PALO ALTO XSIAM-ANALYST

Palo Alto XSIAM Analyst Certification Questions & Answers

Exam Summary – 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:

Know Your XSIAM-Analyst Certification Well:

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

But don't worry the XSIAM-Analyst 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-Analyst syllabus?
- How many questions are there in the XSIAM-Analyst exam?
- Which Practice test would help me to pass the XSIAM-Analyst exam at the first attempt?

Passing the XSIAM-Analyst exam makes you Palo Alto Networks Certified XSIAM Analyst. Having the XSIAM Analyst 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 Analyst Certification Details:

Exam Name	Palo Alto Networks XSIAM Analyst
Exam Code	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**

XSIAM-Analyst Syllabus:

Section	Weight	Objectives
Alerting and Detection Processes	19%	- Identify and describe the different types of analytic alerts - Explain alert prioritization handling • Incident scoring • Alert starring • Featured fields • Incident domains - Configure custom prioritizations - Identify and describe alert sources and corresponding actions • Correlations • XDR Agent • XDR behavioral indicator of compromise (BIOC) • XDR indicator of compromise (IOC)
Incident Handling and Response	20%	- Explain the incident creation process - Review and investigate alert evidence • Forensics • Identity Threat Detection and Response (ITDR) • Causality chain • Timeline - Identify, analyze, and respond to security events and incidents - Apply the native automation response action - Identify, hunt, and investigate leads and IOCs - Interpret incident context data - Differentiate between alert grouping and data stitching
Automation and Playbooks	15%	- Use playbooks for automated incident response - Identify and describe playbook components • Task types • Sub-playbooks

Section	Weight	Objectives
		• Error handling - Explain the purpose of the playground
Data Analysis with XQL	14%	- Identify and describe Cortex Data Models (XDMs) - Use XDMs to analyze security events - Use XQL to query datasets - Explain XQL data structure • Syntax • Schema • Data sources - Identify and describe XQL options • Query Library • XQL Helper • Scheduled queries
Endpoint Security Management	12%	- Validate endpoint profiles and policies - Validate agent operational status - Monitor endpoint activities - Respond to endpoint alerts and incidents • Live terminal • Endpoint isolation • Malware scan • Endpoint file retrieval
Threat Intelligence Management and ASM	20%	- Import and manage indicators - Validate artifacts, verdicts, reputations, and impact - Explain the process of creating prevention and detection indicator rules - Explain the process of verdict management - Explain indicator relationships - Validate and monitor asset inventory - Use the attack surface threat response center to identify, review, assess, research, and remediate emerging threats - Explain attack surface rules functionality

Palo Alto XSIAM-Analyst Sample Questions:

Question: 1

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: 2

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: 3

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: 4

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: 5

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: 6

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: 7

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

Question: 8

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: 9

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: 10

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

Study Guide to Crack Palo Alto XSIAM Analyst XSIAM-Analyst Exam:

- Getting details of the XSIAM-Analyst 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-Analyst 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-Analyst 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-Analyst 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-Analyst practice tests is must. Continuous practice will make you an expert in all syllabus areas.