PALO ALTO PCSAE

Palo Alto PCSAE Certification Questions & Answers

Exam Summary – Syllabus – Questions

PCSAE

Palo Alto Networks Certified Security Automation Engineer

85 Questions Exam – Variable (70-80 / 100 Approx.) Cut Score – Duration of 80 minutes

Table of Contents:

Know Your PCSAE Certification Well:

The PCSAE is best suitable for candidates who want to gain knowledge in the Palo Alto Engineer. Before you start your PCSAE preparation you may struggle to get all the crucial PCSAE materials like PCSAE syllabus, sample questions, study guide.

But don't worry the PCSAE PDF is here to help you prepare in a stress-free manner.
The PDF is a combination of all your queries like-

- What is in the PCSAE syllabus?
- How many questions are there in the PCSAE exam?
- Which Practice test would help me to pass the PCSAE exam at the first attempt?

Passing the PCSAE exam makes you Palo Alto Networks Certified Security Automation Engineer. Having the PCSAE certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

Palo Alto PCSAE Certification Details:

Exam Name	Security Automation Engineer
Exam Code	PCSAE
Exam Price	$175 USD
Duration	80 minutes
Number of Questions	85
Passing Score	Variable (70-80 / 100 Approx.)
Recommended Training	**Cortex XSOAR IT Administrator** **Cortex XSOAR Engineer- Building the Next Generation SOC** **Cortex XSOAR SOC Analyst**
Exam Registration	**PEARSON VUE**
Sample Questions	**Palo Alto PCSAE Sample Questions**

Practice Exam	Palo Alto Networks Certified Security Automation Engineer Practice Test

PCSAE Syllabus:

Section	Weight	Objectives
Playbook Development	27%	- Reference and manipulate context data to manage automation workflow - Summarize inputs, outputs, and results for playbook tasks - Configure inputs and outputs for subplaybook tasks - Enable and configure looping on a subplaybook - Differentiate among playbook task types • Manual • Automated • Conditional • Data collection • Subplaybook - Apply filters and transformers to manipulate data - Apply the playbook debugger to aid in developing playbooks
Incident Objects	13%	- Configure incident types - Identify the role of an incident type within the incident lifecycle - Configure an incident layout • Fields and buttons • Tabs • New/Edit and Close Forms - Summarize the function, capabilities, and purpose of incident fields - Configure classifiers and mappers
Automations, Integrations, and Related Concepts	18%	- Define the capabilities of automation across XSOAR functions • Playbook tasks • War room • Layouts (dynamic sections, buttons)

Section	Weight	Objectives
		• Jobs • Field trigger scripts • Pre/post-processing - Differentiate between automations, commands, and scripts - Interpret and modify automation scripts • Script helper • Script settings • Language types • Script text - Identify the properties and capabilities of the XSOAR framework for integration - Configure and manage integration instances
Content Management and Solution Architecture	17%	- Apply marketplace concepts for the management of content • Searching in marketplace • Installation and updates • Dependencies • Version history • Partner supported versus XSOAR supported • Submitting content to the marketplace - Apply general content customization and management concepts • Custom versus system content • Duplicating content • Importing/exporting custom content • Version control - Manage local changes in a remote repository (dev-prod) configuration - Describe the components of the XSOAR system architecture • System hardware requirements • Remote repositories (dev-prod)

Section	Weight	Objectives
		• Engines • Multitenancy • Elasticsearch/HA • Docker - Describe the incident lifecycle within XSOAR - Define the capabilities of RBAC • Page access • Integration permissions • Incident tabs (layout specification) • Automation permissions • Incident viewing permissions by role - Identify the troubleshooting tools available to obtain more diagnostic information • Log bundles • Integration testing - Identify options available for performance tuning • Ignore output • Quiet mode - Monitor system health using the System Diagnostics page
UI Workflow, Dashboards, and Reports	13%	- Identify methods for querying data • Indicators • Incidents • Dashboards • Global search - Summarize the workflow elements used during an investigation • Layouts • War Room • Work Plan • Evidence Board

Section	Weight	Objectives
		• Actions menu - Interact with layouts for incident management • Sections • Fields • Buttons - Summarize tools used for managing incidents • Bulk incident actions • Table view versus summary view • Table settings - Identify the capabilities of existing dashboards and reports - Summarize what information can be created, edited, or shared within dashboards and reports - Summarize the capabilities of widget builder
Threat Intel Management	12%	- Identify the parameters available for configuring indicator Objects • Layouts and types • Fields • Reputation scripts and commands • Expiration - Generate threat intel reports - Describe the features of the Threat Intel page • Unit 42 intel feature • XSOAR indicators • Export/import capabilities - Configure threat intel feed integrations - Identify the options available to auto extract • Exclusion list • Playbook auto extract • Regex for auto extract • System defaults • Extraction settings for incident types

Palo Alto PCSAE Sample Questions:

Question: 1

On which task does the default indicator extraction value depend?

a) Playbook task
b) Commands
c) Indicator extract
d) Default

Answer: a

Question: 2

Why is Demistomock library used?

a) To integrate script
b) To find source of the problem in the code
c) To debug your integration
d) To check logs and War Room entries

Answer: d

Question: 3

At which layer is indicator expiration applied?

a) Intel report level
b) Indicator type level
c) Management layer
d) Unit level

Answer: b

Question: 4

Where do logs appear after creating a log bundle?

a) /var/log
b) /var/log/demisto
c) DbotRole
d) demisto.dockerfiles

Answer: b

Question: 5

Which two types of actions can be specified with a Standard playbook task?

(Choose two.)

a) Manual
b) Automated
c) Conditional
d) Data Collection

Answer: a, b

Question: 6

The indicator verdict is based on what?

a) User script
b) Indicator type
c) Reputation script
d) Verdict Score

Answer: d

Question: 7

How will you determine whether an incident requires further investigation or not?

a) Using rules and automation
b) Running playbooks
c) Using Cortex XSOAR
d) Using tenants

Answer: a, d

Question: 8

You can install the Cortex XSOAR Engine on which two types of machine? (Choose two.)

a) Windows
b) Mac OS
c) Linus
d) Ubuntu

Answer: a, c

Question: 9

What dynamic field can you add to an Incident Layout?

(Choose two)

a) Phishing link
b) Email header
c) Graph of the number of bad indicators
d) Email body
e) Severity of bad indicators

Answer: c, e

Question: 10

When can the incident team populate Incident fields?

(Choose two)

a) At the beginning of the investigation
b) After accepting the incident data coming from incidents
c) After adding custom fields for incidents, evidence and indicators
d) During an investigation
e) After closing the investigation

Answer: a, d

Study Guide to Crack Palo Alto PCSAE Exam:

- Getting details of the PCSAE syllabus, is the first step of a study plan. This pdf is going to be of ultimate help. Completion of the syllabus is must to pass the PCSAE exam.
- Making a schedule is vital. A structured method of preparation leads to success. A candidate must plan his schedule and follow it rigorously to attain success.
- Joining the Palo Alto provided training for PCSAE exam could be of much help. If there is specific training for the exam, you can discover it from the link above.

- Read from the PCSAE sample questions to gain your idea about the actual exam questions. In this PDF useful sample questions are provided to make your exam preparation easy.
- Practicing on PCSAE practice tests is must. Continuous practice will make you an expert in all syllabus areas.

Reliable Online Practice Test for PCSAE Certification

Make NWExam.com your best friend during your Security Automation Engineer exam preparation. We provide authentic practice tests for the PCSAE exam. Experts design these online practice tests, so we can offer you an exclusive experience of taking the actual PCSAE exam. We guarantee you 100% success in your first exam attempt if you continue practicing regularly. Don't bother if you don't get 100% marks in initial practice exam attempts. Just utilize the result section to know your strengths and weaknesses and prepare according to that until you get 100% with our practice tests. Our evaluation makes you confident, and you can score high in the PCSAE exam.

Start Online practice of PCSAE Exam by visiting URL
https://www.nwexam.com/palo-alto/pcsae-palo-alto-security-automation-engineer