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

Updated on 29/11/2023

Sign up

SOC Analyst Training

2 days (14 hours)

Presentation

SOC (Security Operation Center) is a platform designed to monitor, prevent and detect cyber-attacks thanks to technological solutions and a set of approaches. The SOC Analyst is responsible for monitoring and protecting the organization's assets, including intellectual property, employee data, business systems and brand integrity. His or her objective is to implement the organization's overall cybersecurity strategy and act as a central point of collaboration in coordinated efforts to monitor, assess and defend against cyberattacks. Our SOC Analyst training will teach you the principles and advanced features needed to become an SOC Analyst. You'll learn how to manage and correlate logs, deploy SIEM, detect and respond to incidents. By the end of our training, you'll be able to implement best practices in threat monitoring and prevention.

Objectives

- Understanding the challenges of the SOC Analyst profession
- Interpret threats and system vulnerabilities
- Implementing preventive measures in a SOC
- Event management with SIEM (Security information Event Management)
- Detect intrusions and manage incidents
- Improve information system security

Target audience

- System administrators
- Pentesters
- Information Security Consultant
- Safety engineers

Prerequisites

Basic knowledge of cybersecurity

SOC Analyst training program

Introduction

- What is SOC?
- How does an SOC team work in an organization?
- What are the roles and responsibilities of a SOC Analyst?
- SOC governance models

SOC functionalities

- ITSM
- SOC newsletter system
- SIEM basics (Elastic and Splunk)
- Main survey data sources
- SIEM alerts
- IDS alerts, firewalls, network traffic logs, endpoints

How the SOC works

- Incident detection
- Incident management
- Different SOC functions
- Collecting data and logs

Vulnerability management

- Identify attacker vulnerabilities
- Vulnerability management steps
- Evolution of the vulnerability management cycle
- Modern vulnerability management systems (VMS)

SOC analysis

- Migration strategies
- Threat Hunting
- Sort alerts
- Analysis techniques

- Intrusion detection

Log management

- Analyze log files
- Centralized log supervision
- Log supervision issues

Forensic analysis

- Forensic analysis of the computer system
- Modern cybercrime techniques
- Computer forensics

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.