Palo Alto Networks Certified Cybersecurity Entry Level Technician (PCCET)
Exam Blueprint

Domain Weight (%)	
Fundamentals of Cybersecurity	**30%**
Network Security Components	**30%**
Cloud Technologies	**20%**
Elements of Security Operations	**20%**

Domain 1 Fundamentals of Cybersecurity 30%

Task 1.1 Distinguish between Web 2.0 and 3.0 applications and services

Task 1.2 Describe port-scanning methodologies and their impact

- 1.2.1 Nonstandard ports
- 1.2.2 Identify applications by their port number

Task 1.3 Recognize applications used to circumvent port-based firewalls

Task 1.4 Differentiate between common cloud computing service models

- 1.4.1 SaaS
- 1.4.2 PaaS
- 1.4.3 IaaS

Task 1.5 Describe the business processes of supply-chain management

Task 1.6 Describe the vulnerabilities associated with data being stored in the SaaS environment

- 1.6.1 Describe roles within a SaaS environment
- 1.6.2 Describe security controls for SaaS applications

Task 1.7 Describe the impact of governance, regulation, and compliance

- 1.7.1 Differentiate between compliance and security
- 1.7.2 Identify major cybersecurity laws and their implications

Task 1.8 Describe the tactics of the MITRE ATT&CK framework

1.8.1 Identify a leading indicator of a compromise
1.8.2 Describe how to use CVE
1.8.3 Describe how to use CVS

Task 1.9 Identify the different attacker profiles and motivations

1.9.1 Describe the different value levels of the information that needs to be protected (political, financial, etc.)

Task 1.10 Describe the different phases and events of the cyberattack lifecycle

1.10.1 Describe the purpose of command and control (C2)

Task 1.11 Identify the characteristics, capabilities, and appropriate actions for different types of malware and ransomware

Task 1.12 Differentiate between vulnerabilities and exploits

1.12.1 Differentiate between various business email compromise attacks
1.12.2 Identify different methodologies for social engineering
1.12.3 Identify the chain of events that result from social engineering

Task 1.13 Identify what chain of events follows an attack

Task 1.14 Differentiate between the functional aspects of bots and botnets

1.14.1 Describe the type of IoT devices that are part of a botnet attack

Task 1.15 Differentiate the TCP/IP roles in DDoS attacks

1.15.1 Differentiate between DoS and DDoS

Task 1.16 Describe advanced persistent threats

Task 1.17 Describe risks with Wi-Fi networks

1.17.1 Differentiate between common types of Wi-Fi attacks
1.17.2 Describe how to monitor your Wi-Fi network

Task 1.18 Describe perimeter-based network security

1.18.1 Identify the types of devices used in perimeter defense

Task 1.19 Describe the Demilitarized Zone (DMZ)

Task 1.20 Describe the transition from a trusted network to an untrusted network

1.20.1 Differentiate between North-South and East-West zones

Task 1.21 Describe Zero Trust

1.21.1 Identify the benefits of the Zero Trust model
1.21.2 Identify the design principles for Zero Trust
1.21.3 Describe a microperimeter
1.21.4 Differentiate between Trust and Untrust zones

Task 1.22 Describe the integration of services for network, endpoint, and cloud

Task 1.23 Identify the capabilities of an effective Security Operating Platform

1.23.1 Describe the components of the Security Operating Platform

Domain 2 Network Security Components 30%

Task 2.1 Differentiate between hubs, switches, and routers

2.1.1 Given a network diagram, Identify the icons for hubs, switches, and routers

Task 2.2 Describe the use of VLANs

Task 2.3 Differentiate between routed and routing protocols

Task 2.4 Differentiate between static and dynamic routing protocols

2.4.1 Differentiate between link state and distance vector

Task 2.5 Identify the borders of collision and broadcast domains

Task 2.6 Differentiate between different types of area networks

2.6.1 WAN
2.6.2 LAN

Task 2.7 Describe the advantages of SD-WAN

Task 2.8 Describe the purpose of the Domain Name System (DNS)

2.8.1 Describe how DNS record types are used
2.8.2 Identify a fully qualified domain name (FQDN)
2.8.3 Describe the DNS hierarchy

Task 2.9 Differentiate between categories of IoT devices

2.9.1 Identify the known security risks and solutions associated with IoT

Task 2.10 Identify IoT connectivity technologies

Task 2.11 Differentiate between IPv4 and IPv6 addresses

2.11.1 Describe binary-to-decimal conversion
2.11.2 Describe IPv4 CIDR notation
2.11.3 Describe IPv4 classful subnetting
2.11.4 Given a scenario, identify the proper subnet mask
2.11.5 Describe the purpose of subnetting
2.11.6 Describe the structure of IPv4 and IPv6
2.11.7 Describe the purpose of IPv4 and IPv6 addressing

Task 2.12 Describe the purpose of a default gateway

Task 2.13 Describe the role of NAT

Task 2.14 Describe OSI and TCP/IP models

2.14.1 Identify the order of the layers of both OSI and TCP/IP models
2.14.2 Compare the similarities of some OSI and TCP/IP layers
2.14.3 Identify the protocols and functions of each OSI layer

Task 2.15 Describe the data-encapsulation process

2.15.1 Describe the PDU format used at different layers

Task 2.16 Identify the characteristics of various types of network firewalls

2.16.1 Traditional firewalls
2.16.2 Next-generation firewalls
2.16.3 Differentiate between NGFWs and traditional firewalls

Task 2.17 Describe the application of NGFW deployment options (i.e., PA-, VM- and CN-Series)

Task 2.18 Differentiate between intrusion detection systems and intrusion prevention systems

2.18.1 Differentiate between knowledge-based and behavior-based systems

Task 2.19 Describe virtual private networks

2.19.1 Describe when to use VPNs

Task 2.20 Differentiate between the different tunneling protocols

Task 2.21 Describe the purpose of data loss prevention

2.21.1 Classify different types of data (e.g., sensitive, inappropriate)

Task 2.22 Differentiate the various types of security functions from those that are integrated into UTM devices

Task 2.23 Describe endpoint security standards

2.23.1 Describe the advantages of endpoint security
2.23.2 Describe host-based intrusion detection/prevention systems
2.23.3 Differentiate between signature-based and behavioral-based malware protection
2.23.4 Describe application block and allow listing
2.23.5 Describe the concepts of false-positive and false-negative alerts
2.23.6 Describe the purpose of anti-spyware software

Task 2.24 Identify differences in managing wireless devices compared to other endpoint devices

Task 2.25 Describe the purpose of identity and access management

2.25.1 Single- and multi-factor Authentication
2.25.2 Separation of duties and impact on privileges
2.25.3 RBAC, ABAC, DAC, and MAC
2.25.4 User profiles

Task 2.26 Describe the integration of NGFWs with the cloud, networks, and endpoints

Task 2.27 Describe App-ID, User-ID, and Content-ID

Task 2.28 Describe Palo Alto Networks firewall subscription services

2.28.1 WildFire
2.28.2 URL Filtering
2.28.3 Threat Prevention
2.28.4 DNS Security
2.28.5 IoT Security
2.28.6 SD-WAN
2.28.7 Advanced Threat Prevention
2.28.8 Advanced URL Filtering
2.28.9 GlobalProtect
2.28.10 Enterprise DLP
2.28.11 SaaS Security Inline
2.28.12 Virtual Systems

Task 2.29 Describe network security management

2.29.1 Identify the deployment modes of Panorama

2.29.2 Describe the three components of Best Practice Assessment (BPA)

Domain 3 Cloud Technologies 20%

Task 3.1 Describe the NIST cloud service and deployment models

Task 3.2 Recognize and list cloud security challenges

3.2.1 Describe the vulnerabilities in a shared community environment

3.2.2 Describe cloud security responsibilities

3.2.3 Describe cloud multitenancy

3.2.4 Differentiate between security tools in various cloud environments

3.2.5 Describe identity and access management controls for cloud resources

3.2.6 Describe different types of cloud security alerts and notifications

Task 3.3 Identify the 4 Cs of cloud native security

Task 3.4 Describe the purpose of virtualization in cloud computing

3.4.1 Describe the types of hypervisors

3.4.2 Describe characteristics of various cloud providers

3.4.3 Describe economic benefits of cloud computing and virtualization

3.4.4 Describe the security implications of virtualization

Task 3.5 Explain the purpose of containers in application deployment

3.5.1 Differentiate containers versus virtual machines

3.5.2 Describe Container as a Service

3.5.3 Differentiate a hypervisor from a Docker Container

Task 3.6 Describe how serverless computing is used

Task 3.7 Describe DevOps

Task 3.8 Describe DevSecOps

Task 3.9 Illustrate the continuous integration/continuous delivery pipeline

Task 3.10 Explain governance and compliance related to deployment of SaaS applications

3.10.1 Describe security compliance to protect data

3.10.2 Describe privacy regulations globally

3.10.3 Describe security compliance between local policies and SaaS

applications

Task 3.11 **Describe the cost of maintaining a physical data center**

Task 3.12 **Differentiate between data-center security weaknesses of traditional solutions versus cloud environments**

Task 3.13 **Differentiate between east-west and north-south traffic patterns**

Task 3.14 **Describe the four phases of hybrid data-center security**

Task 3.15 **Describe how data centers can transform their operations incrementally**

Task 3.16 **Describe the cloud-native security platform**

Task 3.17 **Identify the four pillars of Prisma Cloud application security**

Task 3.18 **Describe the concept of SASE**

Task 3.19 **Describe the SASE layer**

3.19.1 Describe sanctioned, tolerated, and unsanctioned SaaS applications

3.19.2 List how to control sanctioned SaaS usage

Task 3.20 **Describe the network-as-a-service layer**

Task 3.21 **Describe how Prisma Access provides traffic protection**

Task 3.22 **Describe Prisma Cloud Security Posture Management (CSPM)**

Domain 4 **Elements of Security Operations** **20%**

Task 4.1 **Describe the main elements included in the development of SOC business objectives**

Task 4.2 **Describe the components of SOC business management and operations**

Task 4.3 **List the six essential elements of effective security operations**

Task 4.4 **Describe the four SecOps functions**

- 4.4.1 Identify
- 4.4.2 Investigate
- 4.4.3 Mitigate
- 4.4.4 Improve

Task 4.5 **Describe SIEM**

Task 4.6 **Describe the purpose of security orchestration, automation, and response (SOAR)**

Task 4.7 **Describe the analysis tools used to detect evidence of a security compromise**

Task 4.8 **Describe how to collect security data for analysis**

Task 4.9 **Describe the use of analysis tools within a security operations environment**

Task 4.10 **Describe the responsibilities of a security operations engineering team**

Task 4.11 **Describe the Cortex platform in a security operations environment and the purpose of Cortex XDR for various endpoints**

Task 4.12 **Describe how Cortex XSOAR improves security operations efficiency**

Task 4.13 **Describe how Cortex Data Lake improves security operations visibility**

Task 4.14 **Describe how XSIAM can be used to accelerate SOC threat response**