intelligence feeds

正解：B、C、D

解説：
Splunk SOAR (Security Orchestration, Automation, and Response) playbooks automate security processes, reducing response times.
#1. Defined Workflows (A)
A structured flowchart of actions for handling security events.
Ensures that the playbook follows a logical sequence (e.g., detect # enrich # contain # remediate).
Example:
If a phishing email is detected, the workflow includes:
Extract email artifacts (e.g., sender, links).
Check indicators against threat intelligence feeds.
Quarantine the email if it is malicious.
#2. Actionable Steps or Tasks (C)
Each playbook contains specific, automated steps that execute responses.
Examples:
Extracting indicators from logs.
Blocking malicious IPs in firewalls.
Isolating compromised endpoints.
#3. Integration with External Tools (E)
Playbooks must connect with SIEM, EDR, firewalls, threat intelligence platforms, and ticketing systems.
Uses APIs and connectors to integrate with tools like:
Splunk ES
Palo Alto Networks
Microsoft Defender
ServiceNow
#Incorrect Answers:
B: Threat intelligence feeds # These enrich playbooks but are not mandatory components of playbook development.
D: Manual approval processes # Playbooks are designed for automation, not manual approvals.
#Additional Resources:
Splunk SOAR Playbook Documentation

Best Practices for Developing SOAR Playbooks

質問 # 43
Which Splunk feature helps in tracking and documenting threat trends over time?

- A. Event sampling
- B. Risk-based dashboards
- C. Data model acceleration
- D. Summary indexing

正解：B

解説：
Why Use Risk-Based Dashboards for Tracking Threat Trends?
Risk-based dashboards in Splunk Enterprise Security (ES) provide a structured way to track threats over time.
#How Risk-Based Dashboards Help:#Aggregate security events into risk scores # Helps prioritize high-risk activities.#Show historical trends of threat activity.#Correlate multiple risk factors across different security events.
#Example in Splunk ES:#Scenario: A SOC team tracks insider threat activity over 6 months.#The Risk-Based Dashboard shows:
Users with rising risk scores over time.
Patterns of malicious behavior (e.g., repeated failed logins + data exfiltration).
Correlation between different security alerts (e.g., phishing clicks # malware execution).
Why Not the Other Options?
#A. Event sampling - Helps with performance optimization, not threat trend tracking.#C. Summary indexing - Stores precomputed data but is not designed for tracking risk trends.#D. Data model acceleration - Improves search speed, but doesn't track security trends.
References & Learning Resources
#Splunk ES Risk-Based Alerting Guide: https://docs.splunk.com/Documentation/ES#Tracking Security Trends Using Risk-Based Dashboards: https://splunkbase.splunk.com#How to Build Risk-Based Analytics in Splunk: https://www.splunk.com/en_us/blog/security

質問 # 44
What is the primary purpose of developing security metrics in a Splunk environment?

- A. To enhance data retention policies
- B. To identify low-priority alerts for suppression
- C. To measure and evaluate the effectiveness of security programs
- D. To automate case management workflows

正解：C

解説：
Security metrics help organizations assess their security posture and make data-driven decisions.
Primary Purpose of Security Metrics in Splunk:
Measure Security Effectiveness (B)
Tracks incident response times, threat detection rates, and alert accuracy.
Helps SOC teams and leadership evaluate security program performance.
Improve Threat Detection & Incident Response
Identifies gaps in detection logic and false positives.
Helps fine-tune correlation searches and notable events.

質問 # 45
What methods enhance risk-based detection in Splunk?(Choosetwo)

- A. Defining accurate risk modifiers
- B. Enriching risk objects with contextual data
- C. Using summary indexing for raw events
- D. Limiting the number of correlation searches

正解：A、B

解説：
Risk-based detection in Splunk prioritizes alerts based on behavior, threat intelligence, and business impact.
Enhancing risk scores and enriching contextual data ensures that SOC teams focus on the most critical threats.
Methods to Enhance Risk-Based Detection:
Defining Accurate Risk Modifiers (A)
Adjusts risk scores dynamically based on asset value, user behavior, and historical activity.
Ensures that low-priority noise doesn't overwhelm SOC analysts.
Enriching Risk Objects with Contextual Data (D)
Adds threat intelligence feeds, asset criticality, and user behavior data to alerts.
Improves incident triage and correlation of multiple low-level events into significant threats.

質問 # 46
A Splunk administrator is tasked with creating a weekly security report for executives.
Whatelements should they focus on?

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

正解：C

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 # 47
.....

5002 }問題集ファイルは{ www.xhs1991.com }にて検索SPLK-5002日本語版テキスト内容

- SPLK-5002赤本合格率 □ SPLK-5002模擬試験問題集 □ SPLK-5002試験攻略 □ □ www.goshiken.com □を入力して[SPLK-5002]を検索し、無料でダウンロードしてくださいSPLK-5002合格対策
- 実用的なSPLK-5002関連資格試験対応試験-試験の準備方法-信頼的なSPLK-5002最新受験攻略 □ ➠ www.passtest.jp □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復習資料
- 実用的なSPLK-5002関連資格試験対応試験-試験の準備方法-信頼的なSPLK-5002最新受験攻略 □ ➡ www.goshiken.com □□□サイトで[SPLK-5002]の最新問題が使えるSPLK-5002赤本合格率
- 有難いSPLK-5002関連資格試験対応試験-試験の準備方法-実際的なSPLK-5002最新受験攻略 □ 今すぐ{ www.mogiexam.com }で⇒ SPLK-5002 ⇐を検索し、無料でダウンロードしてくださいSPLK-5002合格対策
- 有難いSPLK-5002関連資格試験対応試験-試験の準備方法-実際的なSPLK-5002最新受験攻略 □ ➤ www.goshiken.com □サイトにて□ SPLK-5002 □問題集を無料で使おうSPLK-5002受験記対策
- SPLK-5002模擬試験問題集 □ SPLK-5002試験 □ SPLK-5002日本語対策問題集 □ ➡ www.xhs1991.com □□□は、{ SPLK-5002 }を無料でダウンロードするのに最適なサイトですSPLK-5002実際試験
- SPLK-5002日本語試験情報 □ SPLK-5002赤本合格率 □ SPLK-5002試験時間 ⁜ ☀ www.goshiken.com □☀□で使える無料オンライン版✔ SPLK-5002 □✔□ の試験問題SPLK-5002資格専門知識
- SPLK-5002資料的中率 □ SPLK-5002シュミレーション問題集 □ SPLK-5002日本語版テキスト内容 □ 今すぐ➤ www.jptestking.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試験攻略
- www.stes.tyc.edu.tw, motionentrance.edu.np, ixvangrif.alboompro.com, 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, eazybioacademy.com, 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, www.stes.tyc.edu.tw, www.61921.com, Disposable vapes

BONUS！！！ PassTest SPLK-5002ダンプの一部を無料でダウンロード：https://drive.google.com/open?id=1mRzRYzQSOk_DbuXaPo7oqiQuR9QXA-3x