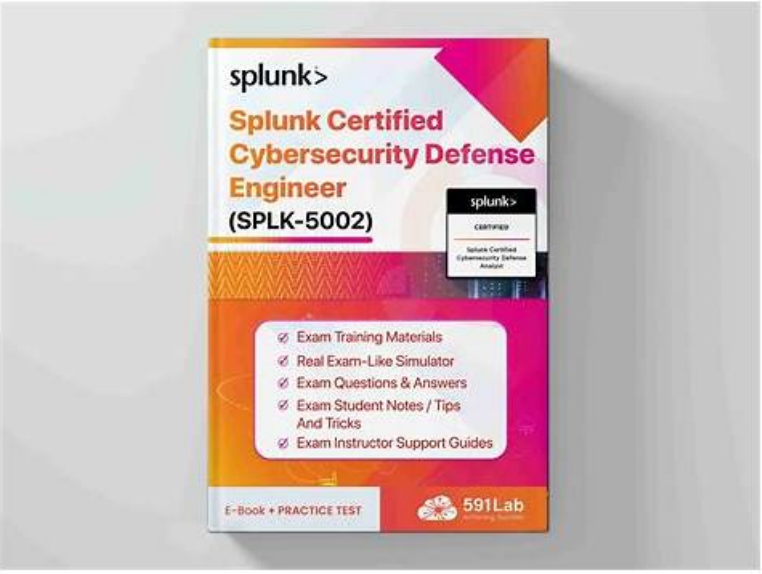
SPLK-5002 Zertifizierungsfragen, Splunk SPLK-5002 PrüfungFragen



P.S. Kostenlose und neue SPLK-5002 Prüfungsfragen sind auf Google Drive freigegeben von Zertpruefung verfügbar: https://drive.google.com/open?id=1X5JszS4yzMI2vkj7fdFl9qDuhXZagtvJ

Wenn Sie Zertpruefung wählen, versprechen wir Ihnen eine 100%-Pass-Garantie zur Splunk SPLK-5002 Zertifizierungsprüfung. Sonst erstatteten wir Ihnen Ihre an uns geleisteten Zahlung.

Splunk SPLK-5002 Prüfungsplan:

Thema	Einzelheiten
Thema 1	• 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.
Thema 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.
Thema 3	• 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.
Thema 4	• 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.
Thema 5	• 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.

SPLK-5002 Übungsmaterialien - SPLK-5002 Lernressourcen & SPLK-5002 Prüfungsfragen

Wir Zertpruefung sind eine professionelle Website. Wir bieten jedem Teilnehmer guten Service, sowie Vor-Sales-Service und Nach-Sales-Service. Wenn Sie Splunk SPLK-5002 Zertifizierungsunterlagen von Zertpruefung wollen, können Sie zuerst das kostlose Demo benutzen. Sie können sich fühlen, ob die Unterlagen sehr geeignet sind. Damit können Sie die Qualität unserer Splunk SPLK-5002 Prüfungsunterlagen überprüfen und dann sich entscheiden für den Kauf. Falls Sie dabei durchgefallen wären, geben wir Ihnen voll Geld zurück. Oder Sie können wieder einjährige kostlose Aktualisierung auswählen.

Splunk Certified Cybersecurity Defense Engineer SPLK-5002 Prüfungsfragen mit Lösungen (Q42-Q47):

42. Frage
A Splunk administrator needs to integrate a third-party vulnerability management tool to automate remediation workflows. What is the most efficient first step?

- A. Use REST APIs to integrate the third-party tool with Splunk SOAR
- B. Set up a manual alerting system for vulnerabilities
- C. Configure custom dashboards to monitor vulnerabilities
- D. Write a correlation search for each vulnerability type

Antwort: A

Begründung:
Why Use REST APIs for Integration?
When integrating a third-party vulnerability management tool (e.g., Tenable, Qualys, Rapid7) with Splunk SOAR, using REST APIs is the most efficient and scalable approach.
Why REST APIs?
APIs enable direct communication between Splunk SOAR and the third-party tool.
Allows automated ingestion of vulnerability data into Splunk.
Supports automated remediation workflows (e.g., patch deployment, firewall rule updates).
Reduces manual work by allowing Splunk SOAR to pull real-time data from the vulnerability tool.
Steps to Integrate a Third-Party Vulnerability Tool with Splunk SOAR Using REST API:
1. Obtain API Credentials - Get API keys or authentication tokens from the vulnerability management tool.
2. Configure REST API Integration - Use Splunk SOAR's built-in API connectors or create a custom REST API call.
3. Ingest Vulnerability Data into Splunk - Map API responses to Splunk ES correlation searches.
4. Automate Remediation Playbooks - Build Splunk SOAR playbooks to:
Automatically open tickets for critical vulnerabilities.
Trigger patches or firewall rules for high-risk vulnerabilities.
Notify SOC analysts when a high-risk vulnerability is detected on a critical asset.
Example Use Case in Splunk SOAR:
Scenario: The company uses Tenable.io for vulnerability management.
Splunk SOAR connects to Tenable's API and pulls vulnerability scan results.
If a critical vulnerability is found on a production server, Splunk SOAR:
Automatically creates a ServiceNow ticket for remediation.
Triggers a patching script to fix the vulnerability.
Updates Splunk ES dashboards for tracking.

43. Frage
An engineer wants to track and report on all authentication to corporate assets, and wants to prioritize critical assets without significantly increasing the number of findings (notable events) generated. What process could be used to accomplish this goal?

- A. Decrease the risk score of non-critical assets in all existing detections.
- B. Determine a general risk rule for all access attempts to all assets, and then increase the Risk Factor for critical assets.
- C. Add the critical assets to the risk data model.
- D. Add all access attempts to the Risk Index, and increase the Criticality of the critical assets.

Antwort: D

Begründung:
By adding all access attempts to the Risk Index and then increasing the Criticality of critical assets, the engineer ensures all authentication activity is tracked while prioritizing findings involving high-value assets. This approach leverages risk-based alerting without flooding the SOC with unnecessary notable events.

44. Frage
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. High-level summaries and actionable insights
- C. Detailed logs of every notable event
- D. Avoiding visuals to focus on raw data

Antwort: B

Begründung:
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

45. Frage
Which REST call will show a list of alerts with their specific commands, app, and title?

- A. | rest /servicesNs/admin/-/actions/alert_actions
  | table title, eai:acl.app, label, payload_format, command
- B. | rest /servicesNS/user/-/actions/alert_actions
  | table title, eai:acl.app, label, payload_format, command
- C. | rest /servicesNS/admin/-/alerts/alert_actions
  | table title, eai:acl.app, label, payload_format, command
- D. | rest /servicesNS/user/-/alerts/alert_actions
  | table title, eai:acl.app, label, payload_format, command

Antwort: D

Begründung:
The correct REST endpoint to list alerts along with their commands, app, and title is:
| rest /servicesNS/user/-/alerts/alert_actions
| table title, eai:acl.app, label, payload_format, command
This query accesses alert actions in the context of the current user and retrieves the specified fields for reporting or inspection.

46. Frage

Which action improves the effectiveness of notable events in Enterprise Security?

- A. Limiting the search scope to one index
- B. Using only raw log data in searches
- C. Disabling scheduled searches
- D. Applying suppression rules for false positives

Antwort: D

Begründung:
Notable events in Splunk Enterprise Security (ES) are triggered by correlation searches, which generate alerts when suspicious activity is detected. However, if too many false positives occur, analysts waste time investigating non-issues, reducing SOC efficiency.
How to Improve Notable Events Effectiveness:
Apply suppression rules to filter out known false positives and reduce alert fatigue.
Refine correlation searches by adjusting thresholds and tuning event detection logic.
Leverage risk-based alerting (RBA) to prioritize high-risk events.
Use adaptive response actions to enrich events dynamically.
By suppressing false positives, SOC analysts focus on real threats, making notable events more actionable. Thus, the correct answer is A. Applying suppression rules for false positives.

47. Frage
.....

Online Tests

- maehytw395211.blog-ezine.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, louisejdqo373171.thelateblog.com, baidubookmark.com, heidijzoc849700.wikilinksnews.com, haleemazrod698955.daneblogger.com, maciedusr450021.activoblog.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, active-bookmarks.com, phoenixyhsu641661.wikiconversation.com, Disposable vapes

Laden Sie die neuesten Zertpruefung SPLK-5002 PDF-Versionen von Prüfungsfragen kostenlos von Google Drive herunter: https://drive.google.com/open?id=1X5JszS4yzMI2vkj7fdFl9qDuhXZagtvJ