+33 (0)1 48 10 09 46
formation@ambient-it.net 140 Avenue Jean Lolive 93500 Pantin - France

Updated on 04/12/2024

Sign up

Cortex XSOAR training

3 days (21 hours)

Presentation

Cortex Xsoar is a SOAR (Security Orchestration, Automation and Response) platform developed by Palo Alto Networks, designed to centralize security incident management, automate repetitive tasks and orchestrate security tools. It helps security teams automate repetitive tasks, orchestrate incident response workflows and improve their overall threat management efficiency.

This course focuses on optimizing security operations by using XSOAR features to automate repetitive processes and improve incident management.

You'll learn to understand the basics of SOAR and XSOAR , as well as explore its key components such as incident types, integrations and instances. You'll learn how to develop automations and playbooks to respond effectively to incidents, and how to design automated workflows to improve productivity.

By the end of the course, you'll be able to create sophisticated automated workflows and integrations within XSOAR, dramatically improving your organization's response to security incidents and strengthening overall security management.

Our training will be based on the latest version of on-prem or on-premises technology.

Objectives

- Efficiently automate security incident management
- Mastering custom development with Cortex XSOAR
- Optimize security workflows with advanced automation

Target audience

- Safety automation engineers
- Safety engineer
- Systems integrator

Prerequisites

- Basic knowledge of Linux
- Familiarity with APIs and Webhooks
- How to write and understand Python scripts

OUR CORTEX XSOAR TRAINING PROGRAM

INTRODUCTION & XSOAR OVERVIEW

- What is Cortex XSOAR?
- Differences between different versions (on-prem, cloud)
- Why use it?
- Basic features
- Architectural overview
- User interface exploration and configuration

KEY CONCEPTS OF CORTEX XSOAR

- XSOAR security incident management and classification
- Integration configuration and instance management
- Using lists to store and manage information
- Integration of incident information sources
- Create automated playbooks and add relevant context

PLAYBOOK DEVELOPMENT

- Implementation of error handling in playbooks and use of metadata
- Application of filters to transform, manipulate and refine data
- Creating sub-playbooks
- Understanding different types of tasks on XSOAR
- Using loops in playbooks

AUTOMATION SCRIPT DEVELOPMENT

- Configuring and using the IDE (integrated development environment) to code and test scripts
- Using the Demisto class and common server functions
- Use Docker images to facilitate deployment and script execution
- Creating and deploying automation scripts in XSOAR

- Use the XSOAR API to integrate external applications

INTEGRATION DEVELOPMENT

- Analysis of the different integration categories in XSOAR and exploration of use cases
- Study of available commands, methods and functions
- Introduction to the XSOAR integration development process
- Advanced integration development techniques

PRE-TREATMENT AND POST-TREATMENT

- Creating and managing pre-processing rules in XSOAR
- Development of pre-processing scripts
- Use of post-processing scripts to refine, analyze or transform data after main processing

WORKFLOW CREATION AND AUTOMATION

- Presentation of tools and methods for automating use cases
- Understanding the link between use cases and automated workflows
- Analysis of the benefits of automation in business processes
- Steps for transforming a use case into an automated workflow
- Practical study: implementing an automated workflow using a concrete example

BONUS

- Additional resources: Links to relevant guides, white papers and tutorials
- Suggestions for further action (e.g. certifications, expert modules)

Companies concerned

This course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced computer technology, or to acquire specific business knowledge or modern methods.

Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as registration is finalized, the learner receives a self-assessment questionnaire which enables us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives for the training to come, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

Teaching methods

Practical course: 60% Practical, 40% Theory. Training material distributed in digital format to all participants.

Organization

The course alternates theoretical input from the trainer, supported by examples, with brainstorming sessions and group work.

Validation

At the end of the session, a multiple-choice questionnaire verifies the correct acquisition of skills.

Sanction

A certificate will be issued to each trainee who completes the course.