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

Updated on 16/02/2024

Sign up

Cloud SIEM Enterprise training

4 days (28 hours)

Presentation

With this Cloud SIEM (Security Information and Event Management) Enterprise training course, you'll be able to exploit basic functionalities such as data collection, storage, threat intelligence and ingestion.

Revolutionize your security with this SIEM solution. Improve visibility across your enterprise to deeply understand the context and scope of a cyber attack.

You can choose from hundreds of ready-to-use integrations and playbooks, or write your own. This tool lets you run playbooks automatically or manually when an insight is created or closed.

With multi-cloud protection, secure your hybrid cloud adoption and digital transformation efforts with cloud-native collection and detection on new threat surfaces.

As with all our training courses, this one will introduce you to the latest version of the platform (at the time of writing).

Objectives

- Audit and review of logs
- Real-time analysis of security alerts
- Identity and access management
- Understanding integration and playbooks
- Understanding how SIEM tools work

Target audience

- Cybersecurity Analyst
- Cybersecurity Auditor
- Pentester

Prerequisites

- Basic knowledge of the cloud environment
- Experience in corporate security

CLOUD SIEM ENTERPRISE TRAINING PROGRAM

INTRODUCTION TO CLOUD SIEM

- What is a SIEM and why is it essential in the cloud?
- Understand the role and importance of data ingestion in Cloud SIEM
- Configuring the Cloud SIEM environment for optimum performance
- Browse the Cloud SIEM main interface and discover its key features
- Create a checklist for Cloud SIEM administrators during integration

SIEM CLOUD ARCHITECTURE AND INFRASTRUCTURE

- Understanding the key components of Cloud SIEM
- The importance of elasticity and scalability
- Integration with other Cloud services and applications
- Safety and compliance
- Best practices for designing a robust Cloud SIEM architecture

MANAGEMENT OF RECORDS, SIGNALS, ENTITIES AND INSIGHTS

- Configure and customize insight generation parameters
- Using global intelligence to improve the quality of security insights
- Efficient entity management: visualization, criticality and customization
- Explore entity look-up tables and custom entity types
- Search and analyze records associated with signals and manage deletions

SENSORS

- Sensor download location
- Deploy and troubleshoot network and log sensors for efficient data collection
- Ingesting Zeek newspapers

- Using the parser editor for customization and troubleshooting

INTEGRATIONS

- ThreatQ Source
- Insight enrichment server
- Enable VirusTotal enrichment
- Flux TAXII
- Security incident response (SIR)
- Enhancements and threat indicators

MAILING LISTS AND AUTOMATION

- Create a concordance list
- Custom columns in the concordance list
- Correspondence field reference
- Entity tags and standard mapping lists
- Deleted lists
- Automations in Cloud SIEM
- Examples of automation

INGESTION AND SCHEMATICS

- Record processing pipeline
- Log mapping
- Understanding and configuring log mappings for product integration
- Exploring the records processing pipeline and mappable attributes
- Viewing Log Mappers
- Configure ingestion mapping

THREAT DETECTION AND INVESTIGATION

- Monitor user activity with a dashboard
- Creating model variables
- Monitor the geolocation of console connections
- Monitor failed connection attempts
- Detecting brute force attacks
- CrowdStrike

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.