paloalto® NETWORKS

Palo Alto Networks Prisma Cloud Certified Security Engineer (PCCSE)
Blueprint

Domain Weight (%)

Install and Upgrade	**8%**
Visibility, Security, Compliance, and Data Security	**33%**
Cloud Workload Protection Platform	**18%**
Web Application and API Security (WAAS)	**8%**
Dev SecOps Security (Shift Left)	**13%**
Prisma Cloud Administration	**20%**

Domain 1 Install and upgrade 8%

Task 1.1 Deploy and manage Console for the Compute Edition

1.1.1 Locate and download Prisma Cloud release software.

1.1.2 Install Console in onebox configuration.

1.1.3 Install Console in Kubernetes.

1.1.4 Perform upgrade on Console.

Task 1.2 Deploy and manage Defenders

1.2.1 Deploy Container Defenders.

1.2.2 Deploy Host Defenders.

1.2.3 Deploy Serverless Defenders.

1.2.4 Deploy App-embedded Defenders.

1.2.5 Configure networking for Defender to Console connectivity.

1.2.6 Perform upgrade on Defenders.

Domain 2 Visibility, Security, Compliance, and Data Security 33%

Task 2.1 Configure policies

2.1.1 Understand policies related to compliance standards.

2.1.2 Build custom policies.

2.1.3 Identify policy types.

Task 2.2 Configure alerting and notifications

2.2.1 Understand alert states.

2.2.2 Build alert rules.

2.2.3 Create alert notifications.

2.2.4 Investigate alerts.

Task 2.3 Understand third-party integrations

2.3.1 Understand inbound and outbound notifications.

Task 2.4 Perform ad hoc investigations

2.4.1 Investigate resource configuration with RQL.

2.4.2 Investigate user activity using RQL.

2.4.3 Investigate network activity using RQL.

2.4.4 Investigate anomalous user event(s).

Task 2.5 Identify assets in a Cloud account

2.5.1 Identify inventory of resources in a cloud account.

2.5.2 Identify how to check resource configuration history.

Task 2.6 Use Prisma Cloud APIs

2.6.1 Use APIs for automation of tasks.

2.6.2 Use APIs for custom queries.

Task 2.7 Remediation

2.7.1 Identify the requirements to use auto-remediation.

2.7.2 Differentiate between when to use manual versus automated remediation.

Task 2.8 Onboarding

2.8.1 Identify the process for onboarding cloud accounts with data protection

2.8.2 Configure CloudTrail and SNS.

2.8.3 Configure Scan options.

Task 2.9 Use Data Dashboard Features

2.9.1 Classify Objects.

2.9.2 List object permissions for visibility.

2.9.3 View Data Inventory,

2.9.4 View Resource Explore.

2.9.5 List Object Identifiers.

2.9.6 Understand Object exposure rates.

Task 2.10 Assess Data Policies and Alerts

2.10.1 Differentiate between malware and regular policies.

2.10.2 Understand the scope of alert notifications.

Domain 3 Cloud Workload Protection Platform 18%

Task 3.1 Monitor and Protect Against Image Vulnerabilities

3.1.1 Understand how to Investigate Image Vulnerabilities.

3.1.2 Configure Image Vulnerability Policy.

Task 3.2 Monitor and Protect Host Vulnerabilities

3.2.1 Understand how to Investigate Host Vulnerabilities.

3.2.2 Configure Host Vulnerability Policy.

Task 3.3 Monitor and Enforce Image/Container Compliance

3.3.1 Understand how to Investigate Image and Container Compliance.

3.3.2 Configure Image and Container Compliance Policy.

Task 3.4 Monitor and Enforce Host Compliance

3.4.1 Understand how to Investigate Host Compliance.

3.4.2 Configure Host Compliance Policy.

Task 3.5 Monitor and Enforce Container Runtime

3.5.1 Understand container models.

3.5.2 Configure container runtime policies.

3.5.3 Understand container runtime audits.

3.5.4 Investigate incidents using Incident Explorer.

Task 3.6 Configure WAAS policies

3.6.1 Configure WAAS policies to create a relevant WAAS rule.

Task 3.7 Monitor and Protect Against Serverless Vulnerabilities

3.7.1 Understand how to Investigate Serverless Vulnerabilities.

3.7.2 Configure Serverless Vulnerability Policy.

3.7.3 Configure Serverless Auto-Protect functionality.

Domain 4 Web Application and API Security (WAAS) 8%

Task 4.1 Create a WAAS policy and an App rule

4.1.1 Define the application specifications.

4.1.2 Define or import API methods.

4.1.3 Limit access to different REST API endpoints.

Task 4.2 Configure application firewall settings and exceptions

4.2.1 Configure DoS protection.

4.2.2 Configure access controls to limit inbound sources.

4.2.3 Manage network lists

4.2.4 Configure access controls to enforce HTTP headers and file uploads.

4.2.5 Configure bot protection.

Task 4.3 Investigate WAAS runtime audit

4.3.1 Determine the reasons for a WAAS runtime audit.

Domain 5 Dev SecOps Security (Shift Left) 13%

Task 5.1 Implement scanning for IAC templates

5.1.1 Differentiate between Terraform and Cloudformation scanning configurations.

5.1.2 List OOTB IAC scanning integrations.

5.1.3 Configure API scanning for IAC templates.

.

Task 5.2 Configure policies in Console for IAC scanning

5.2.1 Review OOTB policies for IAC scanning.

5.2.2 Configure custom build policies for IAC scanning.

Task 5.3 Integrate Compute scans into CI/CD pipeline.

5.3.1 Integrate image scans into CI/CD pipeline.

5.3.2 Integrate serverless scans into CI/CD pipeline.

5.3.3 Identify different options for scanning: twistclip and plugins.

Task 5.4 Configure CI policies for Compute scanning.

5.4.1 Review default CI policies for Compute scanning

5.4.2 Configure custom CI policies for Compute scanning.

Domain 6 Prisma Cloud Administration 20%

Task 6.1 Onboard Accounts

6.1.1 Onboard cloud accounts.

6.1.2 Configure account groups.

Task 6.2 Configure RBAC

6.2.1 Differentiate between Primsa Cloud and Compute roles.

6.2.2 Configure Prisma Cloud and Compute roles.

Task 6.3 Configure admission controller

6.3.1 Configure defender as an admission controller.

6.3.2 Create OPA policies.

Task 6.4 Configure logging

6.4.1 Familiarize with audit logging.

6.4.2 Enable defender logging.

Task 6.5 Manage enterprise settings

6.5.1 Differentiate Anomaly settings.

6.5.2 Configure idle timeout.

6.5.3 Set autoenable policies.

6.5.4 Set mandatory dismissal reason.

6.5.5 Enable user attribution.

Task 6.6 Understand third-party integrations

6.6.1 Understand inbound and outbound notifications.

6.6.2 Configure third-party integration for alerts.

Task 6.7 Leverage Cloud and Compute APIs

6.7.1 Authenticate with APIs.

6.7.2 Locate API documentation.

6.7.3 List policies by API.

6.7.4 Manage alerts using APIs.

6.7.5 Create reports using APIs.

6.7.6 Download vulnerability results via API.

6.7.7 Configure Single Sign On.

6.7.8 Use the access key.