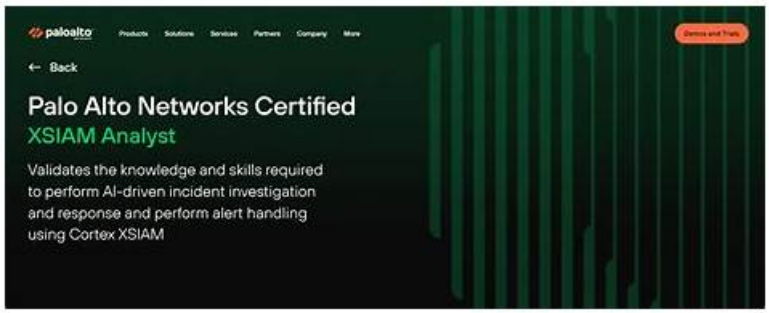
XSIAM-Analyst완벽한덤프 - XSIAM-Analyst최신인증시험기출자료



2026 DumpTOP 최신 XSIAM-Analyst PDF 버전 시험 문제집과 XSIAM-Analyst 시험 문제 및 답변 무료 공유: https://drive.google.com/open?id=1J2qOxLcf-qbv-iTHOoYAjtmG3tJKCEeT

Palo Alto Networks XSIAM-Analyst 시험이 어렵다고해도 DumpTOP의 Palo Alto Networks XSIAM-Analyst시험잡이 덤프가 있는한 아무리 어려운 시험이라도 쉬워집니다. 어려운 시험이라 막무가내로 시험준비하지 마시고 문항수도 적고 모든 시험문제를 커버할수 있는Palo Alto Networks XSIAM-Analyst자료로 대비하세요. 가장 적은 투자로 가장 큰 득을 보실수 있습니다.

Palo Alto Networks XSIAM-Analyst 시험요강:

주제	소개
주제 1	• Endpoint Security Management: This section of the exam measures the skills of Endpoint Security Administrators and focuses on validating endpoint configurations and monitoring activities. It includes managing endpoint profiles and policies, verifying agent status, and responding to endpoint alerts through live terminals, isolation, malware scans, and file retrieval processes.
주제 2	• Alerting and Detection Processes: This section of the exam measures the skills of Security Analysts and focuses on recognizing and managing different types of analytic alerts in the Palo Alto Networks XSIAM platform. It includes alert prioritization, scoring, and incident domain handling. Candidates must demonstrate understanding of configuring custom prioritizations, identifying alert sources like correlations and XDR indicators, and taking corresponding actions to ensure accurate threat detection.
주제 3	• Data Analysis with XQL: This section of the exam measures the skills of Security Data Analysts and covers using the XSIAM Query Language (XQL) to analyze and correlate security data. It involves understanding Cortex Data Models, analyzing events through datasets, and interpreting XQL syntax, schema, and query options such as libraries and scheduled queries.
주제 4	• Automation and Playbooks: This section of the exam measures the skills of SOAR Engineers and focuses on leveraging automation within XSIAM. It includes using playbooks for automated incident response, identifying playbook components like tasks, sub-playbooks, and error handling, and understanding the purpose of the playground environment for testing and debugging automated workflows.

>> XSIAM-Analyst완벽한 덤프 <<

XSIAM-Analyst최신 인증시험 기출자료, XSIAM-Analyst최신버전 덤프데모문제

Palo Alto Networks인증XSIAM-Analyst시험을 패스하여 자격증을 취득한다면 여러분의 미래에 많은 도움이 될 것입니다.Palo Alto Networks인증XSIAM-Analyst시험자격증은 it업계에서도 아주 인지도가 높고 또한 알아주는 시험이며 자격증 하나로도 취직은 문제없다고 볼만큼 가치가 있는 자격증이죠.Palo Alto Networks인증XSIAM-Analyst시험은 여러분이 it지식테스트시험입니다.

최신 Security Operations XSIAM-Analyst 무료샘플문제 (Q110-Q115):

질문 # 110
An analyst conducting a threat hunt needs to collect multiple files from various endpoints. The analyst begins the file retrieval process by using the Action Center, but upon review of the retrieved files, notices that the list is incomplete and missing files, including kernel files.
What could be the reason for the issue?

- A. The analyst must manually retrieve kernel files by accessing the machine directly
- B. The file retrieval policy applied to the endpoints may restrict access to certain system or kernel files
- C. The retrieval process is limited to 500 MB in total file size
- D. The endpoint agents were in offline mode during the file retrieval process, causing some files to be skipped

정답：B

설명:
The correct answer isA - The file retrieval policy applied to the endpoints may restrict access to certain system or kernel files. Cortex XSIAM and XDR implement security policies and permissions that mayrestrict the retrieval of sensitive system files, including kernel files, for safety and compliance reasons. When a file retrieval action is initiated, the endpoint policy controls which files are accessible; kernel and other protected files are often excluded from remote retrieval actions to prevent accidental or unauthorized access.
"The file retrieval policy controls which files can be remotely collected from endpoints. Sensitive files, such as kernel or system files, may be restricted by policy and are not accessible through standard remote retrieval actions." Document Reference:EDU-270c-10-lab-guide_02.docx (1).pdf Exact Page:Page 13 (Agent Deployment and Configuration section)

질문 # 111
Which two methods can be used to create and share queries into the Query Library? (Choose two.)

- A. From the Query Center, locate the query to save to a personal Query Library. Right-click, and select "Save query to library". Enable the "Share with others" option
- B. From XQL Search, locate the query to save to a personal Query Library. Right-click, and select "Save query to library". Enable the "Share with others" option
- C. From XQL Search, in the XQL query field, define the parameters of the query. Save as, and choose the "Query to Library" option. Enable the "Share with others" option
- D. From the Query Center, in the XQL query field, define the parameters of the query. Save as, and choose the "Query to Library" option. Enable the "Share with others" option

정답：B,C

설명:
The correct answers areB and C.
* FromXQL Search, you can save existing queries directly to your personal Query Library and then choose to share them with others by enabling the sharing option.
* You can also build new queries in the XQL Search field, then use "Save as" and select "Query to Library," followed by enabling the "Share with others" option.
"Queries can be created and saved to the Query Library from XQL Search either by saving existing queries or using the 'Save as' feature after building a new query. The 'Share with others' option allows for team collaboration." Document Reference:XSIAM Analyst ILT Lab Guide.pdf Page:Page 25 (Dashboards, Reports, and Widgets section)

질문 # 112
Which Cortex XSIAM feature displays the latest agent health and connection status?
Response:

- A. Incident scoring
- B. Live terminal
- C. Correlation center
- D. Agent monitoring dashboard

정답：D

질문 # 113
What is the primary function of hunting in Cortex XSIAM?
Response:

- A. Searching for indicators across datasets
- B. Uploading endpoint profiles
- C. Creating manual scoring policies
- D. Performing backups

정답：A

질문 # 114
An on-demand malware scan of a Windows workstation using the Cortex XDR agent is successful and detects three malicious files. An analyst attempts further investigation of the files by right-clicking on the scan result, selecting "Additional data," then "View related alerts," but no alerts are reported.
What is the reason for this outcome?

- A. The malware scan action detects malicious files but does not generate alerts for them
- B. The malicious files are currently in an excluded directory in the Malware Profile
- C. The malicious files were true positives and were automatically quarantined from the scan results
- D. The malicious files were false positives and were automatically removed from the scan results

정답：A

설명：
The correct answer isB. The malware scan action detects malicious files but does not generate alerts for them.
In Cortex XSIAM and XDR, an on-demand malware scan effectively identifies malicious files on an endpoint. However, such scans typically record their findings directly in the scan results without generating separate alerts. Alerts are generally created through real-time protection mechanisms or detection rules, not through manually triggered scans.
Exact Reference from Official Document:
"The on-demand malware scan capability is designed to detect and identify malicious files but does not automatically generate alerts for those files. Alerts are primarily generated through real-time endpoint protection policies and detection rules." Therefore, the absence of alerts despite successful malware detection is due to the designed behavior of on- demand scans.

질문 # 115
.....

하십시오XSIAM-Analyst인기덤프문제

- XSIAM-Analyst인기덤프문제 □ XSIAM-Analyst최고품질 시험덤프 공부자료 □ XSIAM-Analyst시험대비 최신 덤프공부자료 □ 지금□ www.itdumpskr.com □에서「 XSIAM-Analyst 」를 검색하고 무료로 다운로드하세요XSIAM-Analyst인기덤프문제
- XSIAM-Analyst최신 인증시험 기출자료 □ XSIAM-Analyst최고품질 시험덤프 공부자료 □ XSIAM-Analyst퍼펙트 최신 덤프공부자료 □ ⇛ www.itdumpskr.com ⇚에서「 XSIAM-Analyst 」를 검색하고 무료 다운로드 받기XSIAM-Analyst덤프샘플문제
- XSIAM-Analyst완벽한 덤프 최신 인증시험정보 □ 검색만 하면▸ www.itdumpskr.com ◂에서{ XSIAM-Analyst } 무료 다운로드XSIAM-Analyst최신시험후기
- XSIAM-Analyst퍼펙트 최신 덤프공부자료 □ XSIAM-Analyst참고자료 □ XSIAM-Analyst시험준비자료 □ ➥ www.pass4test.net □의 무료 다운로드➥ XSIAM-Analyst □페이지가 지금 열립니다XSIAM-Analyst높은 통과율 시험덤프자료
- ncon.edu.sa, gov.elearnzambia.cloud, www.stes.tyc.edu.tw, 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, 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, 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, Disposable vapes

2026 DumpTOP 최신 XSIAM-Analyst PDF 버전 시험 문제집과 XSIAM-Analyst 시험 문제 및 답변 무료 공유: https://drive.google.com/open?id=1J2qOxLcf-qbv-iTHOoYAjtmG3tJKCEeT