更新するXDR-Analyst赤本勉強 &合格スムーズXDR-Analyst資格講座 |信頼的なXDR-Analyst最新テスト

XDR-Analystガイドトレントの3つの異なるバージョンの中で最も普及しているのはPDFバージョンであり、Palo Alto Networksは特に適切であり、若者に歓迎されていることは間違いありません。このバージョンにはいくつかの機能があります。まず、XDR-Analyst準備ガイドのPDFバージョンを紙に印刷できます。ただし、メモを作成して重要な試験ポイントを強調することができます。前述のように、XDR-Analyst試験トレントサポート無料のデモダウンロードに加えて、XDR-Analyst準備ガイドを十分に理解し、適切で満足できる場合は購入することが理想的です。

Palo Alto Networks XDR-Analyst 認定試験の出題範囲:

トピック	出題範囲
トピック 1	• アラートおよび検出プロセス: このドメインでは、アラートの種類とソースの識別、スコアリングとカスタム構成によるアラートの優先順位付け、インシデントの作成、データステッチング手法によるアラートのグループ化について説明します。
トピック 2	• インシデントの処理と対応: このドメインは、フォレンジック、因果関係の連鎖、タイムラインを使用したアラートの調査、セキュリティ インシデントの分析、自動修復などの対応アクションの実行、除外の管理に重点を置いています。
トピック 3	• データ分析: このドメインには、XQL 言語を使用したデータのクエリ、クエリ テンプレートとライブラリの利用、ルックアップ テーブルの操作、IOC の検索、Cortex XDR ダッシュボードの使用、データ保持とホスト インサイトの理解が含まれます。
トピック 4	• エンドポイント セキュリティ管理: このドメインでは、エンドポイント防止プロファイルとポリシーの管理、エージェントの動作状態の検証、エージェントのバージョンとコンテンツの更新の影響の評価について説明します。

>> XDR-Analyst赤本勉強 <<

完璧なXDR-Analyst赤本勉強 & 合格スムーズXDR-Analyst資格講座 | 効果的なXDR-Analyst最新テスト

Palo Alto Networksの認証資格は最近ますます人気になっていますね。国際的に認可された資格として、Palo Alto Networksの認定試験を受ける人も多くなっています。その中で、XDR-Analyst認定試験は最も重要な一つです。では、この試験に合格するためにどのように試験の準備をしているのですか。がむしゃらに試験に関連する知識を勉強しているのですか。それとも、効率が良い試験XDR-Analyst参考書を使っているのですか。

Palo Alto Networks XDR Analyst 認定 XDR-Analyst 試験問題 (Q69-Q74):

質問 # 69
Which profiles can the user use to configure malware protection in the Cortex XDR console?

- A. Malware Detection profile
- B. Malware Protection profile
- C. Anti-Malware profile
- D. Malware profile

正解：B

解説：
The user can use the Malware Protection profile to configure malware protection in the Cortex XDR console. The Malware Protection profile defines the actions that Cortex XDR takes when it detects malware on your endpoints. You can configure different actions for different types of malware, such as ransomware, password theft, or child process. You can also configure the scan frequency and scope for periodic malware scans. The Malware Protection profile is part of the Endpoint Security policy that you assign to your endpoints. Reference:
Malware Protection Profile
Endpoint Security Policy

質問 # 70
Which license is required when deploying Cortex XDR agent on Kubernetes Clusters as a DaemonSet?

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

正解：B

解説：
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

質問 # 71
Which statement best describes how Behavioral Threat Protection (BTP) works?

- A. BTP matches EDR data with rules provided by Cortex XDR.
- B. BTP uses machine Learning to recognize malicious activity even if it is not known.
- C. BTP injects into known vulnerable processes to detect malicious activity.
- D. BTP runs on the Cortex XDR and distributes behavioral signatures to all agents.

正解：B

解説：
The statement that best describes how Behavioral Threat Protection (BTP) works is D, BTP uses machine learning to recognize malicious activity even if it is not known. BTP is a feature of Cortex XDR that allows you to define custom rules to detect and block malicious behaviors on endpoints. BTP uses machine learning to profile behavior and detect anomalies indicative of attack. BTP can

recognize malicious activity based on file attributes, registry keys, processes, network connections, and other criteria, even if the activity is not associated with any known malware or threat. BTP rules are updated through content updates and can be managed from the Cortex XDR console.
The other statements are incorrect for the following reasons:
A is incorrect because BTP does not inject into known vulnerable processes to detect malicious activity. BTP does not rely on process injection, which is a technique used by some malware to hide or execute code within another process. BTP monitors the behavior of all processes on the endpoint, regardless of their vulnerability status, and compares them with the BTP rules.
B is incorrect because BTP does not run on the Cortex XDR and distribute behavioral signatures to all agents. BTP runs on the Cortex XDR agent, which is installed on the endpoint, and analyzes the endpoint data locally. BTP does not use behavioral signatures, which are predefined patterns of malicious behavior, but rather uses machine learning to identify anomalies and deviations from normal behavior.
C is incorrect because BTP does not match EDR data with rules provided by Cortex XDR. BTP is part of the EDR (Endpoint Detection and Response) capabilities of Cortex XDR, and uses the EDR data collected by the Cortex XDR agent to perform behavioral analysis. BTP does not match the EDR data with rules provided by Cortex XDR, but rather applies the BTP rules defined by the Cortex XDR administrator or the Palo Alto Networks threat research team.
Reference:
Cortex XDR Agent Administrator Guide: Behavioral Threat Protection
Cortex XDR: Stop Breaches with AI-Powered Cybersecurity

質問 # 72
What is the purpose of the Cortex Data Lake?

- A. the workspace for your Cortex XDR agents to detonate potential malware files
- B. a local storage facility where your logs and alert data can be aggregated
- C. the interface between firewalls and the Cortex XDR agents
- D. a cloud-based storage facility where your firewall logs are stored

正解：D

解説：
The purpose of the Cortex Data Lake is to provide a cloud-based storage facility where your firewall logs are stored. Cortex Data Lake is a service that collects, transforms, and integrates your enterprise's security data to enable Palo Alto Networks solutions. It powers AI and machine learning, detection accuracy, and app and service innovation. Cortex Data Lake automatically collects, integrates, and normalizes data across your security infrastructure, including your next-generation firewalls, Prisma Access, and Cortex XDR. With unified data, you can run advanced AI and machine learning to radically simplify security operations with apps built on Cortex. Cortex Data Lake is available in multiple regions and supports data residency and privacy requirements. Reference:
Cortex Data Lake - Palo Alto Networks
Cortex Data Lake - Palo Alto Networks
Cortex Data Lake, the technology behind Cortex XDR - Palo Alto Networks CORTEX DATA LAKE - Palo Alto Networks
Sizing for Cortex Data Lake Storage - Palo Alto Networks

質問 # 73
What functionality of the Broker VM would you use to ingest third-party firewall logs to the Cortex Data Lake?

- A. Pathfinder
- B. Netflow Collector
- C. Syslog Collector
- D. DB Collector

正解：C

解説：
The Broker VM is a virtual machine that acts as a data broker between third-party data sources and the Cortex Data Lake. It can ingest different types of data, such as syslog, netflow, database, and pathfinder. The Syslog Collector functionality of the Broker VM allows it to receive syslog messages from third-party devices, such as firewalls, routers, switches, and servers, and forward them to the Cortex Data Lake. The Syslog Collector can be configured to filter, parse, and enrich the syslog messages before sending them to the Cortex Data Lake. The Syslog Collector can also be used to ingest logs from third-party firewall vendors, such as Cisco, Fortinet, and Check Point, to the Cortex Data Lake. This enables Cortex XDR to analyze the firewall logs and provide visibility and threat detection across the network perimeter. Reference:

Cortex XDR Data Broker VM
Syslog Collector
Supported Third-Party Firewall Vendors

質問 # 74
......