EDU-380
Cortex XSOAR: Automation and Orchestration

Overview

The Cortex™ XSOAR 6.2: Automation and Orchestration (EDU-380) course is four days of instructor-led training that will help you:

- Configure integrations, create tasks, and develop playbooks.
- Build incident layouts that enable analysts to triage and investigate incidents efficiently.
- Identify how to categorize event information and map that information to display fields.
- Develop automations, manage content, indicator data, and artifact stores, schedule jobs, organize users and user roles, oversee case management, and foster collaboration.

Course Objectives

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

The course includes coverage of a complete playbook-development process for automating a typical analyst workflow to address phishing incidents. This end-toend view of the development process provides a framework for more focused discussions of individual topics that are covered in the course.

Scope

- Level: Advanced
- Duration: 4 days
- Format: Instructor-led training
- Platform support: Cortex XSOAR server 6.8

Target Audience

Security-operations (SecOps), or security, orchestration, automation, and response (SOAR) engineers, managed security service providers (MSSPs), service delivery partners, system integrators, and professional services engineers.

Prerequisites

Participants must complete the Cortex XSOAR Analyst digital learning. Participants who have experience with scripting, the use of Python and JavaScript, and the use of JSON data objects will likely be able to apply what they learn more quickly than participants without such experience. However, completion of the course does not require proficiency in writing code.

Course Modules

- Core functionality and Feature Sets
- Enabling and Configuring Integrations
- Playbook Development
- Classification and Mapping
- Layout Builder
- Solution Architecture
- Docker
- Automation Development & Debugging
- The Marketplace and Content Management
- Indicators and Threat Intelligence Management
- Jobs and Job Scheduling
- Users and Role-Based Access Controls (RBAC)
- Integration Development