PALO ALTO CYBERSEC-PRACTITIONER

Palo Alto Cybersecurity Practitioner Certification Questions & Answers

Exam Summary – Syllabus – Questions

CYBERSEC-PRACTITIONER

[Palo Alto Networks Certified Cybersecurity Practitioner]

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

Table of Contents:

Know Your CyberSec-Practitioner Certification Well:

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

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

Passing the CyberSec-Practitioner exam makes you Palo Alto Networks Certified Cybersecurity Practitioner. Having the Cybersecurity Practitioner 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 CyberSec-Practitioner Certification Details:

Exam Name	Cybersecurity Practitioner
Exam Code	CyberSec-Practitioner
Exam Price	$150 USD
Duration	90 minutes
Number of Questions	75
Passing Score	860/300 to 1000
Exam Registration	**PEARSON VUE**
Sample Questions	**Palo Alto CyberSec-Practitioner Sample Questions**
Practice Exam	**Palo Alto Networks Certified Cybersecurity Practitioner Practice Test**

CyberSec-Practitioner Syllabus:

Section	Weight	Objectives
Cybersecurity	24%	- Identify the components of the authentication, authorization, and accounting (AAA) framework - Differentiate between tactics and techniques as defined by the MITRE ATT&CK framework - Identify common threat vectors • Command-and-control (C2) • Circumvention • Port evasion • DNS tunneling • Social engineering - Differentiate between types of phishing attacks - Differentiate between types of botnets • Spamming • DDoS • Financial - Describe the characteristics of advanced malware - Describe the characteristics of an advanced persistent threat (APT) - Explain the security function of mobile device management (MDM)
Network Security	22%	- Identify common TLS processes and components • TLS handshake • Session key • Pre-shared key (PSK) - Explain the security function of SSL/TLS decryption - Explain the function of the following technologies • Intrusion prevention system (IPS) • URL filtering • DNS Security • Data loss prevention (DLP)

Section	Weight	Objectives
		• Cloud Access Security Broker (CASB) - Identify next-generation firewall (NGFW) placement options • Physical • Virtual • Container - Explain the limitations of signature-based network protection - Describe the following Palo Alto Networks Cloud-Delivered Security Services (CDSS) • Advanced WildFire • Advanced Threat Prevention • Advanced URL Filtering • IoT security - Explain the function of the Prisma SASE components • Prisma SD-WAN • Prisma Access
Endpoint Security	19%	- Explain the limitations of signature-based anti-malware software - Describe application allow listing - Identify security risks of Portable Executable (PE) files - Describe Identity Threat Detection and Response (ITDR) - Describe host-based intrusion prevention systems (HIPS) - Explain the application of endpoint detection and response (EDR) - Differentiate between incident response (IR) tools • Endpoint detection and response (EDR) • Managed detection and response (MDR) • Extended detection and response (XDR) - Describe Cortex XDR

Section	Weight	Objectives
Cloud Security	19%	- Describe host-based architecture - Describe container architecture - Describe serverless functions - Identify cloud security challenges • Visibility • Code security • Multicloud complexity • Threat mitigation (i.e., host, container, serverless) - Identify the core tenets of a cloud native security platform (CNSP) • Workload security • Compliance management • Asset inventory • Identity and access management (IAM) - Describe how Prisma Cloud enables threat detection across Cloud Security Posture Management (CSPM)
Security Operations	16%	- Differentiate between active traffic monitoring systems and passive traffic monitoring systems - Explain the functions of a security information and event management (SIEM) platform - Identify the advantages of security orchestration, automation, and response (SOAR) - Explain the function of an Attack Surface Management (ASM) platform - Describe Cortex solutions • Cortex XSOAR • Cortex Xpanse / ASM • Cortex XSIAM • Cortex XDR

Palo Alto CyberSec-Practitioner Sample Questions:

Question: 1

How does a SIEM platform improve security event analysis?

a) It automatically prevents malware infections
b) It replaces traditional endpoint detection and response (EDR) solutions
c) It only stores logs for compliance audits
d) It aggregates, normalizes, and correlates security events from multiple sources to identify threats

Answer: d

Question: 2

An unauthorized user attempts multiple login attempts across various endpoints in an organization. How can Cortex XDR help mitigate this threat?

a) By manually reviewing all login logs every week
b) By detecting abnormal login behavior and automatically triggering response actions
c) By encrypting all stored passwords
d) By blocking all network activity for legitimate users

Answer: b

Question: 3

What differentiates a SIEM from a SOAR platform?

a) SOAR platforms do not integrate with SIEM solutions
b) SIEM replaces the need for firewalls
c) SIEM collects and analyzes security logs, while SOAR automates incident response workflows
d) SIEM automatically responds to all security threats

Answer: c

Question: 4

Why is compliance management important in cloud security?

a) It ensures cloud services adhere to regulatory frameworks like GDPR and HIPAA
b) It replaces the need for endpoint security
c) It prevents all unauthorized access
d) It eliminates the need for threat detection

Answer: a

Question: 5

Which of the following best describes a DDoS botnet?

a) A network of infected devices used to overwhelm a target system with excessive traffic
b) A system that spreads spam emails to trick users into installing malware
c) A botnet designed to steal financial credentials from infected devices
d) A botnet used exclusively for cryptocurrency mining

Answer: a

Question: 6

Attackers often use port evasion techniques to bypass network security devices. Which method is a common example?

a) Blocking all outgoing traffic on TCP 80
b) Sending attacks only during weekends
c) Disabling firewall rules to create an open path
d) Using port 443 (HTTPS) to carry malicious payloads disguised as encrypted web traffic

Answer: d

Question: 7

A company experiences a sudden system lockdown, followed by a demand for cryptocurrency payment to regain access to their data. What type of attack is occurring?

a) Ransomware
b) DDoS Attack
c) Spyware Infection
d) SQL Injection

Answer: a

Question: 8

What is a key benefit of using Cortex Xpanse (ASM)?

a) Replacing endpoint security solutions
b) Blocking all unauthorized web traffic automatically
c) Providing continuous visibility into an organization’s exposed assets and potential security risks
d) Managing user authentication policies

Answer: c

Question: 9

Your company's HR department reports an email requesting employee tax records, appearing to come from the CEO. However, the email address domain is slightly different from the company's official domain.

What type of phishing attack is this?

a) Business Email Compromise (BEC)
b) Vishing
c) Clone Phishing
d) Smishing

Answer: a

Question: 10

How does DNS Security prevent cyber threats?

a) It encrypts all DNS requests automatically
b) It blocks malicious domains and prevents DNS tunneling attacks
c) It acts as a firewall replacement
d) It stores all DNS logs for compliance auditing only

Answer: b

Study Guide to Crack Palo Alto CyberSec-Practitioner Exam:

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