Palo Alto Networks Cybersecurity Apprentice Course

Palo Alto Networks Cybersecurity Apprentice Course

Duration 5 Days

40 Hours

The Palo Alto Networks Certified Cybersecurity Apprentice exam is intended for individuals who are entering or transitioning into the cybersecurity field. It provides an opportunity for candidates pursuing an entry-level cybersecurity role—as well as those coming from non-technical backgrounds such as marketing, sales, program management, or general administration—to demonstrate essential knowledge in networking and cybersecurity.

This certification validates a candidate's foundational understanding of key domains, including cybersecurity concepts, network fundamentals, endpoint protection, security operations, network security, and cloud security.

Audience and Qualifications

Target Audience

This certification is ideal for:

Individuals seeking to validate their foundational understanding of cybersecurity concepts

Members of the emerging workforce, including high school, college, and university students

Professionals looking to transition into a cybersecurity career

Both technical and non-technical IT professionals

Skills Required

Candidates should have a basic understanding of:

Networking concepts, models, and protocols

Endpoint security components, standards, and protection mechanisms

Cloud security concepts, architectures, and service models

Security operations principles and core functions

The cybersecurity lifecycle, common threats, detection techniques, and prevention methods

Current and emerging trends in information security, such as artificial intelligence, machine learning, and crowdsourced intelligence

Topics

1. Cybersecurity 20%

1.1 Identify and describe vulnerabilities and exploits

1.2 Identify and describe the stages of the cyber attack lifecycle

1.2.1 Reconnaissance

1.2.2 Weaponization and Delivery

1.2.3 Exploitation

1.2.4 Installation

1.2.5 Command-and-Control (C2)

1.2.6 Actions on the Objective

1.3 Identify and describe common attack types (e.g., malware, insider threat, C2, social engineering, AI-powered)

1.4 Identify and describe common threat detection systems

1.4.1 Intrusion Detection System (IDS)

1.4.2 Host-Based Intrusion Detection System (HIDS)

1.4.3 Network-Based intrusion detection system (NIDS)

1.5 Identify and describe threat prevention systems and practices (e.g., end user awareness, security updates, antivirus, intrusion prevention systems, firewalls)

1.6 Explain the purpose of a DMZ

1.7 Explain the purpose of Zero Trust

2. Network Fundamentals 14%

2.1 Identify and describe types of area networks

2.1.1 WAN

2.1.2 LAN

2.1.3 SD-WAN

2.2 Explain external (north-south) and internal (east-west) traffic flow patterns for environments

2.3 Explain the function of a default gateway

2.4 Explain the function of NAT, DNS, and DHCP

2.5 Explain routed protocols and routing protocols

2.6 Explain the TCP/IP model and the OSI model

2.7 Identify and describe devices that operate in Layer 1 through Layer 4 of the OSI model

3. Network Security 19%

3.1 Identify and describe network segmentation methods (e.g., IP subnetting, VLAN)

3.2 Explain the function of stateful firewalls and next-generation firewalls (NGFWs)

3.3 Explain the function of URL filtering

3.4 Explain the function of a VPN

3.5 Explain the function of a proxy

3.6 Identify and describe tunneling protocols

3.6.1 SSH

3.6.2 TLS

3.6.3 IKE

3.7 Explain the function of data loss prevention (DLP)

3.8 Explain the function of enterprise browsers

4. Endpoint Security 13%

4.1 Identify and describe internet of things (IoT) devices and endpoints

4.2 Explain the objectives of endpoint security and network security

4.3 Identify and describe endpoint security components

4.3.1 Security updates

4.3.2 Antivirus

4.3.3 Host-based firewalls

4.4 Differentiate between single-factor authentication and multi-factor authentication

4.5 Describe identity and access management (IAM)

5. Cloud Security 16%

5.1 Identify and describe the four cloud-computing deployment models

5.2 Identify and describe common cloud service models

5.2.1 Software as a service (SaaS)

5.2.2 Platform as a service (PaaS)

5.2.3 Infrastructure as a service (IaaS)

5.2.4 Network as a service (NaaS)

5.3 Explain the cloud shared responsibility model

5.4 Explain cloud security and cloud-native security

5.5 Define common cloud terms (e.g., hosted, virtualization, virtual machine, container,

microservice, API)

5.6 Explain the cloud native security platform (CNSP)

5.7 Explain the function of continuous integration and continuous delivery / deployment (CI/CD)

6. Security Operations 18%

6.1 Explain security operations functions

6.1.1 Identify / detect

6.1.2 Investigate

6.1.3 Mitigate

6.1.4 Improve

6.2 Identify methods to optimize security operations center (SOC) performance (e.g., automation

and AI, collaboration and information sharing, regular Security policy updates, security

framework alignment)

6.3 Define common security operations terms (e.g., event, alert, SOC, DevSecOps, incident

response plan, disaster recovery plan)

6.4 Explain the concepts of false positive alerts and false negative alerts

6.5 Explain the function of syslog

6.6 Explain security orchestration, automation, and response (SOAR) and security information

and event management (SIEM)

6.7 Explain AI as it relates to alert analysis