paloalto NETWORKS | CYBERSECURITY PARTNER OF CHOICE

Palo Alto Networks Cybersecurity Apprentice

Datasheet

July 2024

The Palo Alto Networks Certified Cybersecurity Apprentice exam is for individuals entering or transitioning to a career in cybersecurity. The exam is designed to provide those seeking an entry-level cybersecurity position or those with non-technical roles (e.g., marketing, sales, program management, general, administrative) the opportunity to demonstrate their networking and cybersecurity knowledge. It will validate a candidate's foundational-level knowledge and understanding in the areas of cybersecurity concepts, network fundamentals, endpoint security, security operations, network security, and cloud security.

Exam registration: Pearson VUE

The purpose of this document is to help you prepare for the exam and attain the certification. Please note that this document is intended to help identify the topics covered and to provide resources and references for understanding those topics. It is not intended to be used as the sole document to prepare for the Cybersecurity Apprentice exam.

Exam Details:

- Duration: 90 minutes
- Format: Multiple-choice questions
- Language: English
- Cost: $150 USD*
- Recommended Prerequisite: None

** Price may vary by country*

Audience and Qualifications

Target Audience

- Individuals who want to validate their foundational knowledge and understanding of cybersecurity concepts
- An emergent workforce that includes high school, college, and university students
- Individuals who want to transition into a cybersecurity career
- Technical and non-technical IT professionals

Skills Required

Basic knowledge of:

- networking concepts, models, and protocols
- endpoint security components, standards, and protection
- cloud security concepts, models, and services
- security operations concepts and functions
- cybersecurity lifecycle, threats, identification methods, and prevention methods
- current and emergent trends in information security (e.g., artificial intelligence, machine learning, and crowdsourced intelligence)

Blueprint

The blueprint table lists the domains covered and includes domain weighting. The percentage weights represent the portion of the exam score that is attributed to each domain. Many candidates find the table provides focus for studies during exam preparation. Also included in the blueprint table are the more specific tasks associated with each domain. Pay particular attention to these tasks, as they provide more targeted areas of study within the domains.

1. Cybersecurity 20%

1.1 Differentiate between vulnerabilities and exploits

1.2 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 Describe common attack types

- 1.3.1 Malware
- 1.3.2 Spyware
- 1.3.3 Trojan
- 1.3.4 Ransomware
- 1.3.5 Meddler-in-the-middle (MITM)
- 1.3.6 DDoS

1.4 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 Describe threat prevention systems and practices

- 1.5.1 End user awareness
- 1.5.2 Security updates
- 1.5.3 Antivirus
- 1.5.4 Intrusion prevention system (IPS)
- 1.5.5 Firewalls

1.6 Identify the purpose of a demilitarized zone (DMZ)

1.7 Identify the purpose of Zero Trust

2. Network Fundamentals 19%

2.1 Differentiate between types of area networks

- 2.1.1 WAN
- 2.1.2 LAN
- 2.1.3 SD-WAN

2.2 Describe 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

2.5 Explain the function of DNS

2.6 Explain the function of DHCP

2.7 Differentiate between static routing protocols and dynamic routing protocols

2.8 Differentiate between routed protocols and routing protocols

2.9 Differentiate between TCP/IP models and OSI models

2.10 Identify devices that operate in Layer 1 through Layer 4 of the OSI model

3. Network Security 17%

3.1 Differentiate between network segmentation methods

- 3.1.1 IP subnetting
- 3.1.2 VLANs
- 3.1.3 Zones

3.2 Differentiate between 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 Differentiate between tunneling protocols

- 3.6.1 SSH
- 3.6.2 TLS
- 3.6.3 IKE

3.7 Explain the function of data loss prevention (DLP)

4. Endpoint Security 15%

4.1 Differentiate between internet of things (IoT) devices and endpoints

4.2 Differentiate between endpoint security and network security

4.3 Explain the objectives of endpoint security

4.4 Identify endpoint security components

- 4.4.1 Security updates
- 4.4.2 Antivirus
- 4.4.3 Host-based firewalls

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

4.6 Describe identity and access management (IAM)

5. Cloud Security 14%

5.1 Identify the four cloud-computing deployment models

5.2 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 Describe the cloud shared responsibility model

5.4 Identify the four Cs of cloud native security

- 5.4.1 Cloud
- 5.4.2 Clusters
- 5.4.3 Containers
- 5.4.4 Code

5.5 Define common cloud terms

- 5.5.1 Hosted
- 5.5.2 Virtualization
- 5.5.3 Virtual machine (VM)
- 5.5.4 Container
- 5.5.5 Orchestration
- 5.5.6 API

5.6 Describe the cloud native security platform (CNSP)

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

6. Security Operations 15%

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 Describe the pillars of effective security operations

- 6.2.1 Business
- 6.2.2 People
- 6.2.3 Interfaces
- 6.2.4 Visibility
- 6.2.5 Technology
- 6.2.6 Processes

6.3 Define common security operations terms

- 6.3.1 Event
- 6.3.2 Alert
- 6.3.3 Security operations center (SOC)
- 6.3.4 DevSecOps
- 6.3.5 Incident response (IR) plan
- 6.3.6 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 the following security operations technologies

- 6.6.1 Security orchestration, automation, and response (SOAR)
- 6.6.2 Security information and event management (SIEM)

6.7 Describe AI as it relates to alert analysis

Learning Path

External candidates are strongly encouraged to use official Palo Alto Networks resources only to prepare for the exam. The complete Palo Alto Networks recommended learning path can be found here.

References

Palo Alto Networks certification exam items are referenced to various publicly available technical or scholarly sources. The following list includes several sources that may have been referenced during the exam item development process.

- Palo Alto Networks TechDocs
- Palo Alto Networks Resource Center
- Palo Alto Networks Cyberpedia
- Palo Alto Networks Knowledge Base
- Palo Alto Networks Unit 42

English as a Second Language (ESL) Accommodation

The ESL accommodation provides a 30-minute time extension for exams delivered in English in non-English speaking countries where a localized version of the exam is not available. When registering for exams at Pearson VUE, the ESL 30-minute extension is automatically granted to candidates in eligible countries based upon candidate address.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com