Palo Alto Networks XSIAM-Engineer최고품질덤프문제보기, XSIAM-Engineer최신버전시험덤프자료

EXTENDED SECURITY INTELLIGENCE AND AUTOMATION MANAGEMENT
Cortex XSIAM
The AI-Driven SecOps Platform That Goes Beyond Reactive Security
paloalto
CORTEX XSIAM

참고: Pass4Test에서 Google Drive로 공유하는 무료, 최신 XSIAM-Engineer 시험 문제집이 있습니다: https://drive.google.com/open?id=17nHS-QJUz85_wA3XXMRtbHBRG5ItaZT7

우리Pass4Test에서는 각종IT시험에 관심있는분들을 위하여, 여러 가지 인증시험자료를 제공하는 사이트입니다. 우리Pass4Test는 많은 분들이 IT인증시험을 응시하여 성공할수록 도와주는 사이트입니다. 우리의 파워는 아주 대단하답니다. 여러분은 우리Pass4Test 사이트에서 제공하는Palo Alto Networks XSIAM-Engineer관련자료의 일부분문제와답등 샘플을 무료로 다운받아 체험해봄으로 우리에 믿음이 생기게 될 것입니다.

Palo Alto Networks XSIAM-Engineer 시험요강:

주제	소개
주제 1	• Planning and Installation: This section of the exam measures skills of XSIAM Engineers and covers the planning, evaluation, and installation of Palo Alto Networks Cortex XSIAM components. It focuses on assessing existing IT infrastructure, defining deployment requirements for hardware, software, and integrations, and establishing communication needs for XSIAM architecture. Candidates must also configure agents, Broker VMs, and engines, along with managing user roles, permissions, and access controls.
주제 2	• Content Optimization: This section of the exam measures skills of Detection Engineers and focuses on refining XSIAM content and detection logic. It includes deploying parsing and data modeling rules for normalization, managing detection rules based on correlation, IOCs, BIOCs, and attack surface management, and optimizing incident and alert layouts. Candidates must also demonstrate proficiency in creating custom dashboards and reporting templates to support operational visibility.
주제 3	• Maintenance and Troubleshooting: This section of the exam measures skills of Security Operations Engineers and covers post-deployment maintenance and troubleshooting of XSIAM components. It includes managing exception configurations, updating software components such as XDR agents and Broker VMs, and diagnosing data ingestion, normalization, and parsing issues. Candidates must also troubleshoot integrations, automation playbooks, and system performance to ensure operational reliability.
주제 4	• Integration and Automation: This section of the exam measures skills of SIEM Engineers and focuses on data onboarding and automation setup in XSIAM. It covers integrating diverse data sources such as endpoint, network, cloud, and identity, configuring automation feeds like messaging, authentication, and threat intelligence, and implementing Marketplace content packs. It also evaluates the ability to plan, create, customize, and debug playbooks for efficient workflow automation.

>> Palo Alto Networks XSIAM-Engineer최고품질 덤프문제보기 <<

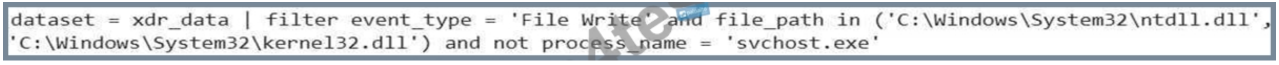
XSIAM-Engineer최신버전 시험덤프자료 & XSIAM-Engineer높은 통과율 덤프데모문제

Pass4Test를 선택함으로, Pass4Test는 여러분Palo Alto Networks인증XSIAM-Engineer시험을 패스할 수 있도록 보장하고,만약 시험실패시 Pass4Test에서는 덤프비용전액환불을 약속합니다.

최신 Security Operations XSIAM-Engineer 무료샘플문제 (Q195-Q200):

질문 # 195

An XSIAM engineer is investigating a persistent alert from an indicator rule that flags 'attempts to modify critical system files.' The rule's current XQL is:



```
dataset = xdr_data | filter event_type = 'File Write' and file_path in ('C:\Windows\System32\ntdll.dll',
'C:\Windows\System32\kernel32.dll') and not process_name = 'svchost.exe'
```

After analysis, it's determined that legitimate patching and antivirus updates are triggering these alerts. How should the engineer refine this rule to eliminate these false positives while preserving detection of malicious activity?

- A. Modify the XQL to include a check for the 'digital_signature' of the process performing the write, ensuring it's not signed by Microsoft or the organization's trusted vendors, specifically for update/patch processes.
- B. Remove the rule, as critical system file modification is too noisy to reliably detect with indicator rules.
- C. Add 'and not (process_name in ('msiexec.exe', 'wusa.exe') and parent_process_name = ' TrustedInstaller.exe')' to the XQL query.
- D. Change the 'file_path' to only look for executable files with a .exe' extension, ignoring DLLs.
- E. Filter by and exclude 'SYSTEM' user, as legitimate updates often run as SYSTEM.

정답： A

설명：

Option C is the most effective and robust solution for handling legitimate updates. Digital Signatures: Legitimate patching and antivirus updates are almost always performed by digitally signed executables from trusted vendors (like Microsoft for OS updates, or a reputable AV vendor). By filtering based on the absence of a valid, trusted digital signature, you can effectively distinguish legitimate updates from malicious attempts to modify system files. This is a high-fidelity filter. Option A is a surrender. Option B is a partial solution, as patchers and installers can use various processes and parent processes, and 'TrustedInstaller.exe' might not always be the direct parent, also it's often more reliable to use signatures. Option D would eliminate many legitimate updates, as SYSTEM often performs these, and also miss malicious activity by SYSTEM. Option E would completely miss malicious modifications to critical DLLS, which is a common technique.

질문 # 196

Which section of a parsing rule defines the newly created dataset?

- A. CONST
- B. COLLECT
- C. INGEST
- D. RULE

정답： B

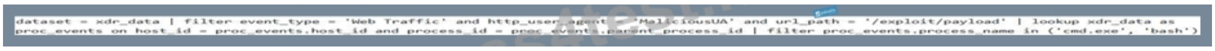
설명：

In a Cortex XSIAM parsing rule, the COLLECT section defines the newly created dataset. This section specifies how the parsed fields and data should be structured and stored for further use in analytics and queries.

질문 # 197

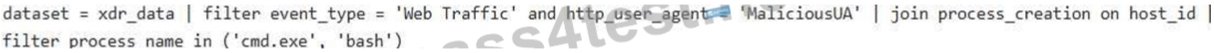
A new zero-day exploit targeting a widely used web server application has been announced. Your XSIAM deployment needs to rapidly deploy an indicator rule to detect exploitation attempts. You receive the following highly specific indicators of compromise (IOCs): a unique HTTP User-Agent string, a specific URL path with a known malicious payload, and a suspicious process execution (e.g., 'cmd.exe' or 'bash') initiated by the web server process. Which XQL query structure would be most appropriate for a robust indicator rule in XSIAM to detect this attack, ensuring high fidelity?

- A.



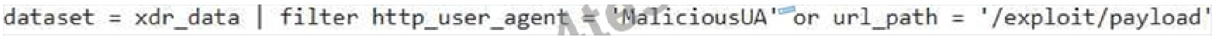
```
dataset = xdr_data | filter event_type = 'Web Traffic' and http_user_agent = 'MaliciousUA' and url_path = '/exploit/payload' | lookup xdr_data as
proc_events on host_id = proc_events.host_id and process_id = proc_events.parent_process_id | filter proc_events.process_name in ('cmd.exe', 'bash')
```

- B.



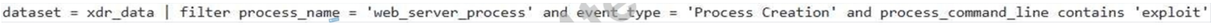
```
dataset = xdr_data | filter event_type = 'Web Traffic' and http_user_agent = 'MaliciousUA' | join process_creation on host_id |
filter process name in ('cmd.exe', 'bash')
```

- C.

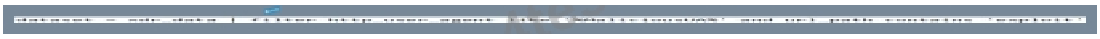


```
dataset = xdr_data | filter http_user_agent = 'MaliciousUA' or url_path = '/exploit/payload'
```

- D.



```
dataset = xdr_data | filter process_name = 'web_server_process' and event_type = 'Process Creation' and process_command_line contains 'exploit'
```

- E. 

```
dataset = xdr_data | filter http_user_agent like 'MaliciousUA' and url_path contains 'exploit'
```

정답： A

설명:
Option C provides the most robust and high-fidelity detection. It correctly combines all three IOCs using logical 'AND' operations, which is crucial for reducing false positives in specific attack scenarios. It specifically looks for 'Web Traffic' events with the specified User-Agent and URL, and then uses a 'lookup' (or a similar join logic, though ' lookup' is often more performant for correlating disparate event types like web traffic and process creation) to find process creations where the parent process initiated the web traffic and the child process is suspicious (cmd.exe or bash). This multi-stage correlation significantly reduces false positives. Options A, B, D, and E either miss critical correlations or are too broad.

질문 # 198
A large financial institution is planning to deploy Palo Alto Networks XSIAM to centralize security operations and automate threat response. A key requirement is to ingest massive volumes of security telemetry from existing SIEM, EDR, network devices, and cloud logs, with a stringent RTO of 15 minutes for critical incidents. Which of the following XSIAM deployment considerations is MOST critical to evaluate initially to meet these requirements?

- A. Evaluating the existing security team's proficiency in XSIAM's AQL and SOAR playbooks.
- B. Optimizing Cortex Data Lake (CDL) retention policies for compliance and cost efficiency.
- C. Planning for custom XSIAM content development, including dashboards and reports, for executive visibility.
- D. Assessing the network bandwidth and latency between data sources, XSIAM tenants, and CDL locations.
- E. Defining a comprehensive playbook library for automated incident response workflows.

정답： D

설명:
The most critical initial consideration for ingesting massive data volumes with a stringent RTO is the underlying network infrastructure. Inadequate bandwidth or high latency will directly impact data ingestion rates and the ability to process and respond to incidents within the desired timeframe. While other options are important, they are secondary to ensuring the data can actually reach XSIAM effectively. CDL retention (A) is for storage, playbook definition (B) is for response logic, team proficiency (D) is for operationalization, and content development (E) is for reporting, all of which are downstream from data ingestion.

질문 # 199
What should be considered when creating a custom incident domain?

- A. Alert grouping will apply, but SmartScore will not.
- B. Alert grouping and SmartScore will not be applied to incidents.
- C. Alert grouping will not apply, but SmartScore will.
- D. Alert grouping and SmartScore will be applied to incidents.

정답： A

설명:
When creating a custom incident domain in Cortex XSIAM, alert grouping still applies, allowing related alerts to be combined into incidents. However, SmartScore is not applied, since it is reserved for predefined domains.

질문 # 200
......

Pass4Test는 여러분이 빠른 시일 내에Palo Alto Networks XSIAM-Engineer인증시험을 효과적으로 터득할 수 있는 사이트입니다.Palo Alto Networks XSIAM-Engineer인증 자격증은 일상생활에 많은 개변을 가져올 수 있는 시험입니다.Palo Alto Networks XSIAM-Engineer인증 자격증을 소지한 자들은 당연히 없는 자들보다 연봉이 더 높을 거고 승진 기회도 많아지며 IT업계에서의 발전도 무궁무진합니다.

XSIAM-Engineer최신버전 시험덤프자료: https://www.pass4test.net/XSIAM-Engineer.html

- 완벽한 XSIAM-Engineer최고품질 덤프문제보기 인증덤프 □ ➽ www.pass4test.net □에서 검색만 하면（ XSIAM-Engineer ）를 무료로 다운로드할 수 있습니다XSIAM-Engineer퍼펙트 최신버전 덤프
- 시험준비에 가장 좋은 XSIAM-Engineer최고품질 덤프문제보기 최신 덤프문제 ✳ 지금《 www.itdumpskr.com 》에서□ XSIAM-Engineer □를 검색하고 무료로 다운로드하세요XSIAM-Engineer완벽한 덤프공부자료
- 최신 XSIAM-Engineer최고품질 덤프문제보기 인증 시험덤프 □ 시험 자료를 무료로 다운로드하려면➤ www.koreadumps.com □을 통해《 XSIAM-Engineer 》를 검색하십시오XSIAM-Engineer최신 시험 기출문제 모음
- 시험패스 가능한 XSIAM-Engineer최고품질 덤프문제보기 최신 덤프공부자료 □ ▶ www.itdumpskr.com ◀웹사이트를 열고□ XSIAM-Engineer □를 검색하여 무료 다운로드XSIAM-Engineer시험대비 덤프공부문제
- XSIAM-Engineer퍼펙트 최신버전 덤프 □ XSIAM-Engineer높은 통과율 덤프공부자료 □ XSIAM-Engineer최고합격덤프 □ ➥ kr.fast2test.com □은➥ XSIAM-Engineer □무료 다운로드를 받을 수 있는 최고의 사이트입니다XSIAM-Engineer질문과 답
- XSIAM-Engineer최신 덤프문제보기 □ XSIAM-Engineer시험대비 공부자료 □ XSIAM-Engineer시험응시료 □ □（ www.itdumpskr.com ）을 통해 쉽게“ XSIAM-Engineer ”무료 다운로드 받기XSIAM-Engineer최신 시험 기출문제 모음
- 최신 업데이트된 XSIAM-Engineer최고품질 덤프문제보기 인증덤프자료 □ 무료 다운로드를 위해➡ XSIAM-Engineer □□□를 검색하려면▹ kr.fast2test.com ◃을(를) 입력하십시오XSIAM-Engineer시험대비 덤프데모문제
- XSIAM-Engineer최신 시험 기출문제 모음 □ XSIAM-Engineer최신버전 시험대비 공부자료 □ XSIAM-Engineer시험응시료 □（ www.itdumpskr.com ）을 통해 쉽게（ XSIAM-Engineer ）무료 다운로드 받기XSIAM-Engineer시험대비 공부자료
- XSIAM-Engineer최신버전 시험대비 공부자료 □ XSIAM-Engineer시험패스 □ XSIAM-Engineer최신버전 시험대비 공부자료 □ “ www.koreadumps.com ”은{ XSIAM-Engineer }무료 다운로드를 받을 수 있는 최고의 사이트입니다XSIAM-Engineer최신 업데이트 인증시험자료
- XSIAM-Engineer최고품질 시험대비자료 □ XSIAM-Engineer시험패스 □ XSIAM-Engineer시험대비 공부자료 □ □ ➠ www.itdumpskr.com □에서【 XSIAM-Engineer 】를 검색하고 무료로 다운로드하세요XSIAM-Engineer완벽한 덤프공부자료
- XSIAM-Engineer퍼펙트 덤프 최신버전 □ XSIAM-Engineer유효한 최신덤프 □ XSIAM-Engineer완벽한 덤프공부자료 □ ➤ www.pass4test.net □에서☀ XSIAM-Engineer □☀□를 검색하고 무료로 다운로드하세요XSIAM-Engineer높은 통과율 덤프공부자료
- myportal.utt.edu.tt, www.stes.tyc.edu.tw, myportal.utt.edu.tt, www.stes.tyc.edu.tw, app.csicosnet.com, 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, Disposable vapes

Pass4Test XSIAM-Engineer 최신 PDF 버전 시험 문제집을 무료로 Google Drive에서 다운로드하세요: https://drive.google.com/open?id=17nHS-QJUz85_wA3XXMRtbHBRG5ItaZT7