DEMISTO ENGINEER: BUILDING THE NEXT-GENERATION SOC

The Demisto Engineer training course is a compilation of narrated videos and demonstrations that will help you:

- Create tasks and develop playbooks
- Describe incident context data
- Build incident layouts that match to the needs of your current practices and the needs of analysts to triage and investigate incidents efficiently
- Identify how to categorize event information and map that information to various fields

Training Outline

1 - Creating Tasks and Developing Playbooks
2 - Introduction to the Incident Context Data
3 - Layout Builder in Demisto
4 - Introduction to Classification and Mapping
5 - Introduction to Lists and Whitelists

Scope

- Level: Intermediate
- Duration: 1 hour 40 minutes
- Format: Self-paced digital learning

Objectives

This training is designed to enable a SOC or SOAR engineer to start working with Demisto integrations, playbooks, incident page/type layouts, and other system features to facilitate resource orchestration, process automation, case management, and analyst workflow.

Target Audience

Palo Alto Networks Employees, Partners, and Customers

Prerequisites

There are no prerequisites, but familiarity with security operations and incident response teams would be helpful.

Palo Alto Networks Education

Training from Palo Alto Networks and Palo Alto Networks Authorized Training Partners delivers knowledge and expertise that prepare you to protect our digital way of life. Our trusted certifications validate your knowledge of the Palo Alto Networks Security Operating Platform and your ability to help prevent successful cyberattacks and safely enable applications.

This digital learning course is available at the Learning Center.