nwexam.com
#1 Networking Certification Guide

PALO ALTO XSIAM-ANALYST STUDY GUIDE PDF

Palo Alto XSIAM Analyst Certification Questions & Answers

Details of the Exam-Syllabus-Questions

XSIAM-Analyst

Palo Alto Networks Certified XSIAM Analyst

50 Questions Exam – 860/300 to 1000 Cut Score – Duration of 90 minutes

Table of Contents:

Get an Overview of the XSIAM-Analyst Certification:

Who should take the **XSIAM-Analyst exam**? This is the first question that comes to a candidate's mind when preparing for the XSIAM Analyst certification. The XSIAM-Analyst certification is suitable for candidates who are keen to earn knowledge on the Security Operations and grab their Palo Alto Networks Certified XSIAM Analyst. When it is about starting the preparation, most candidates get confused regarding the study materials and study approach. But XSIAM-Analyst study guide PDF is here to solve the problem. XSIAM-Analyst PDF combines some effective sample questions and offers valuable tips to pass the exam with ease.

Why Should You Earn the Palo Alto XSIAM-Analyst Certification?

There are several reasons why one should grab the XSIAM-Analyst certification.

- The XSIAM Analyst certification proves to be one of the most recognized certifications.
- The certification badge proves the knowledge of the candidate regarding subject matters and makes his resume presentable to potential candidates.
- Thus earning the **Palo Alto Networks Certified XSIAM Analyst** is a powerful qualification for a prosperous career.

What Is the Palo Alto XSIAM-Analyst Certification Exam Structure?

Exam Name	Palo Alto Networks XSIAM Analyst
Exam Number	XSIAM-Analyst
Exam Price	$250 USD
Duration	90 minutes
Number of Questions	50
Passing Score	860/300 to 1000
Recommended Training	**Cortex XSIAM for Investigation and Analysis**

Exam Registration	**PEARSON VUE**
Sample Questions	**Palo Alto XSIAM-Analyst Sample Questions**
Practice Exam	**Palo Alto Networks Certified XSIAM Analyst Practice Test**

Enhance Knowledge with XSIAM-Analyst Sample Questions:

Question: 1

Which of the following actions is most appropriate in the Playground?

a) Modify live alert data
b) Simulate automation scripts without affecting real data
c) Change alert severities globally
d) Disable incident creation rules

Answer: b

Question: 2

You notice multiple endpoints reporting offline in XSIAM. Which actions would help confirm their operational status?

a) Review recent heartbeat logs
b) Perform a live terminal scan
c) Ping the endpoint from the agent
d) Check agent connection timestamps

Answer: a, d

Question: 3

Which type of alert in Cortex XSIAM is primarily based on endpoint telemetry and behavior?

a) IOC
b) Correlation
c) XDR Agent
d) BIOC

Answer: d

Question: 4

An alert involves credential dumping. Reviewing the causality chain, you notice the following:

- lsass.exe is accessed by powershell.exe

- Prior to this, cmd.exe launched the PowerShell script

What can you infer?

a) Scripted behavior likely launched manually
b) There is an indicator of defense evasion
c) Possible credential access tactic
d) It’s a known benign service activity

Answer: b, c

Question: 5

An alert fires indicating lateral movement between endpoints. It was triggered after evaluating multiple unrelated activities, such as credential access and abnormal port scanning. What are likely characteristics of this alert?

(Choose two)

a) Triggered by an IOC match
b) Behaviorally inferred by a correlation rule
c) Suggests a pre-configured playbook was executed
d) Likely caused by a multi-stage correlation rule

Answer: b, d

Question: 6

An alert for malware propagation triggers an incident. The associated playbook isolates the endpoint and notifies the SOC team. What advantages does this approach provide?

(Choose two)

a) Reduces mean time to respond (MTTR)
b) Prevents SOC teams from seeing alert metadata
c) Automates critical response actions
d) Allows unrestricted user activity

Answer: a, c

Question: 7

In the Identity Threat Detection and Response (ITDR) module, what does "compromised identity" typically indicate?

a) Failed software update
b) Unauthorized access or behavior from a known identity
c) Missing antivirus signature
d) USB device connection

Answer: b

Question: 8

You observe that a CVE is impacting multiple assets. How can you use ASM to investigate further? (Choose two)

a) Review asset tags and status
b) Trigger a Cortex data purge
c) Validate attack surface rule hits
d) Disable detection rules

Answer: a, c

Question: 9

You are hunting for endpoints that have recently executed PowerShell commands. Which two XQL query steps are appropriate?

a) Use the xdm.process table
b) Filter events by command-line arguments
c) Query the xdm.asset table for policy info
d) Export user reports from SIEM

Answer: a, b

Question: 10

Which option allows continuous monitoring and triage of evolving threats?

a) Live terminal execution
b) Threat intelligence API
c) Attack Surface Threat Response Center
d) Asset status logs

Answer: c

What Study Guide Works Best in Acing the Palo Alto XSIAM-Analyst Certification?

The XSIAM-Analyst study guide is a combination of some proven study tips and the combination of all valuable study materials like sample questions, syllabus and practice tests in one place.

Explore the Syllabus Topics and Learn from the Core:

If you are determined to earn success in the XSIAM Analyst exam, getting in full touch of the **syllabus** is mandatory. During preparation, you might not like all syllabus sections or topics, but try to get at least the fundamental knowledge from the sections you don't like. The more you possess knowledge on all syllabus sections, the more is the chance to attempt maximum number of questions during the actual exam.

Make Your Schedule:

Studying and completing the syllabus becomes easier, if you work on the syllabus topics after making a schedule. Your syllabus must mention what areas you want to cover and within what time. Once you make a schedule and follow it regularly, syllabus completion becomes easier and preparation becomes smoother.

Get Expert Advice from the Training:

Do not forget to join the Palo Alto XSIAM-Analyst training if it is providing any. Training enhances the practical knowledge of a candidate, which helps them to work well in the practical field during projects.

Get Access to the PDF Sample Questions:

If your study material is in a **PDF format** or the materials are mobile-friendly, what could be better than that? Get access to the free sample questions and keep enhancing your knowledge beyond the syllabus.

Avoid Dumps and Utilize the Palo Alto XSIAM-Analyst Practice Test:

Why should you rely on practice tests? The reason is simple: you must get familiar with the exam pattern before reaching the exam hall. An aspirant aware of the exam structure and time management during the exam preparation can perform well in the actual exam and attempt the maximum number of questions during the exam.

Many aspirants prefer to read from dumps, but they miss out on the self assessment method. Therefore, XSIAM-Analyst practice tests always stand out to be the better choice than dumps PDF.

Avail the Proven XSIAM-Analyst Practice Test for Success!!!

Do you want to pass the XSIAM-Analyst exam on your first attempt? Stop worrying; we, NWExam.com are here to provide you the best experience during your Palo Alto Networks XSIAM Analyst preparation. Try out our free mock tests to get a glimpse of our quality study materials, and build your confidence with the premium **XSIAM-Analyst practice tests**. Our expert-designed questions help you to improve performance and pass the exam on your first attempt.