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

Updated on 24/01/2025

Sign up

SOAR splunk training

3 days (21 hours)

Presentation

Our Spluk SOAR training will teach you the skills you need to automate, manage and secure your IT environment. Our program covers all the tool's functionalities so that you can effectively analyze and deal with cyber attacks.

In this course, you'll first learn about the basic features of Splunk SOAR, such as configuration, playbook creation and performance optimization. Through a hands-on demonstration, you'll learn how to manipulate the interface and configure your alerts.

By the end of the course, you'll have mastered incident management, advanced use of Splunk SOAR for workflow management, as well as managing and securing sensitive data.

As with all our training courses, we will introduce you to the latest version of the software: Splunk SOAR 6.3.

Objectives

- Understanding Splunk SOAR's role in cybersecurity
- Advanced integration with Splunk
- Creating playbooks
- **playbook** management
- Analysis and visualization with Splunk SOAR
- Performance optimization

Target audience

- **Cybersecurity Analysts**
- SOC Analysts

- Safety engineer
- Network Administrator

Prerequisites

Basic knowledge of networks and systems.

Hardware requirements

Access to Splunk SOAR

Splunk SOAR training program

INTRODUCTION TO PLUNK SOAR

- Understanding splunk SOAR's role in cybersecurity
- Key concepts
  - orchestration
  - automation
  - answer
- Splunk SOAR architecture Data flows and components
- Technical prerequisites for efficient implementation
- Modern SOCs

Advanced integrations with Splunk SOAR

- Integrating Splunk SOAR with a SIEM
- Connecting third-party tools via Webhooks and APIs
- Integration with ticketing systems
- Synchronization with threat intelligence
- Automate flows with IDS/IPS network tools and firewalls

Creating and managing Playbooks

- Splunk SOAR playbook structure
  - conditional logic
  - loops
- Creating advanced playbooks with the visual builder
- Customizing actions with Python
- Playbook debugging and error handling
- Create complex workflows
- Version management and playbook sharing within an SOC

Incident Management

- Collection and centralization of incident data
- Categorizing and prioritizing alerts
- Team collaboration in Splunk SOAR
  - role management
  - access
- Automated response to critical incidents
- Create detailed incident reports
- IOC integration

Analysis and Visualization with Splunk SOAR

- Using dashboards to monitor safety KPIs
- Playbook performance analysis
- Automated reporting
- Using Splunk SOAR logs to diagnose problems
- Customize visualizations
- Measuring the efficiency of automated processes

Performance Optimization

- Techniques for reducing false positives in alerts
- Adjustments to speed up workflows
- Optimizing system resources
- Strategies for prioritizing critical threats
- Updating and maintenance of integrations and playbooks
- Enhanced scalability

Splunk SOAR security and compliance

- Best practices for securing Splunk SOAR
- User access and permissions management
- RGPD
- ISO 27001
- Audits of automated actions
- Protecting sensitive data in workflows
- Preparing systems for safety audits

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 on entry to training complies with Qualiopi quality criteria. As soon as enrolment is finalized, the learner receives a self-assessment questionnaire enabling us to

assess their estimated level of proficiency in different types of technology, and their 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) that 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, 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.