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

Mis à jour le 02/09/2026

S'inscrire

Formation Certification Certified Security Operations Manager

Présentation

La formation Certification Certified Security Operations Manager prépare les professionnels expérimentés à piloter un SOC moderne, à structurer ses capacités de défense et à réussir la certification officielle Certified Security Operations Manager (CSOM).

Cette formation avancée vous permet d'aller au-delà du traitement des alertes pour maîtriser les enjeux stratégiques, opérationnels et humains d'un Security Operations Center. Vous apprendrez à aligner les activités de sécurité avec les objectifs métier, les risques et les exigences de conformité.

Vous étudierez la conception d'un modèle opérationnel SOC, l'organisation des équipes, le pilotage des outils de détection, la gestion des cas et l'industrialisation des processus de réponse aux incidents.

Le parcours couvre également le threat intelligence, la gestion des vulnérabilités, la chasse aux menaces, la réponse à incident, la forensique et l'amélioration continue des capacités défensives.

À l'issue de la formation, vous serez en mesure de préparer efficacement l'examen Certified Security Operations Manager (CSOM), d'appliquer une démarche de maturité SOC et de défendre des choix opérationnels dans des cas pratiques de certification.

Objectifs

- Concevoir et piloter un SOC aligné avec les risques et les priorités métier.
- Structurer les processus de détection, d'investigation et de réponse à incident.
- Évaluer la maturité des capacités SOC et définir une feuille de route d'amélioration.
- Mettre en place des métriques pertinentes pour le pilotage et la communication exécutive.

- Préparer les évaluations théoriques et pratiques de la certification Certified Security Operations Manager (CSOM).

Public visé

- Responsable SOC
- Analyste SOC senior
- Responsable cybersécurité
- Responsable réponse à incident
- Consultant cybersécurité

Pré-requis

- Expérience de deux ans ou plus dans les opérations de cybersécurité défensive.
- Maîtrise des processus de réponse à incident et d'investigation SOC.
- Connaissances opérationnelles des journaux de sécurité, des alertes et des cas d'usage SIEM.
- Compréhension des environnements Windows, Linux et réseau.

Pré-requis techniques

- Poste de travail avec processeur quatre coeurs, 16 Go de RAM et au moins 20 Go d'espace disque disponible.
- Système Windows 11, macOS 13 ou distribution Linux récente.
- Navigateur Google Chrome, Mozilla Firefox ou Microsoft Edge dans une version maintenue.
- Connexion Internet stable, sans filtrage bloquant les plateformes de laboratoire et les accès distants.
- Possibilité d'utiliser une machine virtuelle ou un environnement de laboratoire isolé.

Programme de notre formation Certified Security Operations Manager

[Jour 1 - Matin]

Fondations de la gouvernance SOC

- Positionnement stratégique d'un SOC dans la gouvernance de la cybersécurité.
- Alignement entre objectifs métier, risques, obligations réglementaires et services de sécurité.
- Analyse des modèles opérationnels internes, externalisés et hybrides.
- Définition d'une charte SOC, des responsabilités et des interfaces avec les parties prenantes.
- Atelier pratique : construire la charte et le catalogue de services d'un SOC pour une organisation multisite.

[Jour 1 - Après-midi]

Architecture et organisation des opérations

- Conception d'une architecture de collecte, de corrélation et d'enrichissement des événements.
- Rôles, niveaux de support, compétences et circuits d'escalade au sein des équipes SOC.
- Dimensionnement des capacités selon la couverture, les horaires, les volumes et le niveau de risque.
- Gouvernance des outils SIEM, SOAR, EDR et gestion des cas.
- Atelier pratique : définir l'organisation cible, la matrice RACI et le modèle de couverture d'un SOC 24/7.

[Jour 2 - Matin]

Threat modelling et priorisation défensive

- Identification des actifs critiques, des processus sensibles et des scénarios de menace.
- Application du threat modelling à la conception des capacités de surveillance.
- Priorisation des sources de logs selon la valeur de détection, le coût et les risques couverts.
- Traduction des menaces en exigences de détection et en cas d'usage opérationnels.
- Atelier pratique : produire un modèle de menace et une matrice de priorisation des journaux pour un service critique.

[Jour 2 - Après-midi]

Détection engineering et gestion des cas

- Cycle de vie des règles de détection, de la demande métier à la mise en production.
- Conception de détections fondées sur MITRE ATT&CK, les comportements et les indicateurs.
- Réduction des faux positifs, validation analytique et gestion des exceptions.
- Structuration des dossiers d'investigation, de la qualification à la clôture du cas.
- Atelier pratique : concevoir un cas d'usage de détection, ses critères de triage et son workflow de traitement.

[Jour 3 - Matin]

Réponse à incident et pilotage de crise

- Articulation entre procédures SOC, plan de réponse à incident et gestion de crise.
- Rôles décisionnels, critères d'escalade et coordination des équipes techniques et métier.
- Conception de playbooks adaptés aux scénarios d'incident prioritaires.
- Capitalisation post-incident, actions correctives et retour d'expérience opérationnel.
- Atelier pratique : piloter une réponse à un incident de compromission avec arbitrages, communications et plan d'actions.

[Jour 3 - Après-midi]

Capacités défensives spécialisées

- Organisation des activités de threat intelligence et intégration dans les opérations SOC.
- Pilotage de la gestion des vulnérabilités et articulation avec la détection et la remédiation.
- Contribution de la threat hunting, de la forensique et de l'analyse de malware.
- Choix des compétences, des outils et des livrables pour chaque capacité spécialisée.
- Atelier pratique : élaborer une feuille de route de développement des capacités pour un SOC en phase de maturité.

[Jour 4 - Matin]

Maturité et amélioration continue

- Principes des modèles de maturité SOC et critères d'évaluation des capacités.
- Évaluation des dimensions personnes, processus, technologies, données et gouvernance.
- Analyse des écarts entre l'état actuel, le niveau de maturité cible et les risques résiduels.
- Construction d'une feuille de route priorisée, chiffrée et défendable devant la direction.
- Atelier pratique : réaliser un diagnostic de maturité SOC et proposer un plan de transformation sur douze mois.

[Jour 4 - Après-midi]

Métriques et communication exécutive

- Sélection de KPI, KRI et métriques de performance adaptés aux opérations de sécurité.
- Mesure de la couverture de détection, des délais de réponse, de la qualité et de la charge analytique.
- Construction de tableaux de bord pour les équipes opérationnelles, la direction et les clients internes.
- Évaluation de la valeur, du coût et du retour sur investissement des capacités SOC.
- Atelier pratique : concevoir un tableau de bord de pilotage SOC et présenter les recommandations à un comité de direction.

[Jour 5 - Matin]

Préparation méthodique à la certification

- Cartographie des domaines de compétences évalués par Certified Security Operations Manager (CSOM).
- Révision des notions de gouvernance, de construction SOC, de capacités défensives et de maturité.
- Stratégies de lecture des scénarios, d'analyse des contraintes et de justification des décisions.
- Préparation à l'évaluation théorique et aux mises en situation pratiques de certification.

- Atelier pratique : résoudre un cas blanc de certification portant sur la création et la priorisation d'un programme SOC.

[Jour 5 - Après-midi]

Simulation de certification et plan d'action

- Étude de scénarios transverses mobilisant gouvernance, détection, réponse et métriques.
- Analyse des choix de conception, des compromis opérationnels et des risques de mise en oeuvre.
- Revue des erreurs fréquentes dans les questions théoriques et les livrables pratiques.
- Élaboration d'un plan individuel de révision et de passage de l'examen.
- Atelier pratique : réaliser une simulation finale de certification avec restitution argumentée d'un plan de maturation 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.