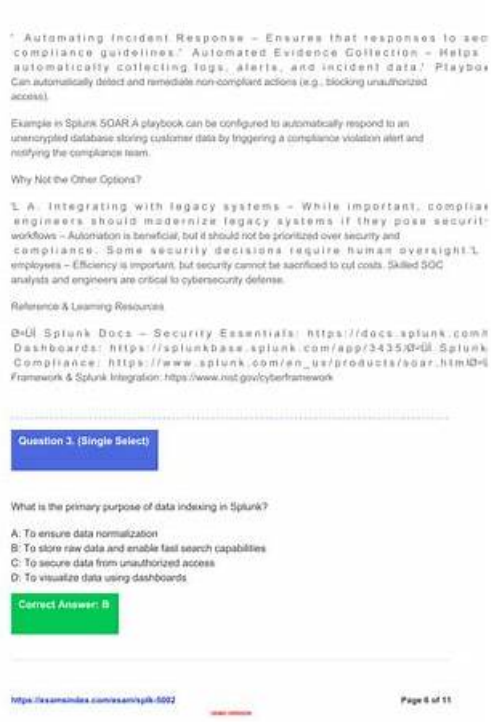
SPLK-5002 PDF題庫 & SPLK-5002考試內容


' Automating Incident Response – Ensures that responses to sec
compliance guidelines.' Automated Evidence Collection – Helps
automatically collecting logs, alerts, and incident data.' Playbo
Can automatically detect and remediate non-compliant actions (e.g., blocking unauthorized
access).

Example in Splunk SOAR:A playbook can be configured to automatically respond to an
unencrypted database storing customer data by triggering a compliance violation alert and
notifying the compliance team.

Why Not the Other Options?

'L A. Integrating with legacy systems – While important, compliar
engineers should modernize legacy systems if they pose securit
workflows – Automation is beneficial, but it should not be prioritized over security and
compliance. Some security decisions require human oversight.'L
employees – Efficiency is important, but security cannot be sacrificed to cut costs. Skilled SOC
analysts and engineers are critical to cybersecurity defense.

Reference & Learning Resources

@='UI Splunk Docs – Security Essentials: https://docs.splunk.com
Dashboards: https://splunkbase.splunk.com/app/3435/@='UI Splunk
Compliance: https://www.splunk.com/en_us/products/soar.html@='U
Framework & Splunk Integration: https://www.nist.gov/cyberframework

Question 3. (Single Select)

What is the primary purpose of data indexing in Splunk?

A: To ensure data normalization
B: To store raw data and enable fast search capabilities
C: To secure data from unauthorized access
D: To visualize data using dashboards

Correct Answer: B

https://examsindex.com/exam/splk-5002 Page 6 of 11

P.S. Testpdf在Google Drive上分享了免費的2026 Splunk SPLK-5002考試題庫：https://drive.google.com/open?id=10-_oPrwwsCHku5kYUDRbA0uw9FoSGMJG

如果你想參加SPLK-5002認證考試，那麼是使用SPLK-5002考試資料是很有必要的。如果你正在漫無目的地到處尋找參考資料，那麼趕快停止吧。如果你不知道應該用什麼資料，那麼試一下Testpdf的SPLK-5002考古題吧。這個考古題的命中率很高，可以保證你一次就取得成功。與別的考試資料相比，這個考古題更能準確地劃出考試試題的範圍。這樣的話，可以讓你提高學習效率，更加充分地準備SPLK-5002考試。

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	• 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.
主題 5	• 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.

SPLK-5002考試內容，SPLK-5002考題套裝

Testpdf就是一個能使 SPLK-5002 認證考試的通過率提高的一個網站。我們的資深IT專家在不斷研究出各種成功通過 Splunk SPLK-5002 認證考試的方案，他們的研究成果可以100%保證一次性通過 Splunk SPLK-5002 認證考試。在我們的支援下，您不但能順利通過考試，還能節省了時間和金錢。此外，我們承諾如果不通過 SPLK-5002 考試，將100％退款。

最新的 Cybersecurity Defense Analyst SPLK-5002 免費考試真題 (Q94-Q99):

問題 #94
What is the purpose of using data models in building dashboards?

- A. To store raw data for compliance purposes
- B. To compress indexed data
- C. To reduce storage usage on Splunk instances
- D. To provide a consistent structure for dashboard queries

答案：D

解題說明：
Why Use Data Models in Dashboards?
SplunkData Modelsallow dashboards toretrieve structured, normalized data quickly, improving search performance and accuracy.
#How Data Models Help in Dashboards?(AnswerB)#Standardized Field Naming- Ensures that queries always useconsistent field names(e.g.,src_ipinstead ofsource_ip).#Faster Searches- Data models allow dashboards torun structured searches instead of raw log queries.#Example:ASOC dashboard for user activity monitoringuses a CIM-compliantAuthentication Data Model, ensuring that querieswork across different log sources.
Why Not the Other Options?
#A. To store raw data for compliance purposes- Raw data is stored in indexes,not data models.#C. To compress indexed data- Data modelsstructuredata but donot perform compression.#D. To reduce storage usage on Splunk instances- Data modelshelp with search performance, not storage reduction.
References & Learning Resources
#Splunk Data Models for Dashboard Optimization: https://docs.splunk.com/Documentation/Splunk/latest /Knowledge/Aboutdatamodels#Building Efficient Dashboards Using Data Models: https://splunkbase.splunk. com#Using CIM-Compliant Data Models for Security Analytics: https://www.splunk.com/en_us/blog/tips- and-tricks

問題 #95

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

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

答案：B

解題說明：
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.
References:
Managing Notable Events in Splunk ES
Best Practices for Tuning Correlation Searches
Using Suppression in Splunk ES

問題 #96
The following SPL is designed to report on a certain SOC metric. Which metric is the most likely topic for this report?

```
| tstats summariesonly=true earliest(_time) as _time FROM datamodel=Incident_Management BY "Notable_Events_Meta.rule_id"
| rename "Notable_Events_Meta.*" as "*"
| lookup update=true incident_updates_lookup rule_id OUTPUTNEW time
| search time=*
| stats earliest(_time) as create_time, min(time) as triage_time by rule_id
| eval diff=triage_time-create_time, stat_type=if(create_time < relative_time(now(), "-7d@d"), "past", "current"), past=if(stat_type="past", 1, 0), current=if(stat_type="current", 1, 0),
    past_diff=if(stat_type="past", diff, 0), current_diff=if(stat_type="current", diff, 0)
| stats sum(past) AS past, sum(current) AS current, sum(past_diff) AS past_diff, sum(current_diff) as current_diff
| eval past = round(past_diff/past/60), current = round(current_diff/current/60)
| table past, current
| transpose
```

- A. Mean time to Triage
- B. Mean time to Respond
- C. Mean time to Resolve
- D. Dwell Time

答案：A

解題說明：
The SPL calculates the time difference between create_time and triage_time for notable events.
This directly measures how long it takes analysts to triage an alert after it is created, which is the definition of Mean Time to Triage (MTTT).

問題 #97
What external support consideration should an engineer account for if they plan to automate the disabling of a system or user?

- A. Communicate the actions to the IT Help Desk.
- B. Enable logging on the playbook.
- C. Validate that the system or user is not already disabled.
- D. Add the "support" tag to the playbook.

答案：A

解題說明：
If an engineer plans to automate disabling a system or user, they must communicate the actions to the IT Help Desk. This ensures

that support teams are aware of automated responses, preventing confusion, unnecessary troubleshooting, or accidental business disruption.

問題 #98
The threat-hunting team has identified suspicious activity. An analyst manually creates a notable event using an event action to track the activity. How should a detection engineer ensure this activity automatically produces findings in the future?

- A. Create a SOAR playbook to assign risk modifiers for events matching the activity.
- B. Create a risk modifier for events matching the activity.
- C. Create a correlation search to produce notable events for the activity.
- D. Create a SOAR playbook to identify events matching the activity and assign an urgency.

答案：C

解題說明：
To ensure that suspicious activity consistently generates findings in the future, the detection engineer should create a correlation search for the identified activity. This automates detection by continuously monitoring for the same pattern and producing notable events when it occurs again.

問題 #99
.....

想要通過 SPLK-5002 考古題並不是僅僅依靠與考試相關的書籍就可以辦到的。與其盲目地學習考試要求的相關知識，不如做一些有價值的試題。一本高效率的 SPLK-5002 考古題是大家準備考試時必不可少的工具。所以，快點購買 Splunk 的 SPLK-5002 考古題吧。這是一本命中率很高的考古題，比其他任何學習方法都有效。這是可以保證你一次就成功的難得的資料。

SPLK-5002考試內容: https://www.testpdf.net/SPLK-5002.html

- SPLK-5002考試指南 □ SPLK-5002在線考題 □ SPLK-5002最新考證 □ （ www.vcesoft.com ）上的免費下載【 SPLK-5002 】頁面立即打開SPLK-5002考試資料
- 最佳的SPLK-5002 PDF題庫和認證考試的領導者材料和精准覆盖的SPLK-5002考試內容 □ 立即在[www.newdumpspdf.com]上搜尋[SPLK-5002]並免費下載SPLK-5002題庫分享
- SPLK-5002證照指南 □ SPLK-5002題庫分享 □ SPLK-5002參考資料 □ 在▹ tw.fast2test.com ◃網站上查找➽ SPLK-5002 □的最新題庫SPLK-5002考題資源
- 最新版的SPLK-5002 PDF題庫，提前為Splunk Certified Cybersecurity Defense Engineer SPLK-5002考試做好準備 □ 免費下載□ SPLK-5002 □只需進入{ www.newdumpspdf.com }網站SPLK-5002最新考證
- SPLK-5002真題 □ SPLK-5002證照指南 □ 最新SPLK-5002試題 □ ➡ tw.fast2test.com □□□提供免費➽ SPLK-5002 □問題收集SPLK-5002考古題推薦
- SPLK-5002證照 □ SPLK-5002真題 □ SPLK-5002考古題介紹 □ { www.newdumpspdf.com }上的免費下載□ SPLK-5002 □頁面立即打開SPLK-5002參考資料
- 有用的SPLK-5002 PDF題庫 |第一次嘗試輕鬆學習並通過考試，100％合格率的SPLK-5002：Splunk Certified Cybersecurity Defense Engineer □ 免費下載➥ SPLK-5002 □只需進入✔ www.pdfexamdumps.com □✔□網站SPLK-5002題庫分享
- SPLK-5002權威考題 □ SPLK-5002真題材料 □ SPLK-5002考證 □ 在⇛ www.newdumpspdf.com ⇚上搜索✔ SPLK-5002 □✔□並獲取免費下載SPLK-5002考古題推薦
- SPLK-5002題庫分享 □ SPLK-5002考試指南 □ SPLK-5002最新考證 □ 來自網站{ www.newdumpspdf.com }打開並搜索✔ SPLK-5002 □✔□免費下載SPLK-5002題庫分享
- SPLK-5002考證 □ SPLK-5002考試資料 □ SPLK-5002考試指南 □ 在➠ www.newdumpspdf.com □搜索最新的▸ SPLK-5002 ◂題庫SPLK-5002最新考證
- 完全包括的SPLK-5002 PDF題庫 |高通過率的考試材料|更新的SPLK-5002考試內容 □ 進入▹ www.pdfexamdumps.com ◃搜尋➤ SPLK-5002 □免費下載SPLK-5002真題
- www.stes.tyc.edu.tw, sachinxrea026123.dreamyblogs.com, www.stes.tyc.edu.tw, darrencpbm241027.muzwiki.com, lexieddhb108875.luwebs.com, socialmarkz.com, www.stes.tyc.edu.tw, nybookmark.com, brendabhbr705674.wikidirective.com, bookmarkquotes.com, Disposable vapes

此外，這些Testpdf SPLK-5002考試題庫的部分內容現在是免費的：https://drive.google.com/open?id=10-_oPrwwsCHku5kYUDRbA0uw9FoSGMJG