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

Mis à jour le 23/01/2026

S'inscrire

Formation Analyste SOC

8 jours (56 heures)

Présentation

La cybersécurité est aujourd'hui au cœur des enjeux stratégiques des organisations, confrontées à une intensification des menaces et à une sophistication croissante des attaques. Le soc joue un rôle central dans la détection, l'analyse et la réponse aux incidents. Cette formation d'« Analyste SOC (Security Operations Center) » est conçue pour les professionnels qui souhaitent comprendre les mécanismes de la cybersécurité défensive, maîtriser les outils et méthodologies du SOC et développer les compétences nécessaires pour protéger efficacement les systèmes d'information.

Durant cette formation, vous apprendrez à maîtriser les fondamentaux de la cybersécurité défensive et à comprendre le rôle et les missions de l'analyste SOC au sein d'une organisation. Vous découvrirez l'écosystème des menaces, les techniques d'attaque (phishing, ransomware, APT, exfiltration de données) et les méthodologies de détection et de veille.

Vous serez formés à l'utilisation des outils clés du SOC (SIEM, SOAR, EDR, IDS/IPS, Threat Intelligence), à l'analyse et la corrélation d'événements de sécurité, ainsi qu'à l'investigation sur postes et réseaux. Vous apprendrez également à gérer des incidents selon les standards internationaux (NIST, ISO 27035), de la détection à la remédiation, et à produire des rapports techniques exploitables pour les RSSI, les équipes IT et les directions.

Enfin, vous consoliderez vos compétences à travers des études de cas et des ateliers pratiques : triage d'alertes dans un SIEM, analyse de trafic malveillant, investigation forensic, gestion de crise face à un ransomware et simulation d'une première journée en SOC.

À l'issue de cette formation, vous serez capables de détecter, analyser et répondre efficacement aux incidents de sécurité.

Comme toutes nos formations, celle-ci vous présentera **la dernière version stable** de la technologie et ses nouveautés.

Objectifs

- Connaître le rôle et les missions d’un analyste SOC
- Maîtriser les fondamentaux de la cybersécurité défensive
- Utiliser les outils et technologies du SOC
- Analyser et corréler les événements de sécurité
- Gérer les incidents de sécurité
- Rédiger des rapports techniques
- Travailler en coordination avec les autres équipes de cybersécurité
- Faire de la veille (cybermenaces, techniques d'attaques)

Public visé

- Techniciens et administrateurs Systèmes et Réseaux
- Responsables informatiques
- Consultants en sécurité
- Ingénieurs
- responsables techniques
- architectes réseaux
- chefs de projets

Pré-requis

- Avoir des connaissances en réseau.
- Avoir suivi le parcours introductif à la cybersécurité ou posséder des connaissances équivalentes.

PROGRAMME DE LA FORMATION ANALYSTE SOC

[Jour 1 - Matin]

Introduction à la cybersécurité défensive

- Objectifs pédagogiques et compétences visées
- Fondamentaux de la cybersécurité défensive : principes de protection, détection et réponse
- Panorama de la cybersécurité défensive
- Actifs, menaces et surfaces d’attaque (CIA, MITRE ATT&CK)
- Organisation des métiers cyber & rôle du SOC
- Atelier pratique : Cartographier les menaces d’un SI avec MITRE ATT&CK.

[Jour 1 - Après-midi]

Fondamentaux d’un analyste SOC

- Missions de l’analyste SOC (L1, L2, L3)
- Chaîne de valeur SOC : surveillance, détection, investigation, reporting

- Coordination avec les autres équipes (CERT, CSIRT, Blue Team, Red Team)
- Rôle de l’analyste SOC dans la chaîne de défense et la gestion du cycle de vie d’un incident
- Panorama des outils SOC (SIEM, SOAR, EDR, Threat Intel)
- Atelier pratique : Simulation de triage d’alertes dans un SIEM.

[Jour 2 - Matin]

Panorama des menaces cyber

- Typologie des attaques (phishing, ransomware, DDoS, APT)
- Exploitation des vulnérabilités (CVE, CVSS)
- Ingénierie sociale et attaques hybrides
- Atelier : Analyse d’un email suspect (phishing).

[Jour 2 - Après-midi]

Effectuer sa Veille cyber

- Introduction à la veille cyber (CERT-FR, OSINT, Threat Intel feeds)
- Intégrer la veille dans le quotidien d’un analyste SOC
- Notions de Threat Intelligence (IoC : hash, IP, domaine)
- Atelier pratique : Construire un mini-dashboard de veille cyber.

[Jour 3 - Matin]

SIEM

- Architecture et principes d’un SIEM (Splunk, ELK, QRadar)
- Sources de logs : systèmes, réseaux, applicatifs, cloud
- Parsing et normalisation des événements
- Atelier pratique : Collecte et visualisation de logs via ELK.

[Jour 3 - Après-midi]

Collecte de logs

- Corrélation de logs pour détecter des patterns simples
- Investigation basique dans un SIEM (authentifications suspectes, brute force)
- Analyser et corréler les événements de sécurité pour identifier des incidents potentiels
- Atelier pratique : Corrélation d’événements réseau et système dans un SIEM.

[Jour 4 - Matin]

Endpoint Detection & Response (EDR)

- Détection et réponse sur les postes de travail (EDR)
- Signatures vs détection comportementale
- Investigation d’un poste compromis
- Atelier pratique : Analyse d’un poste infecté via un EDR.

[Jour 4 - Après-midi]

Réseaux et surveillance en temps réel

- Capture et analyse de trafic réseau (Wireshark, Zeek)
- Signatures IDS/IPS (Snort, Suricata)
- Surveillance des flux Netflow
- Détection d’anomalies réseau et exfiltration de données
- Atelier pratique : Analyse d’un trafic malveillant avec Wireshark.

[Jour 5 - Matin]

Méthodologie d’investigation SOC

- Processus de détection ? analyse ? qualification
- Faux positifs, incidents confirmés
- Introduction au reporting technique (rédiger une qualification d’incident)
- Atelier pratique : Qualification d’une alerte brute en incident confirmé.

[Jour 5 - Après-midi]

Processus de gestion d’incident

- Gestion d’incident (NIST SP 800-61, ISO 27035 – simplifié)
- Étapes : préparation, confinement, éradication, retour d’expérience
- Gérer les incidents de sécurité tout au long de leur cycle de vie
- Communication interne et externe en cas d’incident
- Atelier pratique : Table-top exercise sur une attaque ransomware.

[Jour 6 - Matin]

Investigation et forensic

- Introduction au forensic : acquisition et conservation des preuves

- Journaux systèmes, disques, mémoire
- Présentation d’outils (Volatility, Autopsy, FTK Imager – démonstration)
- Atelier pratique : Extraction de preuves sur une machine compromise.

[Jour 6 - Après-midi]

Scripts et automatisation des tâches

- Bonnes pratiques de durcissement (systèmes & réseaux)
- Gestion des vulnérabilités (scanners, patch management)
- Sécurité applicative vue du SOC (OWASP Top 10 simplifié)
- Atelier pratique : Détection d’une injection SQL dans des logs applicatifs.

[Jour 7 - Matin]

Automatisation et orchestration SOC (SOAR)

- Automatisation SOC : SOAR (principes, playbooks simples)
- Scripts utiles (Python/PowerShell – niveau accessible)
- Atelier pratique : Script Python simple pour extraire des IoC de logs.

[Jour 7 - Après-midi]

Reporting & communication

- Reporting technique SOC (rapports post-incident, indicateurs MTTD/MTTR)
- Communication vers RSSI, DSI, COMEX
- Capitalisation et RETEX (knowledge base SOC)
- Rédiger des rapports techniques clairs et exploitables pour documenter les incidents de sécurité
- Atelier pratique : Rédaction d’un rapport d’incident + présentation synthétique au COMEX.

[Jour 8 - Matin]

Étude de cas fil rouge

- Étude de cas complète : compromission d’un SI
- Analyse initiale des logs et détection
- Investigation multi-sources (SIEM, EDR, réseau)
- Containment et remédiation
- Atelier pratique : Exercice pratique complet de bout-en-bout.

[Jour 8 - Après-midi]

Préparation à la prise de poste Analyste SOC

- Threat Hunting proactif (notions de base)
- Anticipation des menaces émergentes (IoT, supply chain, IA – vulgarisé)
- Préparation à la prise de poste Analyste SOC
- Éthique et aspects juridiques de la cybersurveillance
- Certifications et perspectives (CEH, CompTIA Security+, SOC Analyst)
- Atelier mise en situation : Simulation d’une première journée en SOC.

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.