Palo Alto Networks Certified Cybersecurity Entry-level Technician (PCCET) Blueprint

Domain Weight (%)

Fundamentals of Cybersecurity	**15%**
The Connected Globe	**25%**
Cloud Technologies	**30%**
Elements of Security Operations	**30%**

Domain 1 Fundamentals of Cybersecurity 15%

Task 1.1 Identify Web 2.0/3.0 applications and services

1.1.1 List common Web 2.0/3.0 applications.
1.1.2 Differentiate between SaaS, PaaS and IaaS.
1.1.3 Distinguish between Web 2.0 and 3.0 applications and services.

Task 1.2 Recognize applications used to circumvent port-based firewalls

1.2.1 Identify applications by their port number.
1.2.2 Understand port scanning.
1.2.3 Understand how to use port scanning tools.
1.2.4 Understand different risk levels of applications.
1.2.5 Understand the impact of using non standard ports.

Task 1.3 Summarize cloud computing challenges and best practices

1.3.1 Define DevOps.
1.3.2 Understand the impact of Service Level Agreements (SLA) with cloud contracts.
1.3.3 Differentiate between cloud types.
1.3.4 Understand the application of the security within the different types of clouds.
1.3.5 Understand the impact of change management.
1.3.6 Understand the roles within a cloud environment.

Task 1.4 Identify SaaS application risks

1.4.1 Understand the nature of data being stored in the SaaS application.
1.4.2 Understand roles within a SaaS environment.

1.4.3 Understand who has access to what within a system.
1.4.4 Understand security controls for SaaS applications.

Task 1.5 Recognize cybersecurity laws and regulations

1.5.1 Understand the impact of governance regulation and compliance.
1.5.2 Differentiate between major cybersecurity laws and implications.
1.5.3 Understand governance versus regulations.
1.5.4 Understand the code of professional conduct.

Task 1.6 List recent high-profile cyberattack examples

1.6.1 List recent high-profile cyberattack examples.
1.6.2 Understand how to use CVE.
1.6.3 Understand how to use CVS.
1.6.4 Given a cyberattack example, identify what key vulnerability exists.
1.6.5 Identify a leading indicator of a compromise.

Task 1.7 Discover attacker profiles and motivations.

1.7.1 Identify the different attacker profiles.
1.7.2 Understand the different value levels of the information that needs to be protected.
1.7.3 Identify motivations of different types of actors.

Task 1.8 Describe the modern cyberattack life-cycle

1.8.1 Understand the different phases of the modern cyber life-cycle.
1.8.2 Understand events at each level of the cyber life-cycle.

Task 1.9 Classify malware types

1.9.1 Classify the different types of malware.
1.9.2 Understand appropriate actions for the different types of malware.
1.9.3 Identify the characteristics and capabilities for different types of malware.

Task 1.10 List the differences between vulnerabilities and exploits

1.10.1 Order the steps on the vulnerability/exploit timeline.
1.10.2 Differentiate between vulnerabilities and exploits.

Task 1.11 Categorize spamming and phishing attacks

1.11.1 Differentiate between spamming and phishing attacks.
1.11.2 GIven specific examples, define the type of attack.
1.11.3 Identify what the chain of events are as a result of an attack.

Task 1.12 Social Engineering

1.12.1 Identify different methodologies for social engineering.
1.12.2 Identify what the chain events are as a result of social engineering.

Task 1.13

1.13.1 Differentiate between DoS and DDoS.
1.13.2 Define the functionality of bots and botnets.
1.13.3 Differentiate between the use of a bot or botnets.
1.13.4 Understand the type of IoT devices that are part of a botnet attack.
1.13.5 Understand the purpose for Command and Control (C2).
1.13.6 Differentiate the TCP/IP roles in DDoS attacks.

Task 1.14 Define the characteristics of advanced persistent threats

1.14.1 Understand advanced persistent threats.
1.14.2 Understand the purpose for Command and Control (C2).
1.14.3 Identify where the indicators are located.

Task 1.15 Recognize common Wi-Fi attacks

1.15.1 Differentiate between different types of Wi-Fi attacks.
1.15.2 Identify common attack areas for Wi-Fi attacks.
1.15.3 Understand how to monitor your Wi-Fi network.

Task 1.16 Define perimeter-based network security

1.16.1 Define perimeter-based network security.
1.16.2 Define DMZ.
1.16.3 Define where the perimeter is located.
1.16.4 Differentiate between North and South and East and West Zones.
1.16.5 Identify the types of devices used in perimeter defense.
1.16.6 Understand the transition from a trusted network to an untrusted network.

Task 1.17 Explain Zero Trust design principles and architecture configuration

1.17.1 Define Zero Trust.
1.17.2 Differentiate between Trust and Untrust zones.
1.17.3 Identify the benefits of the Zero Trust model.
1.17.4 Identify the design principles for Zero Trust.
1.17.5 Understand microsegmentation.

Task 1.18 Define the capabilities of an effective Security Operating Platform

1.18.1 Understand the integration of services for Network, Endpoint, and Cloud services.
1.18.2 Identify the capabilities of an effective Security Operating Platform.
1.18.3 Understand the components of the Security Operating Platform.

Task 1.19 Recognize Palo Alto Networks Strata, Prisma, and Cortex Technologies

1.19.1 Identify examples of Palo Alto Networks technologies associated with securing the enterprise.
1.19.2 Describe Palo Alto Networks approach to securing the cloud through the most comprehensive threat protection, governance, and compliance offering in the industry.
1.19.3 Understand how Palo Alto Networks technology natively integrates network, endpoint, and cloud to stop sophisticated attacks.

Domain 2 The Connected Globe 25%

Task 2.1 Define the differences between hubs, switches, and routers

2.1.1 Differentiate between hubs, switches and routers.
2.1.2 Define the role of hubs, switches and routers.
2.1.3 Given a network diagram, Identify the icons for hubs, switches and routers.
2.1.4 Understand the use of VLANs.

Task 2.2 Classify routed and routing protocols

2.2.1 Identify routed protocols.
2.2.2 Identify routing protocols.
2.2.3 Differentiate between static and dynamic routing protocols.
2.2.4 Differentiate between link state and distance vector.

Task 2.3 Summarize area networks and topologies

2.3.1 Identify the borders of collision domains.
2.3.2 Identify the borders of broadcast domains.
2.3.3 Identify different types of networks.
2.3.4 Identify WAN technologies.
2.3.5 Understand the advantages of SD-WAN.
2.3.6 Understand LAN technologies.

Task 2.4 Explain the purpose of the Domain Name System (DNS)

2.4.1 Understand the DNS hierarchy.
2.4.2 Understand the DNS record types.
2.4.3 Understand how DNS record types are used.
2.4.4 Identify a fully qualified domain name (FQDN).

Task 2.5 Identify categories of Internet of Things (IoT)

2.5.1 Identify IoT connectivity technologies.
2.5.2 Identify the known security risks associated with IoT.
2.5.3 Identify the security solutions for IoT devices.
2.5.4 Differentiate between categories of IoT devices.

Task 2.6 Illustrate the structure of an IPV4/IPV6 address

2.6.1 Identify dotted decimal notation.
2.6.2 Identify the structure of IPV6.
2.6.3 Understand the purpose of IPV4 and IPV6 addressing.
2.6.4 Understand the purpose of a default gateway.
2.6.5 Understand the role of NAT.
2.6.6 Understand the role of ARP.

Task 2.7 Describe the purpose of IPV4 subnetting.

2.7.1 Understand binary to decimal conversion.
2.7.2 Understand CIDR notation.
2.7.3 Define classful subnetting.
2.7.4 Given a scenario, identify the proper subnet mask.
2.7.5 Understand the purpose of subnetting.

Task 2.8 Illustrate the OSI and TCP/IP models

2.8.1 Identify the order of the layers of both OSI and TCP/IP models.
2.8.2 Compare the similarities of some OSI and TCP/IP models.
2.8.3 Identify the function of each of the layers.
2.8.4 Understand the advantages of using a layered model.
2.8.5 Identify protocols at each layer.

Task 2.9 Explain the data encapsulation process

2.9.1 Understand the data encapsulation process.
2.9.2 Understand the PDU format used at different layers.

Task 2.10 Classify the various types of network firewalls

2.10.1 Identify the characteristics of various types of network firewalls.

2.10.2 Understand the applications of the different types of network firewalls.

Task 2.11 Compare intrusion detection and intrusion prevention systems

2.11.1 Understand the concept of intrusion detection systems.
2.11.2 Understand the concept of intrusion prevention systems.
2.11.3 Differentiate between intrusion detection systems and intrusion prevention systems.
2.11.4 Differentiate between knowledge-based and behavior-based systems.

Task 2.12 Define virtual private networks

2.12.1 Define virtual private networks.
2.12.2 Differentiate between IPSec and SSL.
2.12.3 Differentiate between the different tunneling protocols.
2.12.4 Understand when to use a VPN.
2.12.5 Understand the benefits of tunneling protocols.

Task 2.13 Explain data loss prevention

2.13.1 Define the purpose of data loss prevention.
2.13.2 Understand what would be considered sensitive data.
2.13.3 Understand what would be considered inappropriate data.

Task 2.14 Describe unified threat management

2.14.1 Differentiate between UTM and other portals logged into to do work.
2.14.2 Understand how UTM integrates different aspects of content.
2.14.3 Understand how the different content within the OSIs are being examined with UTM.
2.14.4 Identify the security functions that are integrated with UTM.

Task 2.15 Define endpoint security basics

2.15.1 Understand what is an endpoint.
2.15.2 Understand the advantages of endpoint security.
2.15.3 Understand what endpoints can be supported.
2.15.4 Given an environment, identify what security methods could be deployed.
2.15.5 Understand the concept of a personal firewall.
2.15.6 Understand what traffic flows through a personal firewall.
2.15.7 Define host-based intrusion prevention systems.

2.15.8 Understand the disadvantages of host-based intrusion prevention systems.

Task 2.16 Compare signature and container-based malware protection

2.16.1 Define signature-based malware protection.
2.16.2 Define container-based malware protection.
2.16.3 Differentiate between signature-based and container-based malware protection.
2.16.4 Understand application whitelisting.
2.16.5 Understand the concepts of false-positive and false-negative alerts.
2.16.6 Define the purpose of anti-spyware software.

Task 2.17 Recognize types of mobile device management

2.17.1 Identify the capabilities of mobile device management.
2.17.2 Identify the vulnerabilities of mobile devices.
2.17.3 Identify different types of mobile devices.
2.17.4 Understand how to secure devices using the MDM controls.

Task 2.18 Explain the purpose of identity and access management

2.18.1 Identify the As in the AAA model.
2.18.2 Understand the purpose of identity and access management.
2.18.3 Understand the risk of not using identity and access management.
2.18.4 Understand the concept of least privilege.
2.18.5 Understand the separation of duties.
2.18.6 Understand RBAC and ABAC and Discretionary Access Control and Mandatory Access Control.
2.18.7 Understand the user profile.
2.18.8 Understand the impact of onboarding and offboarding from systems.
2.18.9 Understand directory services.

Task 2.19 Describe configuration management

2.19.1 Understand configuration management.
2.19.2 Identify how configuration management interacts with different development methodologies.
2.19.3 Understand system services required for configuration Management.

Task 2.20 Identify next-generation firewall features and capabilities

2.20.1 Differentiate between NGFWs and FWs.

2.20.2 Understand the integration of NGFWs with the cloud, networks and endpoints.
2.20.3 Define App-ID.
2.20.4 Define Content-ID.
2.20.5 Define User-ID.

Task 2.21 Compare the NGFW four core subscription services

2.21.1 Differentiate between the four core NGFW subscription services.
2.21.2 Define WildFire.
2.21.3 Define URL Filtering.
2.21.4 Define Threat Prevention.
2.21.5 Define DNS security.

Task 2.22 Define the purpose of network security management (Panorama)

2.22.1 Define Panorama services and controls.
2.22.2 Understand network security management.
2.22.3 Identify the deployment modes of Panorama.

Domain 3 Cloud Technologies 30%

Task 3.1 Define the NIST cloud service and deployment models

3.1.1 Define the NIST cloud service models.
3.1.2 Define the NIST cloud deployment models.

Task 3.2 Recognize and list cloud security challenges

3.2.1 Understand where vulnerabilities are in a shared community environment.
3.2.2 Understand security responsibilities.
3.2.3 Understand multi-tenancy.
3.2.4 Differentiate between security tools in different environments.
3.2.5 Define identity and access management controls for cloud resources.
3.2.6 Understand different types of alerts and notifications.
3.2.7 Identify the 4 Cs of cloud native security.

Task 3.3 Define the purpose of virtualization in cloud computing

3.3.1 Define the types of hypervisors.
3.3.2 Describe popular cloud providers.
3.3.3 Define economic benefits of cloud computing and virtualization.

3.3.4 Understand the security implications of virtualization.

Task 3.4 Explain the purpose of containers in application deployment

3.4.1 Understand the purpose of containers.
3.4.2 Differentiate containers versus virtual machines.
3.4.3 Define Container as a Service.
3.4.4 Differentiate hypervisor from a Docker.

Task 3.5 Discuss the purpose of serverless computing

3.5.1 Understand the purpose of serverless computing.
3.5.2 Understand how serverless computing is used.

Task 3.6 Compare the differences between DevOps and DevSecOps

3.6.1 Define DevOps.
3.6.2 Define DevSecOps.
3.6.3 Illustrate the CI/CD pipeline.

Task 3.7 Explain governance and compliance related to deployment of SaaS applications

3.7.1 Understand security compliance to protect data.
3.7.2 Understand privacy regulations globally.
3.7.3 Understand security compliance between local policies and SaaS applications.

Task 3.8 Illustrate traditional data security solution weaknesses

3.8.1 Understand the cost of maintaining a physical data center.
3.8.2 Differentiate between data center security weakness of traditional solution to cloud solution.
3.8.3 Differentiate between data center security weakness of traditional solution to perimeter localization solution.

Task 3.9 Compare east-west and north-south traffic protection

3.9.1 Define east-west traffic patterns.
3.9.2 Define north-south traffic patterns.
3.9.3 Differentiate between east-west and north-south traffic patterns.

Task 3.10 Recognize the four phases of hybrid data center security

3.10.1 Define the four phases of hybrid data center security.
3.10.2 Differentiate between traditional three-tier architectures and evolving virtual data centers.

Task 3.11 List the four pillars of cloud application security (Prisma Cloud)

3.11.1 Define cloud native security platform.

3.11.2 Identify the four pillars of Prisma cloud application security.

Task 3.12 Illustrate the Prisma Access SASE architecture

3.12.1 Understand the concept of SASE.

3.12.2 Define the SASE layer.

3.12.3 Define the Network as a Service layer.

3.12.4 Define how Prisma Access provides traffic protection.

Task 3.13 Compare sanctioned, tolerated and unsanctioned SaaS applications

3.13.1 Define application use and behavior.

3.13.2 List how to control sanctioned SaaS usage.

Domain 4 Elements of Security Operations 30%

Task 4.1 List the six essential elements of effective security operations

4.1.1 List the six essential elements of effective security operations.

4.1.2 Define the “Identify” SecOps function.

4.1.3 Define the “Investigate” SecOps function.

4.1.4 Define the “Mitigate” SecOps function.

4.1.5 Define the “Improve” SecOps function.

Task 4.2 Describe the purpose of security information and event management (SIEM) and SOAR

4.2.1 Define SIEM.

4.2.2 Define SOAR.

4.2.3 Define incident and response procedures in a digital workflow format.

4.2.4 Define the purpose of security orchestration, automation, and response.

Task 4.3 Describe the analysis tools used to detect evidence of a security compromise

4.3.1 Define the analysis tools used to detect evidence of a security compromise.

4.3.2 Understand how to collect data that will be analyzed.

4.3.3 Understand why we use analysis tools within a Security operations environment.

4.3.4 Define the responsibilities of a security operations engineering team.

Task 4.4 Describe features of Cortex XDR endpoint protection technology

4.4.1 Understand the Cortex platform in a Security Operations environment.

4.4.2 Define the purpose of Cortex XDR for various endpoints.

Task 4.5 Describe how Cortex XSOAR improves SOC efficiency and how Cortex Data Lake improves SOC visibility

4.5.1 Understand how Cortex XSOAR improves Security Operations efficiency.

4.5.2 Understand how Cortex Data Lake improves Security Operations visibility.

Task 4.6 Explain how AutoFocus gains threat intelligence for security analysis and response.

4.6.1 Understand how AutoFocus gains threat intelligence for security analysis and response.

4.6.2 Describe how AutoFocus can reduce the time required to investigate
threats by leveraging third party services.