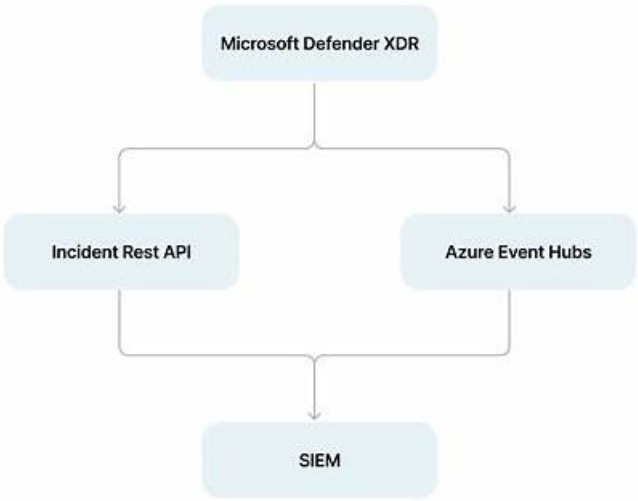
# XDR-Analyst최신버전시험공부 & XDR-Analyst최고기출문제




DumpTOP XDR-Analyst 최신 PDF 버전 시험 문제집을 무료로 Google Drive에서 다운로드하세요: https://drive.google.com/open?id=1CVLiIvmlGh3Lsu9zaoikIF6grCefFHCY

Palo Alto Networks XDR-Analyst시험이 정말 어렵다는 말을 많이 들으신 만큼 저희 DumpTOP는Palo Alto Networks XDR-Analyst덤프만 있으면Palo Alto Networks XDR-Analyst시험이 정말 쉬워진다고 전해드리고 싶습니다. Palo Alto Networks XDR-Analyst덤프로 시험패스하고 자격증 한방에 따보세요. 자격증 많이 취득하면 더욱 여유롭게 직장생활을 즐길수 있습니다.

Palo Alto Networks XDR-Analyst덤프의 유효성을 보장해드릴수 있도록 저희 기술팀은 오랜시간동안Palo Alto Networks XDR-Analyst시험에 대하여 분석하고 연구해 왔습니다. Palo Alto Networks XDR-Analyst 덤프를 한번 믿고 Palo Alto Networks XDR-Analyst시험에 두려움없이 맞서보세요. 만족할수 있는 좋은 성적을 얻게 될것입니다.

**>> XDR-Analyst최신버전 시험공부 <<**

## Palo Alto Networks XDR-Analyst최고기출문제, XDR-Analyst유효한 인증덤프

DumpTOP에서 출시한 Palo Alto Networks인증XDR-Analyst 덤프는 시험문제적유율이 가장 높은 시험대비자료입니다. 실제Palo Alto Networks인증XDR-Analyst시험문제유형과 같은 형식으로 제작된Palo Alto Networks인증XDR-Analyst 시험공부자료로서DumpTOP덤프의 실용가치를 자랑하고 있습니다.덤프를 공부하여 시험불합격하시면 덤프비용은 환불처리해드립니다.

## Palo Alto Networks XDR-Analyst 시험요강:

| 주제 | 소개 |
|---|---|
| 주제 1 | • Endpoint Security Management: This domain addresses managing endpoint prevention profiles and policies, validating agent operational states, and assessing the impact of agent versions and content updates. |

| | |
|---|---|
| 주제 2 | • Incident Handling and Response: This domain focuses on investigating alerts using forensics, causality chains and timelines, analyzing security incidents, executing response actions including automated remediation, and managing exclusions. |
| 주제 3 | • Data Analysis: This domain encompasses querying data with XQL language, utilizing query templates and libraries, working with lookup tables, hunting for IOCs, using Cortex XDR dashboards, and understanding data retention and Host Insights. |
| 주제 4 | • Alerting and Detection Processes: This domain covers identifying alert types and sources, prioritizing alerts through scoring and custom configurations, creating incidents, and grouping alerts with data stitching techniques. |

## 최신 Security Operations XDR-Analyst 무료샘플문제 (Q70-Q75):

**질문 # 70**
Which statement is true for Application Exploits and Kernel Exploits?

- A. The ultimate goal of any exploit is to reach the kernel.
- B. Kernel exploits are easier to prevent then application exploits.
- C. Application exploits leverage kernel vulnerability.
- D. The ultimate goal of any exploit is to reach the application.

**정답： A**

**설명:**
The ultimate goal of any exploit is to reach the kernel, which is the core component of the operating system that has the highest level of privileges and access to the hardware resources. Application exploits are attacks that target vulnerabilities in specific applications, such as web browsers, email clients, or office suites. Kernel exploits are attacks that target vulnerabilities in the kernel itself, such as memory corruption, privilege escalation, or code execution. Kernel exploits are more difficult to prevent and detect than application exploits, because they can bypass security mechanisms and hide their presence from the user and the system. Reference:
Palo Alto Networks Certified Detection and Remediation Analyst (PCDRA) Study Guide, page 8 Palo Alto Networks Cortex XDR Documentation, Exploit Protection Overview

**질문 # 71**
When selecting multiple Incidents at a time, what options are available from the menu when a user right-clicks the incidents? (Choose two.)

- A. Investigate several Incidents at once.
- B. Change the status of multiple incidents.
- C. Assign incidents to an analyst in bulk.
- D. Delete the selected Incidents.

**정답： B,C**

**설명:**
When selecting multiple incidents at a time, the options that are available from the menu when a user right-clicks the incidents are: Assign incidents to an analyst in bulk and Change the status of multiple incidents. These options allow the user to perform bulk actions on the selected incidents, such as assigning them to a specific analyst or changing their status to open, in progress, resolved, or closed. These options can help the user to manage and prioritize the incidents more efficiently and effectively. To use these options, the user needs to select the incidents from the incident table, right-click on them, and choose the desired option from the menu. The user can also use keyboard shortcuts to perform these actions, such as Ctrl+A to select all incidents, Ctrl+Shift+A to assign incidents to an analyst, and Ctrl+Shift+S to change the status of incidents12 Reference:
Assign Incidents to an Analyst in Bulk
Change the Status of Multiple Incidents

**질문 # 72**

Which license is required when deploying Cortex XDR agent on Kubernetes Clusters as a DaemonSet?

- A. Host Insights
- B. Cortex XDR Pro per Endpoint
- C. Cortex XDR Pro per TB
- D. Cortex XDR Cloud per Host

**정답： D**

**설명：**
When deploying Cortex XDR agent on Kubernetes clusters as a DaemonSet, the license required is Cortex XDR Cloud per Host. This license allows you to protect and monitor your cloud workloads, such as Kubernetes clusters, containers, and serverless functions, using Cortex XDR. With Cortex XDR Cloud per Host license, you can deploy Cortex XDR agents as DaemonSets on your Kubernetes clusters, which ensures that every node in the cluster runs a copy of the agent. The Cortex XDR agent collects and sends data from the Kubernetes cluster, such as pod events, container logs, and network traffic, to the Cortex Data Lake for analysis and correlation. Cortex XDR can then detect and respond to threats across your cloud environment, and provide visibility and context into your cloud workloads. The Cortex XDR Cloud per Host license is based on the number of hosts that run the Cortex XDR agent, regardless of the number of containers or functions on each host. A host is defined as a virtual machine, a physical server, or a Kubernetes node that runs the Cortex XDR agent. You can read more about the Cortex XDR Cloud per Host license and how to deploy Cortex XDR agent on Kubernetes clusters here1 and here2. Reference:
Cortex XDR Cloud per Host License
Deploy Cortex XDR Agent on Kubernetes Clusters as a DaemonSet

**질문 # 73**
Where would you go to add an exception to exclude a specific file hash from examination by the Malware profile for a Windows endpoint?

- A. In the Action Center, choose Allow list, select new action, select add to allow list, add your hash to the list, and apply it.
- B. From the rules menu select new exception, fill out the criteria, choose the scope to apply it to, hit save.
- C. Find the Malware profile attached to the endpoint, Under Portable Executable and DLL Examination add the hash to the allow list.
- D. Find the exceptions profile attached to the endpoint, under process exceptions select local analysis, paste the hash and save.

**정답： A**

**설명：**
To add an exception to exclude a specific file hash from examination by the Malware profile for a Windows endpoint, you need to use the Action Center in Cortex XDR. The Action Center allows you to create and manage actions that apply to endpoints, such as adding files or processes to the allow list or block list, isolating or unisolating endpoints, or initiating live terminal sessions. To add a file hash to the allow list, you need to choose Allow list, select new action, select add to allow list, add your hash to the list, and apply it. This will prevent the Malware profile from scanning or blocking the file on the endpoints that match the scope of the action.
Reference: Cortex XDR 3: Responding to Attacks1, Action Center2

**질문 # 74**
What are two purposes of "Respond to Malicious Causality Chains" in a Cortex XDR Windows Malware profile? (Choose two.)

- A. Automatically kill the processes involved in malicious activity.
- B. Automatically block the IP addresses involved in malicious traffic.
- C. Automatically terminate the threads involved in malicious activity.
- D. Automatically close the connections involved in malicious traffic.

**정답： A,B**

**질문 # 75**
.....

부 문제와 답을 다운하여 체험해보시고 결정을 내리시길 바랍니다.그러면 우리의 덤프에 믿음이;갈 것이고,우리 또한 우리의 문제와 답들은 무조건 100%통과 율로 아주 고득점으로Palo Alto Networks인증XDR-Analyst험을 패스하실 수 있습니다,

**XDR-Analyst최고기출문제**: https://www.dumptop.com/Palo-Alto-Networks/XDR-Analyst-dump.html

- 높은 통과율 XDR-Analyst최신버전 시험공부 공부문제 □ [ www.exampassdump.com ]을(를) 열고□ XDR-Analyst □를 입력하고 무료 다운로드를 받으십시오XDR-Analyst시험패스 인증덤프문제
- XDR-Analyst시험덤프샘플 □ XDR-Analyst시험대비 덤프데모 □ XDR-Analyst높은 통과율 시험공부 □ 검색만 하면[ www.itdumpskr.com ]에서□ XDR-Analyst □무료 다운로드XDR-Analyst인기자격증
- 최신 XDR-Analyst최신버전 시험공부 시험자료 ✳ “www.koreadumps.com”웹사이트를 열고➽ XDR-Analyst □를 검색하여 무료 다운로드XDR-Analyst합격보장 가능 덤프자료
- 최신버전 XDR-Analyst최신버전 시험공부 완벽한 시험 최신버전 덤프 ➽ 오픈 웹 사이트□ www.itdumpskr.com □검색[ XDR-Analyst ]무료 다운로드XDR-Analyst인증시험대비자료
- XDR-Analyst응시자료 □ XDR-Analyst최신 업데이트 덤프문제 □ XDR-Analyst높은 통과율 시험자료 □ ➤ www.koreadumps.com □에서「 XDR-Analyst 」를 검색하고 무료로 다운로드하세요XDR-Analyst시험대비 덤프문제
- 최신 XDR-Analyst최신버전 시험공부 시험자료 □ 무료 다운로드를 위해 지금「 www.itdumpskr.com 」에서□ XDR-Analyst □검색XDR-Analyst시험패스 가능 공부자료
- XDR-Analyst유효한 최신덤프자료 □ XDR-Analyst인증덤프 샘플 다운로드 □ XDR-Analyst퍼펙트 최신버전 덤프 □ 지금☀ www.pass4test.net □☀□에서□ XDR-Analyst □를 검색하고 무료로 다운로드하세요XDR-Analyst완벽한 시험공부자료
- XDR-Analyst응시자료 □ XDR-Analyst시험패스 가능 공부자료 □ XDR-Analyst합격보장 가능 덤프자료 □ 【 www.itdumpskr.com 】웹사이트를 열고⇒ XDR-Analyst ⇐를 검색하여 무료 다운로드XDR-Analyst합격보장 가능 덤프자료
- 높은 통과율 XDR-Analyst최신버전 시험공부 공부문제 □ ➡ kr.fast2test.com □□□에서➥ XDR-Analyst □를 검색하고 무료 다운로드 받기XDR-Analyst퍼펙트 최신버전 덤프
- 시험준비에 가장 좋은 XDR-Analyst최신버전 시험공부 공부자료 ❤ 무료 다운로드를 위해➡ XDR-Analyst □□□를 검색하려면「 www.itdumpskr.com 」을(를) 입력하십시오XDR-Analyst퍼펙트 최신버전 덤프
- XDR-Analyst인기자격증 👆 XDR-Analyst합격보장 가능 덤프자료 □ XDR-Analyst시험대비 덤프문제 □ ➥ www.itdumpskr.com □의 무료 다운로드“XDR-Analyst”페이지가 지금 열립니다XDR-Analyst완벽한 시험공부자료
- 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, bbs.t-firefly.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, 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, Disposable vapes

참고: DumpTOP에서 Google Drive로 공유하는 무료, 최신 XDR-Analyst 시험 문제집이 있습니다: https://drive.google.com/open?id=1CVLiIvmlGh3Lsu9zaoikIF6grCefFHCY