Palo Alto Networks Cybersecurity Practitioner Training

OEM: Palo Alto • Duration: 4 Days (32 hrs) • Code: PCNP

COURSE MODULES & TOPICS

Domain 1: Cybersecurity (19%)

- AAA Framework (Authentication, Authorization, Accounting)
- MITRE ATT&CK Framework
- Zero Trust (Continuous Monitoring/Validation, Least Privilege, Breach Assumption)
- Advanced Persistent Threat (APT) Characteristics
- Common Security Technologies: IdP/IAM/MFA, MDM/MAM, Secure Email Gateways

Domain 2: Network Security (19%)

- Zero Trust Network Access (ZTNA)
- Stateless Firewalls vs Next-Generation Firewalls (NGFWs)
- Microsegmentation
- Common Technologies: IPS, URL Filtering, DNS Security, VPN, SSL/TLS Decryption
- Signature-Based Detection Limitations
- NGFW Deployment Options
- OT/IoT Security
- Cloud-Delivered Security Services (CDSS)
- Precision AI

Domain 3: Secure Access (14%)

- SASE vs SSE Architectures
- CIA Challenges: Data, Private Apps, SaaS, AI Apps
- Secure Web Gateway (SWG), Enterprise Browser, RBI, DLP, CASB
- SD-WAN
- Prisma SASE: Prisma Access, Prisma SD-WAN, Prisma Access Browser, Enterprise DLP, AI Access, Prisma AIRS

Domain 4: Cloud Security (20%)

- Cloud Architectures
- Cloud Security Challenges: Application Security, Posture Security, Runtime Security
- CSPM (Cloud Security Posture Management) and CWPP
- CNAPP (Cloud-Native Application Protection Platform)

© Koenig Solutions

- Cortex Cloud

Domain 5: Endpoint Security (15%)

- Indicators of Compromise (IOCs)
- Signature-Based Anti-Malware Limitations
- UEBA (User and Entity Behavior Analytics)
- EDR vs XDR
- Behavioral Threat Prevention
- Endpoint Security Technologies: HBFW/HIPS, Device Control, App Control, Disk Encryption, Patch Management
- Cortex XDR

Domain 6: Security Operations (13%)

- Threat Hunting
- Incident Response
- SIEM (Security Information and Event Management)
- SOAR (Security Orchestration, Automation and Response)
- Attack Surface Management (ASM)
- Cortex Solutions: XSOAR, Xpanse, XSIAM
- Unit 42 Threat Intelligence