paloalto®
NETWORKS

Palo Alto Networks Certified Security Automation Engineer (PCSAE) Blueprint

Domain Weight (%)

Playbook Development	**25%**
Incident Types, Indicator Types, Layouts, and Fields	**20%**
Automations and Integrations and Related Concepts	**20%**
Solution Architecture	**15%**
Content Updates and Content Management	**10%**
UI Workflow, Dashboards, and Reports	**10%**

Domain 1 Playbook Development 25%

Task 1.1 Conceptualize context data.

1.1.1 Query and use context data.
1.1.2 Differentiate between public and private contexts.

Task 1.2 Summarize the difference between inputs, outputs and results for playbook tasks.

1.2.1 Describe inputs and outputs for playbook tasks.
1.2.2 Describe inputs and outputs sub-playbooks.
1.2.3 Configure playbooks using the UI (e.g., box of text that you fill in).
1.2.4 Read, troubleshoot, and respond to error conditions.

Task 1.3 Outline how to use Loop sub-playbooks

1.3.1 Differentiate between the three different loop types of playbooks.

Task 1.4 Differentiate between playbook task types.

1.4.1 Differentiate between manual, automatic, and conditional playbook tasks.
1.4.2 Gather, analyze, and evaluate data to make decisions about specific playbook task types.

Task 1.5 Use Filters and transformers to manipulate data.

1.5.1 Explain the difference between filters and transformers.
1.5.2 Identify when filtering and transforming data is required.
1.5.3 Specify and explain different options of filters and transformers.

Domain 2 Incident Types, Indicator Types, Layouts, and Fields 20%

Task 2.1 Compare and contrast the different incident types.

2.1.1 Outline the capabilities, functions, and features related to each incident type.
2.1.2 Summarize the relationship between external data and the XSOAR incident type.
2.1.3 Assess the consequences of miscategorized incident types.
2.1.4 Describe how to leverage machine learning in XSOAR.
2.1.5 Schedule a job to create a new incident to run a playbook.

Task 2.2 Outline the different layout types.

2.2.1 Summarize the purpose of each layout type.
2.2.2 Specify the different incident layout special sections.
2.2.3 Summarize the main layout options.

Task 2.3 Compare and contrast the different indicator types.

2.3.1 Outline the capabilities, functions, and features related to each indicator type.
2.3.2 Explain how data is mapped to an indicator.
2.3.3 Define criteria for exclusion list entries.

Task 2.4 Summarize field types, associated capabilities, and purpose.

2.4.1 Outline the different field types.
2.4.2 Align appropriate field types to data types.
2.4.3 Summarize how fields are created and used.
2.4.4 Outline advanced field capabilities.

Domain 3 Automations and Integration and Related Concepts 20%

Task 3.1 Use automations to respond to incidents.

3.1.1 Outline the different types of automation.

3.1.2 Differentiate between inputs and outputs.
3.1.3 Apply script helper.
3.1.4 Apply permission access.
3.1.5 Differentiate automation objects.
3.1.6 Apply appropriate automation commands.
3.1.7 Identify how to build and test automations.
3.1.8 Use automations for Incidents and Playbook tasks.

Task 3.2 Outline integration concepts.

3.2.1 Differentiate between parameters and arguments.
3.2.2 Implement role-based access and controls (RBAC).
3.2.3 Define integration types.
3.2.4 Describe capabilities related to custom integrations.
3.2.5 Describe the process of contributing integrations to the marketplace.

Task 3.3 Configure integration instances.

3.3.1 Apply basic troubleshooting if the integration is not performing.
3.3.2 Apply the appropriate classification and mapping technique.
3.3.3 Classify and map a set of data to different types of fields.

Domain 4 Solution Architecture 15%

Task 4.1 Describe the components of the XSOAR System Architecture.

4.1.1 Describe the relationship between servers, live backup, Devprod, and other available components.
4.1.2 Summarize how XSOAR uses the Docker component.
4.1.3 Specify the benefits and differences between back-up types.
4.1.4 Differentiate between a stand-alone tenant and multi-tenant.
4.1.5 Describe threat intelligence management capabilities.

Task 4.2 Assess system architecture and outline scalability opportunities.

4.2.1 Review the system diagram and summarize the flow of data.
4.2.2 Export log bundle and send for investigation.
4.2.3 Identify common errors and refer for troubleshooting.
4.2.4 Identify usage of engines.

Task 4.3 **Create incidents using XSOAR.**

4.3.1 Describe the three ways incidents are created.
4.3.2 Understand the logic and order of incident creation.

Domain 5 **Content Updates and Content Management** **10%**

Task 5.1 **Outline marketplace concepts.**

5.1.1 Identify challenges and benefits related to marketplace concepts.
5.1.2 Describe marketplace content.
5.1.3 Outline the product development lifecycle.
5.1.4 Identify how content can be searched.
5.1.5 Describe the relationship between the marketplace and Docker.

Task 5.2 **Apply custom content and manage content updates.**

5.2.1 Describe the purpose of content updates.
5.2.2 Outline the process of how content is updated and why.
5.2.3 Summarize the relationship between customer content and existing content updates.
5.2.4 Outline recommendations for content updates and when custom content would be appropriate.
5.2.5 Identify the benefits of custom content.
5.2.6 Describe how new content gets implemented.
5.2.7 Explain when imports or exports are appropriate and how it would be done.

Domain 6 **UI Workflow, Dashboards, and Reports** **10%**

Task 6.1 **Navigate the UI and query system data.**

6.1.1 Navigate between the different options in the system.
6.1.2 Write a structured query using the appropriate syntax.

Task 6.2 **Summarize the workflow elements used during an investigation.**

6.2.1 Outline the purpose of the workflow elements.
6.2.2 Differentiate the workflow elements and the impact on an investigation.

Task 6.3 Create dashboards and reports.

6.3.1 Outline the difference between dashboards and reports.
6.3.2 Select the appropriate dashboard or report.
6.3.3 Summarize what information can be added, edited or shared within dashboards and reports.

Task 6.4 Apply the appropriate widget type.

6.4.1 Describe the purpose of widgets.
6.4.2 Define when custom widgets are necessary.