paloalto NETWORKS | CYBERSECURITY PARTNER OF CHOICE

Palo Alto Networks Cybersecurity Practitioner

Datasheet

July 2024

The Palo Alto Networks Certified Cybersecurity Practitioner certification is for individuals wanting to validate their understanding of cybersecurity and explore Palo Alto Networks portfolio of solutions and related technologies. It is designed for those interested in technical roles in cybersecurity and will validate knowledge and basic application of solutions in the areas of cybersecurity, network security, endpoint security, cloud security, and security operations.

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 Practitioner exam.

Exam Details:

- Duration: 90 minutes
- Format: Multiple-choice questions
- Language: English
- Cost: $150 USD*
- Recommended Prerequisite: Palo Alto Networks Cybersecurity Apprentice training and exam

** Prices may vary by country*

Audience and Qualifications

Target Audience

- Individuals who want to validate their knowledge, skills, and understanding of cybersecurity technologies and solutions
- Individuals transitioning into a cybersecurity career
- Individuals continuing their path in a Palo Alto Networks program

Skills Required

Working knowledge of:

- secure 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
- basic solutions provided by network security, cloud security, and security operations platforms at Palo Alto Networks and their component offerings
- 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 24%

1.1 Identify the components of the authentication, authorization, and accounting (AAA) framework

1.2 Differentiate between tactics and techniques as defined by the MITRE ATT&CK framework

1.3 Identify common threat vectors

- 1.3.1 Command-and-control (C2)
- 1.3.2 Circumvention
- 1.3.3 Port evasion
- 1.3.4 DNS tunneling
- 1.3.5 Social engineering

1.4 Differentiate between types of phishing attacks

1.5 Differentiate between types of botnets

- 1.5.1 Spamming
- 1.5.2 DDoS
- 1.5.3 Financial

1.6 Describe the characteristics of advanced malware

1.7 Describe the characteristics of an advanced persistent threat (APT)

1.8 Explain the security function of mobile device management (MDM)

2. Network Security 22%

2.1 Identify common TLS processes and components

- 2.1.1 TLS handshake
- 2.1.2 Session key
- 2.1.3 Pre-shared key (PSK)

2.2 Explain the security function of SSL/TLS decryption

2.3 Explain the function of the following technologies

- 2.3.1 Intrusion prevention system (IPS)
- 2.3.2 URL filtering
- 2.3.3 DNS Security
- 2.3.4 Data loss prevention (DLP)
- 2.3.5 Cloud Access Security Broker (CASB)

2.4 Identify next-generation firewall (NGFW) placement options

- 2.4.1 Physical
- 2.4.2 Virtual
- 2.4.3 Container

2.5 Explain the limitations of signature-based network protection

2.6 Describe the following Palo Alto Networks Cloud-Delivered Security Services (CDSS)

- 2.6.1 Advanced WildFire
- 2.6.2 Advanced Threat Prevention
- 2.6.3 Advanced URL Filtering
- 2.6.4 IoT security

2.7 Explain the function of the Prisma SASE components

- 2.7.1 Prisma SD-WAN
- 2.7.2 Prisma Access

3. Endpoint Security 19%

3.1 Explain the limitations of signature-based anti-malware software

3.2 Describe application allow listing

3.3 Identify security risks of Portable Executable (PE) files

3.4 Describe Identity Threat Detection and Response (ITDR)

3.5 Describe host-based intrusion prevention systems (HIPS)

3.6 Explain the application of endpoint detection and response (EDR)

3.7 Differentiate between incident response (IR) tools

- 3.7.1 Endpoint detection and response (EDR)
- 3.7.2 Managed detection and response (MDR)
- 3.7.3 Extended detection and response (XDR)

3.8 Describe Cortex XDR

4. Cloud Security 19%

4.1 Describe host-based architecture

4.2 Describe container architecture

4.3 Describe serverless functions

4.4 Identify cloud security challenges

- 4.4.1 Visibility
- 4.4.2 Code security
- 4.4.3 Multicloud complexity
- 4.4.4 Threat mitigation (i.e., host, container, serverless)

4.5 Identify the core tenets of a cloud native security platform (CNSP)

- 4.5.1 Workload security
- 4.5.2 Compliance management
- 4.5.3 Asset inventory
- 4.5.4 Identity and access management (IAM)

4.6 Describe how Prisma Cloud enables threat detection across Cloud Security Posture Management (CSPM)

5. Security Operations 16%

5.1 Differentiate between active traffic monitoring systems and passive traffic monitoring systems

5.2 Explain the functions of a security information and event management (SIEM) platform

5.3 Identify the advantages of security orchestration, automation, and response (SOAR)

5.4 Explain the function of an Attack Surface Management (ASM) platform

5.5 Describe Cortex solutions

- 5.5.1 Cortex XSOAR
- 5.5.2 Cortex Xpanse / ASM
- 5.5.3 Cortex XSIAM
- 5.5.4 Cortex XDR

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