PALO ALTO SECOPS-GENERALIST

Palo Alto SecOps-Generalist Certification Questions & Answers

Exam Summary – Syllabus – Questions

SECOPS-GENERALIST

Palo Alto Networks Certified Security Operations Generalist

60-75 Questions Exam – 860/300 to 1000 Cut Score – Duration of 90 minutes

Table of Contents:

Know Your SecOps-Generalist Certification Well:

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

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

Passing the SecOps-Generalist exam makes you Palo Alto Networks Certified Security Operations Generalist. Having the SecOps-Generalist 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 SecOps-Generalist Certification Details:

Exam Name	Security Operations Generalist
Exam Code	SecOps-Generalist
Exam Price	$200 USD
Duration	90 minutes
Number of Questions	60-75
Passing Score	860/300 to 1000
Exam Registration	**PEARSON VUE**
Sample Questions	**Palo Alto SecOps-Generalist Sample Questions**
Practice Exam	**Palo Alto Networks Certified Security Operations Generalist Practice Test**

SecOps-Generalist Syllabus:

Section	Weight	Objectives
Security Operations Fundamentals	25%	- Explain the function of users, roles, log management, compliance, and data protection in Cortex XDR - Explain the process of creating and managing reports and dashboards in Cortex products - Explain the common components and functions of a Security Operations Center (SOC) • Roles and responsibilities • Tools, technologies, and analytics - Dierentiate between AI and machine learning (ML) in Security Operations
Threat Intelligence and Incident Response	16%	- Identify and explain the steps of the NIST incident response plan - Explain the concept of incident management and response - Explain the role of threat intelligence in incident response - Explain the function of incident categorization and prioritization - Explain how le, IP address, domain, and URL indicator types are used in Cortex products - Compare and contrast WildFire, Unit 42 intelligence, and VirusTotal - Evaluate false positive, false negative, and true positive security incidents - Conduct basic threat hunting based on a common indicator types
Cortex XDR	23%	- Identify and explain the use of key Cortex XDR elements • Sensors • Log Stitching • Causality View • WildFire

Section	Weight	Objectives
		• Detection and response • Behavioral analytics • Data sources, users, artifacts, and assets in investigations - Explain the process of agent management and deployment, including cloud workloads - Identify use cases where a business would benefit from Cortex XDR compared to an EDR solution
Cortex XSOAR	16%	- Explain the features and functionality of Cortex XSOAR • Marketplace • Playbooks • Third-party system integration • Indicators and feeds in Threat Intelligence Management • War Room • Incident investigation - Dierentiate between scripts and jobs in Cortex XSOAR
Cortex XSIAM	20%	- Explain the function of key Cortex XSIAM components • Sensors • Log Stitching • Automations and integrations • Content packs • Playbooks - Explain Cortex XSIAM processes, capabilities, use cases, and rules • Data ingestion • Key investigation artifacts and assets • Threat management, detection, and response • Threat hunting and investigation searches and queries • IOC, BIOC, and correlations

Palo Alto SecOps-Generalist Sample Questions:

Question: 1

An alert is triggered in Cortex XDR indicating that PowerShell is being used to execute commands remotely. The analyst investigates and confirms that the activity is expected administrator behavior.

What type of alert classification is this?

a) True Positive
b) Benign Positive
c) False Negative
d) False Positive

Answer: d

Question: 2

A SOC analyst receives an alert about a suspicious IP address attempting multiple login attempts across several endpoints. The analyst wants to automate the process of gathering intelligence on the IP before escalating the case.

Which Cortex XSOAR feature should be used to automate this enrichment process?

a) Manually searching the IP address on different threat intelligence platforms
b) A Playbook that queries threat intelligence feeds and correlates IOCs
c) Running a forensic investigation on each affected endpoint before taking action
d) Manually forwarding the alert to another team for verification

Answer: b

Question: 3

Your team is responsible for configuring Cortex XDR to improve compliance reporting. Your organization needs to meet GDPR data protection standards. Which of the following actions would be most effective?

a) Disable all logging to avoid storing personal data
b) Allow public access to compliance dashboards for transparency
c) Enable encryption for all stored logs
d) Use default Cortex XDR configurations without changes

Answer: c

Question: 4

How does Cortex XSIAM enhance proactive security operations?

a) By enabling AI-powered threat hunting and anomaly detection
b) By automatically blocking all external network traffic
c) By eliminating the need for EDR solutions
d) By focusing only on known attack signatures

Answer: a

Question: 5

In Cortex XSOAR, what is the key difference between scripts and jobs?

a) Scripts run on-demand or as part of playbooks, whereas jobs execute on a scheduled basis
b) Scripts require manual execution, while jobs are fully automated
c) Jobs only execute when Cortex XDR detects a new security threat
d) Scripts store historical security incidents, whereas jobs do not

Answer: a

Question: 6

What is the purpose of log stitching in Cortex XDR?

a) To remove duplicate log entries for better performance
b) To compress large log files for easier storage
c) To correlate different log sources into a unified attack storyline
d) To automatically archive logs after 30 days

Answer: c

Question: 7

Which of the following is a characteristic of a "true positive" security alert?

a) An alert is triggered for a real threat that needs response
b) An alert is incorrectly flagged as malicious but is actually benign
c) A malicious attack occurs but is not detected
d) An alert is ignored because it is too frequent

Answer: a

Question: 8

Causality View in Cortex XDR provides analysts with:

a) A simple list of alert logs without additional correlation
b) Automatic remediation capabilities for all detected threats
c) The ability to ignore false positives without investigation
d) A visual representation of how a security event evolved over time

Answer: d

Question: 9

Log stitching in Cortex XDR is used for:

a) Automatically blocking all detected threats
b) Correlating multiple security events to create a unified incident timeline
c) Encrypting security logs for compliance purposes
d) Aggregating network traffic data only

Answer: b

Question: 10

The War Room in Cortex XSOAR is used for:

a) Collaborative real-time investigation and response to security incidents
b) Running playbooks automatically without human intervention
c) Storing all historical threat intelligence reports
d) Generating compliance reports for regulatory audits

Answer: a

Study Guide to Crack Palo Alto SecOps-Generalist Exam:

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