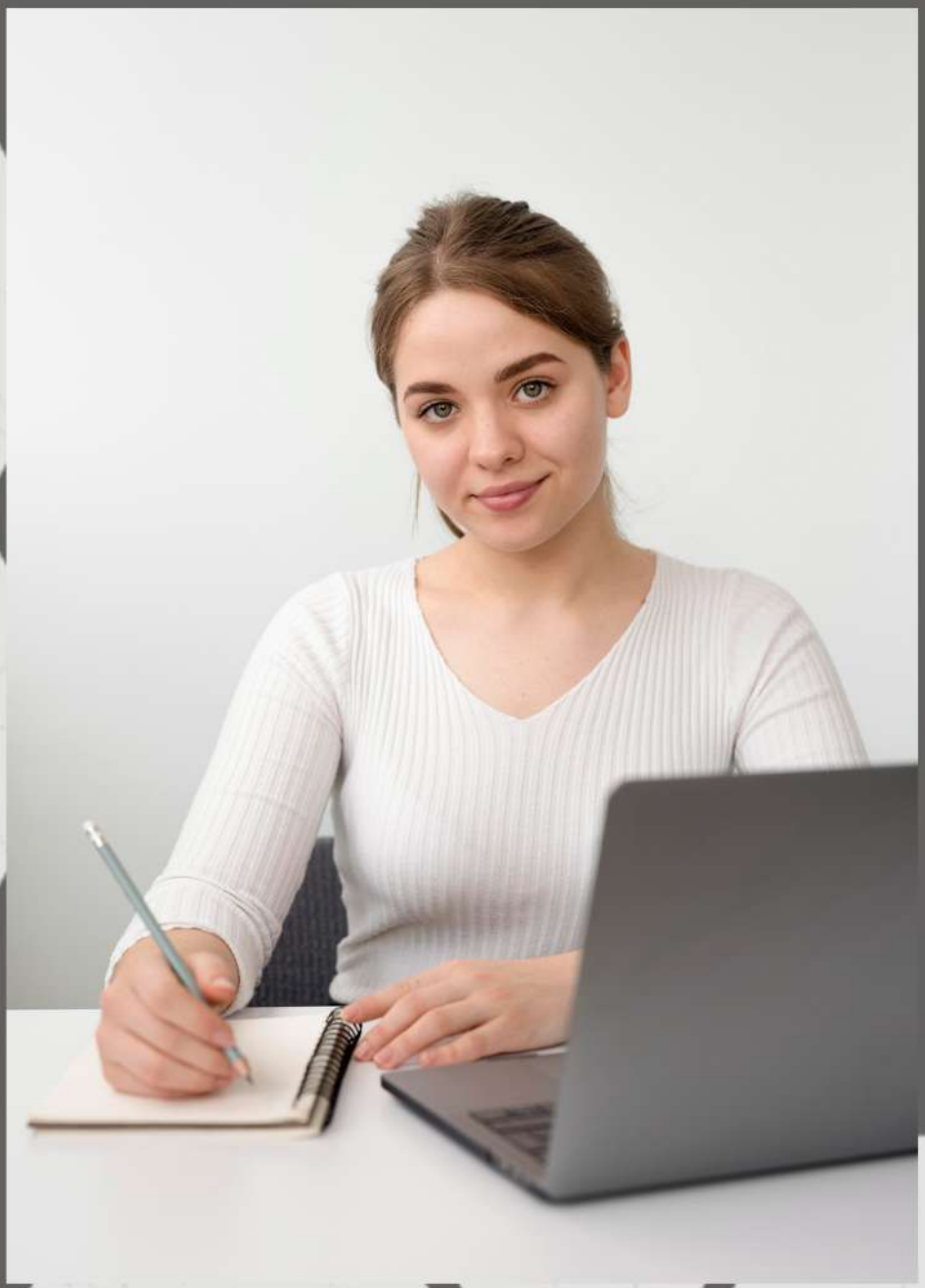
Palo Alto Network Certified Security Automation Engineer

Zetlan Technologies



Online Course

ZETLAN TECHNOLOGIES
www.zetlantech.com

Course Modules

1.Playbook Development

- Ref & 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
  - Sub playbook
- Apply filters and transformers to manipulate data
- Apply the playbook debugger to aid in developing playbooks

2.Incident Objects

- Configure incident types
- Identify the role of an incident type within the incident lifecycle
- Configure an incident layout
  - Fields and buttons
  - New/Edit and Close Forms
  - Summarize the functn, capabilities, & purpose of incident fields
- Configure classifiers and mappers

3.Automations, Integrations, and Related Concepts

- Define the capabilities of automation across XSOAR functions
  - Playbook tasks
  - War room
  - Layouts (dynamic sections, buttons)
  - 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
- Configure and manage integration instances

Palo Alto Network Certified Security Automation Engineer

4.Content Management and Solution Architecture

- 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) Config
- Describe the components of the XSOAR system architecture
  - System hardware requirements
  - Remote repositories (dev-prod)
  - Engines
  - Multitenancy
  - Elasticsearch/HA
  - Docker

Palo Alto Network Certified Security Automation Engineer

- 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 tshooting tools available to obtain more diagnostic
  - Log bundles
  - Integration testing
- Identify options available for performance tuning
  - Ignore output
  - Quiet mode
  - Monitor system health using the System Diagnostics page

5.UI Workflow, Dashboards, and Reports

- 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
  - 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,
- Summarize the capabilities of widget builder

Zetlan Technologies

LEARN REMOTELY!!

The efficiency of online learning in terms of time management, flexibility, and the ability to access resources anytime, anywhere can be compelling.

ZETLAN TECHNOLOGIES

www.zetlantech.com

For contact: +91 8680961847
+91 9600579474