Updated 04/26/2024

Sign up

Alienvault OSSIM training

2 days (14 hours)

Presentation

Our Alienvault OSSIM training course will help you master unified security information and event management (SIEM) for your infrastructure.

OSSIM is a robust solution that integrates intrusion detection, vulnerability management, log monitoring and much more, providing a complete view of the security of your IT environment.

This course covers in detail the configuration, management and analysis of security logs, as well as the optimization of Alienvault OSSIM's advanced features.

You'll learn how to interpret the data generated by OSSIM to identify potential threats, configure customized alerts and implement effective corrective measures.

We also focus on understanding the Alienvault OSSIM architecture, user and role management, and best practices for system maintenance and upgrades.

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

Objectives

- Configuring and deploying Alienvault OSSIM
- Understanding OSSIM architecture
- Administering the OSSIM solution
- Analyze and respond to security events

Target audience

- Cybersecurity Analysts
- Cybersecurity managers
- Network administrators

Prerequisites

- Basic knowledge of IT security and risk management
- Familiarity with intrusion detection and vulnerability management concepts
- Experience in systems and network administration
- Understanding the fundamentals of relational databases
- Basic knowledge of Linux

ALIENVAULT OSSIM TRAINING PROGRAM

INTRODUCTION TO ALIENVAULT OSSIM

- Introducing AlienVault OSSIM and its capabilities
- Exploring the key components of the OSSIM system
- Benefits of using AlienVault OSSIM for security information and event management (SIEM)
- OSSIM architecture overview
- Distinction between AlienVault OSSIM and other SIEM solutions on the market

SOFTWARE REQUIREMENTS AND OSSIM INSTALLATION

- List of software required to install OSSIM
- Preparing the installation environment (compatible operating systems and tools)
- Detailed AlienVault OSSIM server installation process
- Checking installation and solving common problems
- Overview of installing Kali Linux as a penetration testing tool

OSSIM SERVER CONFIGURATION AND SENSOR INSTALLATION

- Navigation and initial configuration via the OSSIM web interface
- Installation and configuration of sensors for data collection
- Importance and role of sensors in the network
- Best practices for sensor deployment
- Setting up a web server to interact with OSSIM

EVENT MANAGEMENT AND LOG FORWARDING

- Understanding the role and configuration of Log Forwarding

- Configuring log transfer via Syslog
- Log formatting and management for efficient analysis
- Use integrated tools to view and analyze events
- Create correlation rules and notifications

ADVANCED CONFIGURATION AND INCIDENT MANAGEMENT

- Advanced server configuration via OSSIM web console
- Using directives and policies in OSSIM
- Incident response and alert management
- Customize dashboards and reports for optimal monitoring
- OSSIM integration with other cybersecurity tools

CONCLUSION AND NEXT STEPS

- Summary of skills and knowledge acquired during training
- Discussion of OSSIM best practices and operating strategies
- Identify opportunities for further training and post-training specialization
- Tips for implementing OSSIM in a production environment
- Resources and community for ongoing support and learning

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.