PALO ALTO CYBERSEC-APPRENTICE

Palo Alto CyberSec Apprentice Certification Questions & Answers

Exam Summary – Syllabus – Questions

CYBERSEC-APPRENTICE

Palo Alto Networks Certified Cybersecurity Apprentice

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

Table of Contents:

Know Your CyberSec-Apprentice Certification Well: 2

Palo Alto CyberSec-Apprentice Certification Details: 2

CyberSec-Apprentice Syllabus: 3

Palo Alto CyberSec-Apprentice Sample Questions: 6

Study Guide to Crack Palo Alto CyberSec-Apprentice Exam: 9

Know Your CyberSec-Apprentice Certification Well:

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

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

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

Exam Name	Palo Alto Cybersecurity Apprentice
Exam Code	CyberSec-Apprentice
Exam Price	$150 USD
Duration	90 minutes
Number of Questions	50
Passing Score	860/300 to 1000
Exam Registration	**PEARSON VUE**
Sample Questions	**Palo Alto CyberSec-Apprentice Sample Questions**
Practice Exam	**Palo Alto Networks Certified Cybersecurity Apprentice Practice Test**

CyberSec-Apprentice Syllabus:

Section	Weight	Objectives
Cybersecurity	- Differentiate between vulnerabilities and exploits - Describe the stages of the cyber attack lifecycle • Reconnaissance • Weaponization and Delivery • Exploitation • Installation • Command-and-control (C2) • Actions on the Objective - Describe common attack types • Malware • Spyware • Trojan • Ransomware • Meddler-in-the-middle (MITM) • DDoS - Describe common threat detection systems • Intrusion detection system (IDS) • Host-based intrusion detection system (HIDS) • Network-based intrusion detection system (NIDS) - Describe threat prevention systems and practices • End user awareness • Security updates • Antivirus • Intrusion prevention system (IPS) • Firewalls - Identify the purpose of a demilitarized zone (DMZ) - Identify the purpose of Zero Trust	20%
Network Fundamentals	- Differentiate between types of area networks • WAN • LAN • SD-WAN	19%

Section	Weight	Objectives
	- Describe external (north-south) and internal (east-west) traffic flow patterns for environments - Explain the function of a default gateway - Explain the function of NAT - Explain the function of DNS - Explain the function of DHCP - Differentiate between static routing protocols and dynamic routing protocols - Differentiate between routed protocols and routing protocols - Differentiate between TCP/IP models and OSI models - Identify devices that operate in Layer 1 through Layer 4 of the OSI model	
Network Security	- Differentiate between network segmentation methods • IP subnetting • VLANs • Zones - Differentiate between stateful firewalls and next-generation firewalls (NGFWs) - Explain the function of URL filtering - Explain the function of a VPN - Explain the function of a proxy - Differentiate between tunneling protocols • SSH • TLS • IKE - Explain the function of data loss prevention (DLP)	17%
Endpoint Security	- Differentiate between internet of things (IoT) devices and endpoints - Differentiate between endpoint security and network security - Explain the objectives of endpoint security - Identify endpoint security components	15%

Section	Weight	Objectives
	Security updates Antivirus Host-based firewalls - Differentiate between single-factor authentication and multi-factor authentication - Describe identity and access management (IAM)	
Cloud Security	- Identify the four cloud-computing deployment models - Describe common cloud service models • Software as a service (SaaS) • Platform as a service (PaaS) • Infrastructure as a service (IaaS) • Network as a service (NaaS) - Describe the cloud shared responsibility model - Identify the four Cs of cloud native security • Cloud • Clusters • Containers • Code - Define common cloud terms • Hosted • Virtualization • Virtual machine (VM) • Container • Orchestration • API - Describe the cloud native security platform (CNSP) - Explain the function of continuous integration and continuous delivery / deployment (CI/CD)	14%
Security Operations	- Explain security operations functions • Identify / Detect • Investigate • Mitigate • Improve - Describe the pillars of effective security operations	15%

Section	Weight	Objectives
	• Business • People • Interfaces • Visibility • Technology • Processes - Define common security operations terms • Event • Alert • Security operations center (SOC) • DevSecOps • Incident response (IR) plan • Disaster recovery plan - Explain the concepts of false positive alerts and false negative alerts - Explain the function of syslog - Explain the following security operations technologies Security orchestration, automation, and response (SOAR) Security information and event management (SIEM) - Describe AI as it relates to alert analysis	

Palo Alto CyberSec-Apprentice Sample Questions:

Question: 1

Which features are typically found in Next-Generation Firewalls (NGFWs) but not in traditional stateful firewalls?

(Choose two)

a) Port-based filtering
b) Application-layer inspection
c) Integrated intrusion prevention
d) Simple packet forwarding

Answer: b, c

Question: 2

Which two benefits do security updates provide for endpoints? (Choose two)

a) Close security gaps
b) Reduce firewall inspection
c) Fix bugs and improve performance
d) Disable antivirus

Answer: a, c

Question: 3

Which of the following are characteristics of a Meddler-in-the-Middle (MITM) attack? (Choose two)

a) Uses brute force to guess passwords
b) Attacker intercepts communication between two parties
c) Often occurs on public Wi-Fi
d) Requires no access to network traffic

Answer: b, c

Question: 4

A company enforces strict role-based access control (RBAC), requiring employees to access only the systems necessary for their roles. Authentication is performed using passwords and a one-time code sent to employees' mobile devices. Which IAM practices are reflected here?

a) SSO and static routing
b) Least privilege and multi-factor authentication
c) Biometric authorization and DLP
d) IP tunneling and MAC filtering

Answer: b

Question: 5

Which of the following is a characteristic of dynamic routing protocols?

a) Require manual route configuration
b) Automatically adapt to network changes
c) Only work on Layer 7
d) Are used exclusively for wireless networks

Answer: b

Question: 6

What is the primary goal of a Data Loss Prevention (DLP) system?

a) Enhance packet forwarding
b) Prevent unauthorized data transfers
c) Assign IP addresses
d) Track bandwidth usage

Answer: b

Question: 7

Which devices operate at Layers 3 and 4 of the OSI model? (Choose two)

a) Router
b) Hub
c) Firewall
d) Repeater

Answer: a, c

Question: 8

Which of the following activities are typical of the reconnaissance stage of a cyber-attack?

(Choose two)

a) Installing malware
b) Scanning for open ports
c) Harvesting employee emails
d) Encrypting critical files

Answer: b, c

Question: 9

In the cloud shared responsibility model, which party is responsible for physical infrastructure?

a) Customer
b) End user
c) Government
d) Cloud provider

Answer: d

Question: 10

What is the primary distinction between endpoint security and network security?

a) Endpoint security protects the internet
b) Network security secures end-user devices
c) Endpoint security protects individual devices; network security protects traffic flow
d) Network security only applies to wireless networks

Answer: c

Study Guide to Crack Palo Alto CyberSec-Apprentice Exam:

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

Reliable Online Practice Test for CyberSec-Apprentice Certification

Make NWExam.com your best friend during your Palo Alto Cybersecurity Apprentice exam preparation. We provide authentic practice tests for the CyberSec-Apprentice exam. Experts design these online practice tests, so we can offer you an exclusive experience of taking the actual CyberSec-Apprentice exam. We guarantee you 100% success in your first exam attempt if you continue practicing regularly. Don't bother if you don't get 100% marks in initial practice exam attempts. Just utilize the result section to know your strengths and weaknesses and prepare according to that until you get 100% with our practice tests. Our evaluation makes you confident, and you can score high in the CyberSec-Apprentice exam.

Start Online practice of CyberSec-Apprentice Exam by visiting URL
https://www.nwexam.com/palo-alto/cybersec-apprentice-palo-alto-cybersecurity-apprentice