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

Mis à jour le 16/05/2025

S'inscrire

# Formation Analyste SOC

2 jours (14 heures)

## Présentation

SOC (Security Operations Center ou Centre des Opérations de Sécurité) est une plateforme destinée à surveiller, prévenir et détecter les cyberattaques grâce aux solutions technologiques et d'un ensemble de démarches. L'Analyste SOC est chargé de surveiller et de protéger les actifs de l'organisation, notamment la propriété intellectuelle, les données du personnel, les systèmes commerciaux et l'intégrité de la marque. Son objectif est de mettre en œuvre la stratégie globale de cybersécurité de l'organisation et agir en tant que point central de collaboration dans les efforts coordonné pour surveiller, évaluer et se défendre contre les cyberattaques. Notre formation Analyste SOC vous enseignera les principes et les fonctionnalités avancées pour devenir un Analyste SOC. Vous apprendrez comment gérer et corréler des logs, déployer SIEM, détecter et répondre aux incidents. À l'issue de notre formation, vous serez capables de mettre en œuvre des meilleures pratiques de la surveillance et de la prévention de menaces informatiques.

## Objectifs

- Comprendre les enjeux du métier de SOC Analyste
- Savoir interpréter des menaces et des vulnérabilités du système
- Mettre en œuvre les moyens de préventions dans un SOC
- Gérer des événements avec SIEM (Security information Event Management)
- Savoir détecter des intrusions et gérer des incidents
- Être capable d'améliorer la sécurité du système d'information

## Public visé

- Administrateurs système
- Pentesters
- Consultant en sécurité de l'information
- Ingénieurs de sécurité

## Pré-requis

Connaissance de base en cybersécurité

# Programme de notre formation Analyste SOC

## Introduction

- Qu'est-ce que SOC ?
- Comment une équipe SOC travaille-t-elle dans une organisation ?
- Quels sont les rôles et responsabilités d'un Analyste SOC ?
- Modèles de gouvernance du SOC

## Fonctionnalités de SOC

- ITSM
- Système de bulletterie SOC
- Bases du SIEM (Elastic et Splunk)
- Principales sources de données à l'origine des enquêtes
- Alertes SIEM
- Alertes IDS, pare-feux, journaux de trafic réseau, points d'extrémité

## Fonctionnement du SOC

- Détection des incidents
- Gestion des incidents
- Différentes fonctionnalités du SOC
- Collecter des données et des journaux

## Gestion des vulnérabilités

- Identifier des vulnérabilités des attaquants
- Étapes de gestion des vulnérabilités
- Évolution du cycle de gestion des vulnérabilités
- Les systèmes modernes de gestion des vulnérabilités (VMS)

## Analyse SOC

- Stratégies de migration
- Threat Hunting
- Trier les alertes
- Techniques d'analyse

- Détection d'intrusion

### Gestion des logs

- Analyser des fichiers logs
- Supervision centralisée des logs
- Problématiques de supervision des logs

### Analyse forensic

- Faire analyse forensic du système informatique
- Techniques modernes de cybercriminalité
- Informatique judiciaire

## Sociétés concernées

Cette formation s’adresse à la fois aux particuliers ainsi qu’aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

## Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d’auto-évaluation nous permettant d’apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d’anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

## Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

## Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

## Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l’acquisition correcte des compétences.

## Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.