PALO ALTO XSIAM-ENGINEER

Palo Alto XSIAM-Engineer Certification Questions & Answers

Exam Summary – Syllabus – Questions

XSIAM-ENGINEER

Palo Alto Networks Certified XSIAM Engineer

75 Questions Exam – 860 on a scale of 300 to 1000 Cut Score – Duration of 90 minutes

Table of Contents:

Know Your XSIAM-Engineer Certification Well:

The XSIAM-Engineer is best suitable for candidates who want to gain knowledge in the Palo Alto Security Operations. Before you start your XSIAM-Engineer preparation you may struggle to get all the crucial XSIAM-Engineer materials like XSIAM-Engineer syllabus, sample questions, study guide.

But don't worry the XSIAM-Engineer PDF is here to help you prepare in a stress free manner.
The PDF is a combination of all your queries like-

- What is in the XSIAM-Engineer syllabus?
- How many questions are there in the XSIAM-Engineer exam?
- Which Practice test would help me to pass the XSIAM-Engineer exam at the first attempt?

Passing the XSIAM-Engineer exam makes you Palo Alto Networks Certified XSIAM Engineer. Having the XSIAM-Engineer certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

Palo Alto XSIAM-Engineer Certification Details:

Exam Name	Palo Alto Networks XSIAM Engineer
Exam Code	XSIAM-Engineer
Exam Price	$250 USD
Duration	90 minutes
Number of Questions	75
Passing Score	860 on a scale of 300 to 1000
Recommended Training	**Cortex XSIAM: Security Operations, Integration, and Automation**
Exam Registration	**PEARSON VUE**
Sample Questions	**Palo Alto XSIAM-Engineer Sample Questions**
Practice Exam	**Palo Alto Networks Certified XSIAM Engineer Practice Test**

XSIAM-Engineer Syllabus:

Section	Weight	Objectives
Planning and Installation	22%	- Evaluate the existing IT infrastructure and security posture to align with XSIAM architecture - Evaluate deployment requirements, objectives, and resources • Hardware • Software • Data sources • Integrations - Identify communication requirements for XSIAM components - Install and configure Cortex XSIAM components • Agentsf • Broker VM • Engine - Configure user roles, permissions, and access controls
Integration and Automation	30%	- Onboard data sources (e.g., endpoint, network, cloud, identity) - Configure automation and feed integrations (e.g., messaging, SIEM, authentication, threat intelligence feeds) - Implement and maintain Marketplace content packs - Manage automation workflow • Plan • Playbook tasks • Customize • Debug
Content Optimization	24%	- Deploy parsing rules for unique data formats - Deploy data modeling rules for data normalization - Manage detection rules to align with provided requirements • Correlation

Section	Weight	Objectives
		• Indicators of compromise (IOCs) and behavioral indicators of compromise (BIOCs) • Indicator rules • Scoring rules • Attack Surface Management (ASM) rules - Manage incident and alert layout - Create custom dashboards and reporting templates
Maintenance and Troubleshooting	24%	- Manage exception and exclusion configurations - Manage XSIAM software component updates (e.g., content, XDR agent, XDR collector, Broker VM) - Troubleshoot data management issues (e.g., data ingestion, normalization, parsing) - Troubleshoot Cortex XSIAM components (e.g., agents, integrations, playbooks)

Palo Alto XSIAM-Engineer Sample Questions:

Question: 1

If Cortex XSIAM is ingesting logs from a custom application, which is most likely required?

a) Deactivating data modeling
b) Creating a custom BIOC rule
c) Building a custom parsing rule
d) Switching to agentless logging

Answer: c

Question: 2

Before updating the XDR Collector, what should an administrator verify to avoid disruption?

a) The number of ingestion pipelines
b) That the device is marked as 'untrusted'
c) The health and connectivity status of the collector
d) The number of playbooks running

Answer: c

Question: 3

How can administrators validate the effectiveness of exclusion rules in Cortex XSIAM? (Choose two)

a) Simulate alerts using the Threat Detection Lab
b) Generate correlation reports
c) Monitor alert counts before and after rule implementation
d) Check the ingestion pipeline latency

Answer: a, c

Question: 4

Which component is responsible for identifying the correct parsing rule to apply for a unique data source in Cortex XSIAM?

a) Data model rule
b) Log ingestion filter
c) Parsing rule tag
d) Parsing classifier

Answer: d

Question: 5

What indicates that a new version of a content pack is available for update in Cortex XSIAM Marketplace?

a) Green badge next to the pack name
b) "Update Available" tag under the pack listing
c) Alert generated in Incident dashboard
d) An email from the SOC automation system

Answer: b

Question: 6

What are two commonly used automation integrations in Cortex XSIAM for third-party connectivity?

a) PagerDuty
b) Amazon CloudWatch
c) Wireshark
d) ServiceNow

Answer: a, d

Question: 7

When a newly installed agent is not reporting telemetry to Cortex XSIAM, which two steps should you check first? (Choose two)

a) Agent connectivity to Cortex gateways
b) Assigned user permission groups
c) Broker VM version compatibility
d) Agent certificate status

Answer: a, d

Question: 8

To enable authentication integration for automated user provisioning in Cortex XSIAM, what steps are essential?

a) Enable LDAP sync
b) Configure SAML SSO
c) Set up a proxy for endpoint filtering
d) Connect to Azure Monitor

Answer: a, b

Question: 9

After deploying a new content pack, a user cannot access associated playbooks. What is the most likely cause?

a) The engine is in maintenance mode
b) User role lacks sufficient playbook permissions
c) The agent is not upgraded
d) The dashboard is misconfigured

Answer: b

Question: 10

Why is it important to understand the organization's current threat detection capabilities before deploying XSIAM?

a) To reduce software licensing costs
b) To benchmark XSIAM against existing SOC KPIs
c) To prioritize upgrades to Prisma Access
d) To enable Engine offline processing

Answer: b

Study Guide to Crack Palo Alto XSIAM-Engineer Exam:

- Getting details of the XSIAM-Engineer syllabus, is the first step of a study plan. This pdf is going to be of ultimate help. Completion of the syllabus is must to pass the XSIAM-Engineer exam.
- Making a schedule is vital. A structured method of preparation leads to success. A candidate must plan his schedule and follow it rigorously to attain success.
- Joining the Palo Alto provided training for XSIAM-Engineer exam could be of much help. If there is specific training for the exam, you can discover it from the link above.
- Read from the XSIAM-Engineer sample questions to gain your idea about the actual exam questions. In this PDF useful sample questions are provided to make your exam preparation easy.
- Practicing on XSIAM-Engineer practice tests is must. Continuous practice will make you an expert in all syllabus areas.