SPLK-5002英語版 & SPLK-5002無料問題

P.S. Topexam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=1T2bCzbGja5pk3tN3clU68kjBrNhxTkHC

Topexamは、Splunk Certified Cybersecurity Defense Engineer試験に必要な人向けの安定した信頼できる試験問題プロバイダーです。 私たちは長い間市場に滞在し、成長してきました。SPLK-5002試験問題の優れた品質と高い合格率のため、私たちは常にここにいます。 安全な環境と効果的な製品については、数千人の候補者が私たちの研究の質問を選んでいます。なぜあなたは私たちTopexamの研究の質問に挑戦してみてください。

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	• 検知エンジニアリング：このセクションでは、セキュリティ検知の開発と改良における脅威ハンターとSOCエンジニアの専門知識を評価します。トピックには、相関検索の作成と調整、検知へのコンテキストデータの統合、リスクベースの修飾子の適用、実用的な重要イベントの生成、進化する脅威に適応するための検知ルールのライフサイクル管理などが含まれます。
トピック 2	• 自動化と効率性：このセクションでは、セキュリティ運用の効率化における自動化エンジニアとSOARスペシャリストの能力を評価します。SOP（標準運用手順）の自動化の開発、ケース管理ワークフローの最適化、REST APIの活用、レスポンス自動化のためのSOARプレイブックの設計、Splunk Enterprise SecurityとSOARツールの統合の評価などを網羅します。
トピック 3	• データエンジニアリング：このセクションでは、セキュリティアナリストとサイバーセキュリティエンジニアのスキルを測定し、基本的なデータ管理タスクを網羅します。データのレビューと分析の実行、効率的なデータインデックスの作成と維持、そしてSplunkメソッドを用いたデータ正規化を適用し、セキュリティ運用において構造化され利用可能なデータセットを確保することが含まれます。
トピック 4	• 効果的なセキュリティプロセスとプログラムの構築：このセクションは、セキュリティプログラムマネージャーとコンプライアンス担当者を対象とし、セキュリティワークフローの運用化に焦点を当てています。脅威インテリジェンスの調査と統合、リスクと検知の優先順位付け手法の適用、そして堅牢なセキュリティ対策を維持するためのドキュメントや標準運用手順（SOP）の作成が含まれます。
トピック 5	• セキュリティプログラムの監査と報告：このセクションでは、監査担当者とセキュリティアーキテクトがプログラムの有効性を検証し、伝達する能力をテストします。セキュリティ指標の設計、コンプライアンスレポートの作成、そして関係者向けにプログラムのパフォーマンスと脆弱性を視覚化するダッシュボードの構築などが含まれます。

>> SPLK-5002英語版 <<

試験の準備方法-ユニークなSPLK-5002英語版試験-素晴らしいSPLK-5002無料問題

我々社のSplunk　SPLK-5002認定試験問題集の合格率は高いのでほとんどの受験生はSPLK-5002認定試験に合格するのを保証します。もしあなたはSplunk　SPLK-5002試験問題集に十分な注意を払って、SPLK-5002試験の解答を覚えていれば、SPLK-5002認定試験の成功は明らかになりました。Splunk　SPLK-5002模擬問題集で実際の質問と正確の解答に疑問があれば、無料の練習問題集サンプルをダウンロードし、チェックしてください。

Splunk Certified Cybersecurity Defense Engineer 認定 SPLK-5002 試験問題 (Q55-Q60):

質問 # 55
A security analyst wants to validate whether a newly deployed SOAR playbook is performing as expected.
Whatsteps should they take?

- A. Test the playbook using simulated incidents
- B. Monitor the playbook's actions in real-time environments
- C. Automate all tasks within the playbook immediately
- D. Compare the playbook to existing incident response workflows

正解：A

解説：
A SOAR (Security Orchestration, Automation, and Response) playbook is a set of automated actions designed to respond to security incidents. Before deploying it in a live environment, a security analyst must ensure that it operates correctly, minimizes false positives, and doesn't disrupt business operations.
#Key Reasons for Using Simulated Incidents:
Ensures that the playbook executes correctly and follows the expected workflow.
Identifies false positives or incorrect actions before deployment.
Tests integrations with other security tools (SIEM, firewalls, endpoint security).
Provides a controlled testing environment without affecting production.
How to Test a Playbook in Splunk SOAR?
1##Use the "Test Connectivity" Feature - Ensures that APIs and integrations work.2##Simulate an Incident - Manually trigger an alert similar to a real attack (e.g., phishing email or failed admin login).3##Review the Execution Path - Check each step in the playbook debugger to verify correct actions.4##Analyze Logs & Alerts - Validate that Splunk ES logs, security alerts, and remediation steps are correct.5##Fine-tune Based on Results - Modify the playbook logic to reduce unnecessary alerts or excessive automation.
Why Not the Other Options?
#B. Monitor the playbook's actions in real-time environments - Risky without prior validation. Itcan cause disruptions if the playbook misfires.#C. Automate all tasks immediately - Not best practice. Gradual deployment ensures better security control and monitoring.#D. Compare with existing workflows - Good practice, but it does not validate the playbook's real execution.
References & Learning Resources
#Splunk SOAR Documentation: https://docs.splunk.com/Documentation/SOAR#Testing Playbooks in Splunk SOAR: https://www.splunk.com/en_us/products/soar.html#SOAR Playbook Debugging Best Practices: https://splunkbase.splunk.com

質問 # 56
An effective method for building automation workflows is to follow the OODA (Observe, Orient, Decide, Act) loop stages. When transitioning between the Decide and Act stages, what additional work should be included before automating the Act stage?

- A. Create a new automation playbook.
- B. Create a new response template.
- C. Validate if the asset, identity, or service has an exemption.
- D. Validate response data paths from Decide stage.

正解：C

解説：
Before automating the Act stage of the OODA loop, it is essential to validate whether the asset, identity, or service has an exemption. This ensures that automated actions do not negatively impact business-critical systems or users who are intentionally excluded from automated remediation.

質問 # 57
A company wants to implement risk-based detection for privileged account activities. What should they configure first?

- A. Correlation searches with low thresholds
- B. Asset and identity information for privileged accounts
- C. Automated dashboards for all accounts
- D. Event sampling for raw data

正解：B

解説：
Why Configure Asset & Identity Information for Privileged Accounts First?
Risk-based detection focuses on identifying and prioritizing threats based on the severity of their impact. For privileged accounts (admins, domain controllers, finance users), understanding who they are, what they access, and how they behave is critical.
Key Steps for Risk-Based Detection in Splunk ES:
1. Define Privileged Accounts & Groups - Identify high-risk users (Admin, HR, Finance, CISO).
2. Assign Risk Scores - Apply higher scores to actions involving privileged users.
3. Enable Identity & Asset Correlation - Link users to assets for better detection.
4. Monitor for Anomalies - Detect abnormal login patterns, excessive file access, or unusual privilege escalation.

質問 # 58
What can an engineer use to capture contextual values from a dashboard and create a drilldown to link to a new search?

- A. JSON
- B. Tokens
- C. Aliases
- D. Environment variables

正解：B

解説：
In Splunk dashboards, tokens are used to capture contextual values such as field selections or time ranges. These tokens can then be passed into a drilldown to dynamically link to and populate a new search with the selected context.

質問 # 59
What methods improve the efficiency of Splunk's automation capabilities? (Choose three)

- A. Implementing low-latency indexing
- B. Optimizing correlation search queries
- C. Employing prebuilt SOAR playbooks
- D. Using modular inputs
- E. Leveraging saved search acceleration

正解：B、C、D

解説：
How to Improve Splunk's Automation Efficiency?
Splunk's automation capabilities rely on efficient data ingestion, optimized searches, and automated response workflows. The following methods help improve Splunk's automation:
#1. Using Modular Inputs (Answer A)
Modular inputs allow Splunk to ingest third-party data efficiently (e.g., APIs, cloud services, or security tools).
Benefit: Improves automation by enabling real-time data collection for security workflows.
Example: Using a modular input to ingest threat intelligence feeds and trigger automatic responses.

#2. Optimizing Correlation Search Queries (Answer B)
Well-optimized correlation searches reduce query time and false positives.
Benefit: Faster detections # Triggers automated actions in SOAR with minimal delay.
Example: Usingtstatsinstead of raw searches for efficient event detection.
#3. Employing Prebuilt SOAR Playbooks (Answer E)
SOAR playbooks automate security responses based on predefined workflows.
Benefit: Reduces manual effort in phishing response, malware containment, etc.
Example: Automating phishing email analysis using a SOAR playbook that extracts attachments, checks URLs, and blocks malicious senders.
Why Not the Other Options?
#C. Leveraging saved search acceleration - Helps with dashboard performance, but doesn't directly improve automation.#D. Implementing low-latency indexing - Reduces indexing lag but is not a core automation feature.
References & Learning Resources
#Splunk SOAR Automation Guide: https://docs.splunk.com/Documentation/SOAR#Optimizing Correlation Searches in Splunk ES: https://docs.splunk.com/Documentation/ES#Prebuilt SOAR Playbooks for Security Automation: https://splunkbase.splunk.com

質問 # 60
......

地下鉄でほかの人はぼかんと座っているとき、あなたはPadまたはスマホでPDF版のSplunkのSPLK-5002試験の資料を読むことができます。ほかの人がインタネットでゲームを遊んでいるとき、あなたはオンラインでSplunkのSPLK-5002の問題集をすることができます。このような努力しているあなたは短い時間でSplunkのSPLK-5002試験に合格できると信じています。ほかの人はあなたの成績に驚いているとき、ひょっとしたら、あなたはよりよい仕事を探しましたかもしれません。

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, substack.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, new.learn2azure.com, guangai.nx567.cn, Disposable vapes