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

Updated on 30/01/2024

Sign up

GrayLog training: modern SIEM solution

3 days (21 hours)

Presentation

Our GrayLog training course will teach you how to centralize the capture, storage, real-time retrieval and analysis of machine logs from all components of your IT infrastructure. GrayLog is a powerful SIEM solution that will help you better understand the data sets within your organization.

Our training covers data exploration and analysis, as well as configuration and processing. You'll also learn about operational optimization, architecture and scalability. GrayLog maintenance tasks will also be covered.

You'll also discover advanced functions such as indexing failure management, user and role administration,

As with all our training courses, we will introduce you to the latest version of the software: GrayLog v5.2.3

Objectives

- Configuring GrayLog
- Familiarity with GrayLog architecture
- Deploy and administer the solution
- Data processing and analysis

Target audience

- **Cybersecurity analysts**
- Cybersecurity Officer
- Network administrator

Prerequisites

- Basic knowledge of networks and systems
- Experience with databases
- Knowledge of Java

Hardware requirements

- A database like Elasticsearch
- Java OpenJDK installed
- Have MongoDB installed

OUR GRAYLOG TRAINING PROGRAM

DISCOVER GRAYLOG AND CENTRALIZED LOG MANAGEMENT

- Overview and objectives of centralized log management
- Introduction to the user interface
- Key components
- Search interface
- Query syntax
- Creating and customizing dashboards

DATA MINING AND ANALYSIS

- Elements of research action
- Exploring logs
- How events and alerts work
- Creation of correlated events
- Alert notification configuration and management

CONFIGURATION AND DATA PROCESSING

- Introduction to streams concepts
- Pipelines and indices
- Setting pipeline rules
- Examples of message routing
- Use of inputs
- Data analysis and enrichment techniques (GeoIP, enterprise intelligence)

IMPROVED DATA PROCESSING

- Optimizing dashboards and interactive widgets
- Setting up advanced alerts
- proactive monitoring and conditions

- Greater flexibility in log processing

ARCHITECTURE AND SCALABILITY

- Architectural considerations
- How to install and configure Graylog
- Scaling strategies and building resilient environments
- Best practices for securing Graylog

GRAYLOG OPERATION AND MAINTENANCE

- Advanced search techniques for data analysis
- Handling indexing failures and resolving common problems
- User and role administration
- Plugin exploration and integration with Graylog Marketplace
- Answers to frequently asked questions and problem solving

Companies concerned

This training 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.