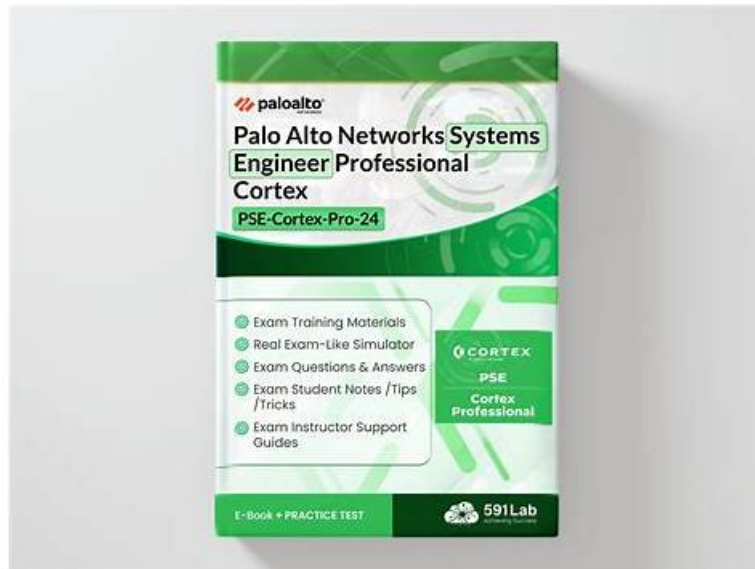


Palo Alto Networks System Engineer - Cortex Professional latest Pass4sures torrent & PSE-Cortex pdf vce collection



P.S. Free & New PSE-Cortex dumps are available on Google Drive shared by Easy4Engine: https://drive.google.com/open?id=1kmobfOsBRpUB-zSV6ha_BrqhV6BDHbY

PDF design has versatile and printable material for Palo Alto Networks PSE-Cortex certification, so you all can breeze through the Palo Alto Networks PSE-Cortex exam without any problem. You can get to the PDF concentrate on material from workstations, tablets, and cell phones for the readiness of Palo Alto Networks System Engineer - Cortex Professional (PSE-Cortex) exam.

The PSE-Cortex Certification is an excellent opportunity for those who wish to advance their careers in the Palo Alto Networks System Engineer - Cortex field. PSE-Cortex exam covers a wide range of topics related to the Cortex platform and is designed to test the candidate's understanding of Cortex functionalities and features. Palo Alto Networks System Engineer - Cortex Professional certification is highly valued in the industry and is recognized as a benchmark for excellence in the Cortex space.

>> **Reliable PSE-Cortex Mock Test** <<

Reliable PSE-Cortex Dumps Book | PSE-Cortex Latest Mock Exam

Our web-based practice exam software is an online version of the Palo Alto Networks PSE-Cortex practice test. It is also quite useful for instances when you have internet access and spare time for study. To study and pass the certification exam on the first attempt, our Palo Alto Networks PSE-Cortex Practice Test software is your best option. You will go through Palo Alto Networks PSE-Cortex exams and will see for yourself the difference in your preparation.

Palo Alto Networks System Engineer - Cortex Professional Sample Questions (Q105-Q110):

NEW QUESTION # 105

A test for a Microsoft exploit has been planned. After some research Internet Explorer 11 CVE-2016-0189 has been selected and a module in Metasploit has been identified (exploit/windows/browser/ms16_051_vbscript) The description and current configuration of the exploit are as follows;

What is the remaining configuration?

- A)
- B)
- C)
-

D)

- A. Option B
- B. Option A
- C. Option D
- D. Option C

Answer: C

NEW QUESTION # 106

What is the size of the free Cortex Data Lake instance provided to a customer who has activated a TMS tenant, but has not purchased a Cortex Data Lake instance?

- A. 100 GB
- B. 10 TB
- C. 10 GB
- D. 1 TB

Answer: A

Explanation:

Cortex Data Lake (often referred to as Strata Logging Service in some contexts) is Palo Alto Networks' cloud-based storage solution that centralizes security data for products like Cortex XDR, Prisma Access, and NGFWs. The question involves a customer who has activated a TMS (Tenant Management Service) tenant but has not purchased a Cortex Data Lake instance. TMS is part of the Palo Alto Networks ecosystem for managing tenants and services, typically associated with Cortex or Prisma deployments. Let's break this down to determine the size of the free Cortex Data Lake instance provided in this scenario.

Understanding TMS and Cortex Data Lake:

* TMS Tenant: The Tenant Management Service is a framework used to manage multiple tenants or instances within Palo Alto Networks' cloud services (e.g., Cortex XDR, Prisma Access). Activating a TMS tenant implies the customer has initialized a management structure but hasn't committed to a full Cortex Data Lake purchase.

* Free Cortex Data Lake Instance: Palo Alto Networks provides a limited, free tier of Cortex Data Lake storage to customers who activate certain services or products, allowing them to evaluate functionality or store minimal data before committing to a paid license.

Free Storage Allocation:

When a customer activates a TMS tenant without purchasing a Cortex Data Lake instance, Palo Alto Networks allocates a default free storage capacity to enable basic functionality. According to official documentation and standard practices:

* The free Cortex Data Lake instance provides 100 GB of storage.

* This amount is intended for initial use cases, such as storing logs from a small number of endpoints (e.g., Cortex XDR Prevent agents), firewall logs, or trial data during evaluation periods.

Option Analysis:

* A. 10 GB:

* Analysis: 10 GB is too small to be a meaningful free tier for a product like Cortex Data Lake, which is designed to handle security telemetry from endpoints, networks, or cloud services. Even basic log storage for a few devices over a short period would exceed this quickly.

* Conclusion: Incorrect.

* B. 1 TB:

* Analysis: 1 TB (1,000 GB) is a substantial amount of storage, typically associated with paid Cortex Data Lake subscriptions rather than a free tier. Offering this much for free would undermine the paid licensing model.

* Conclusion: Incorrect.

* C. 10 TB:

* Analysis: 10 TB is even larger and aligns with enterprise-scale paid deployments, not a free instance. This size is far beyond what's provided without a purchase.

* Conclusion: Incorrect.

* D. 100 GB:

* Analysis: 100 GB is the documented size of the free Cortex Data Lake instance provided to customers who activate a tenant (e.g., via TMS) without purchasing additional storage. It's sufficient for small-scale testing, such as storing logs from a handful of Cortex XDR agents or firewall data for a limited retention period (e.g., 30 days).

* Conclusion: Correct.

Supporting Context:

* Cortex XDR Example: For Cortex XDR Prevent customers, activating a tenant includes 100 GB of free Cortex Data Lake

storage for 30 days of alert data (not full telemetry, which requires XDR Pro).

This aligns with the TMS scenario, where basic tenant activation triggers the same free tier.

* Prisma Access: Similarly, Prisma Access customers activating a tenant without a purchased Data Lake instance receive 100 GB for initial log storage.

* Documentation: While exact wording may vary, Palo Alto Networks consistently references 100 GB as the free tier across product activation guides.

References:

Cortex Data Lake Getting Started Guide (Palo Alto Networks Documentation):

States that customers who activate a tenant without purchasing storage receive "100 GB of free storage" for initial use.

docs-cortex.paloaltonetworks.com/r/Cortex-Data-Lake/Cortex-Data-Lake-Getting-Started/Get-Started-with-Cortex-Data-Lake

Cortex XDR Prevent Activation:

Notes that 100 GB is included for free with tenant activation, supporting basic alert storage.

Palo Alto Networks Sales and Licensing FAQs:

Confirms 100 GB as the standard free tier for Cortex Data Lake when no additional storage is purchased.

NEW QUESTION # 107

A Cortex XSOAR customer wants to ingest from a single mailbox. The mailbox brings in reported phishing emails and email requests from human resources (HR) to onboard new users. The customer wants to run two separate workflows from this mailbox, one for phishing and one for onboarding. What will allow Cortex XSOAR to accomplish this in the most efficient way?

- A. Create a playbook to process and determine incident type based on content of the email
- B. Use machine learning (ML) to determine incident type
- C. Create two instances of the email integration and classify one instance as ingesting incidents of type phishing and the other as ingesting incidents of type boarding
- **D. Use an incident classifier based on field in each type of email to classify those containing "Phish Alert" in the subject as phishing and those containing "Onboard Request" as onboarding**

Answer: D

NEW QUESTION # 108

What is the difference between the intel feed's license quotas of Cortex XSOAR Starter Edition and Cortex XSOAR (SOAR + TIM)?

- A. Cortex XSOAR Started Edition has unlimited access to the Threat Intel Library.
- B. In Cortex XSOAR (SOAR + TIM), intelligence detail view and relationships data are not included.
- **C. Cortex XSOAR Starter Edition includes up to 5 active feeds and 100 indicators/fetch.**
- D. In Cortex XSOAR (SOAR + TIM), Unit 42 Intelligence is not included.

Answer: C

Explanation:

The Cortex XSOAR Starter Edition has a more limited capacity compared to Cortex XSOAR (SOAR + TIM).

It includes up to 5 active threat intelligence feeds and a maximum of 100 indicators per fetch. In contrast, the SOAR + TIM version typically provides more extensive threat intelligence capabilities.

NEW QUESTION # 109

A customer is hesitant to directly connect their network to the Cortex platform due to compliance restrictions.

Which deployment method should the customer use to ensure secure connectivity between their network and the Cortex platform?

- A. Elasticsearch
- B. Syslog collector
- C. Windows Event Collector
- **D. Broker VM**

Answer: D

Explanation:

To ensure secure connectivity between the customer's network and the Cortex platform while adhering to compliance restrictions,

