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

Mis à jour le 26/08/2026

S'inscrire

Formation Cortex XDR

3 jours (21 heures)

Présentation

Cortex XDR permet de centraliser la détection, l'investigation et la réponse face aux menaces avancées, en corrélant les signaux issus des endpoints, du réseau et du cloud. Cette formation vous aide à exploiter une plateforme de sécurité unifiée pour gagner en visibilité, réduire le bruit d'alerte et accélérer les décisions opérationnelles.

Notre formation Cortex XDR vous permettra d'aller au-delà des usages essentiels pour maîtriser les mécanismes clés rencontrés dans un contexte de supervision et de traitement d'incidents.

Vous apprendrez à comprendre l'architecture de la plateforme, à analyser les alertes, à mener des investigations efficaces et à structurer des actions de remédiation adaptées aux menaces détectées.

À l'issue de la formation, vous serez en mesure d'exploiter les fonctions de corrélation, de threat hunting, de triage et de réponse pour renforcer la posture de sécurité de votre organisation.

Cette formation aborde également les bonnes pratiques de déploiement, de paramétrage, de supervision et de fiabilisation des opérations afin de rendre vos analyses plus rapides et plus robustes en environnement réel.

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

Objectifs

- Comprendre les concepts fondamentaux de Cortex XDR et son positionnement dans une stratégie de détection et de réponse.
- Identifier les sources de télémétrie, les alertes et les signaux utiles pour l'analyse de sécurité.

- Explorer les incidents, reconstituer une chaîne d'attaque et qualifier la criticité d'un événement.
- Mettre en œuvre des actions de triage, d'investigation et de remédiation dans l'interface.
- Exploiter les fonctions de recherche et de corrélation pour accélérer le threat hunting.
- Appliquer les bonnes pratiques d'exploitation pour améliorer la réactivité du SOC et la qualité des décisions.

Public visé

- Analyste SOC
- Administrateur sécurité
- Ingénieur cybersécurité
- Responsable sécurité informatique
- Consultant sécurité

Pré-requis

- Maîtrise des bases de la cybersécurité et des principes de détection d'incidents.
- Connaissance des environnements Windows,Linux et des notions d'administration système.
- Compréhension des concepts réseau, des journaux d'événements et du fonctionnement d'un SOC.
- Pratique d'un outil de supervision, de gestion d'incidents ou d'analyse de logs.

Pré-requis techniques

- Ordinateur portable récent avec navigateur web à jour et espace disque suffisant pour les travaux pratiques.
- Connexion Wi-Fi ou Ethernet stable pour accéder aux environnements de démonstration.
- Accès à un poste avec droits suffisants pour utiliser les consoles et outils fournis pendant la session.
- Micro et casque recommandés pour les sessions à distance et les échanges pendant les ateliers.
- Si un environnement de laboratoire est fourni, disposer d'un compte fonctionnel et des accès nécessaires avant le démarrage.

Programme de notre formation Cortex XDR

[Jour 1 - Matin]

Fondamentaux et architecture

- Comprendre le positionnement de Cortex XDR dans une stratégie de détection et réponse.
- Identifier les sources de données, les capteurs et la logique de corrélation multi-sources.
- Découvrir l’architecture générale, les composants clés et les flux d’information.
- Appréhender les notions de télémétrie, d’alertes et d’incidents dans la plateforme.
- Relier les cas d’usage SOC aux capacités natives de la solution.

- Atelier pratique : prise en main de l’interface, repérage des zones utiles et lecture d’un premier incident.

[Jour 1 - Après-midi]

Déploiement et paramétrage

- Comprendre la logique de déploiement des agents et des intégrations.
- Configurer les éléments essentiels pour préparer un environnement exploitable.
- Découvrir les profils de sécurité, les politiques et les paramètres de base.
- Analyser l’impact des choix de configuration sur la visibilité et la protection.
- Appliquer les bonnes pratiques de structuration initiale d’un tenant.
- Atelier pratique : paramétrage d’une configuration de base et validation de la remontée de données.

[Jour 2 - Matin]

Analyse des alertes

- Lire une alerte et distinguer signal utile, faux positif et événement corrélé.
- Explorer les éléments de contexte disponibles pour qualifier un incident.
- Comprendre la notion de chaîne de causalité et de scénario d’attaque.
- Utiliser les vues de synthèse pour accélérer le triage.
- Structurer une méthode d’analyse reproductible pour le SOC.
- Atelier pratique : qualification d’alertes, regroupement des indices et rédaction d’un premier diagnostic.

[Jour 2 - Après-midi]

Investigation et threat hunting

- Approfondir l’investigation d’un incident à partir des données de la plateforme.
- Rechercher les artefacts utiles pour remonter à l’origine d’une compromission.
- Découvrir les principes de threat hunting appliqués à Cortex XDR.
- Exploiter les filtres, la navigation contextuelle et les pivots d’analyse.
- Consolider une démarche d’investigation orientée preuves et chronologie.
- Atelier pratique : reconstitution d’un scénario d’attaque et recherche d’indicateurs associés.

[Jour 3 - Matin]

Réponse et remédiation

- Comprendre les actions de réponse disponibles dans la console.
- Choisir les mesures adaptées selon la criticité et le niveau de confiance.
- Gérer l’isolement, la remédiation et les actions correctives de manière contrôlée.
- Documenter les décisions et préparer la traçabilité opérationnelle.
- Intégrer la réponse dans un processus de traitement d’incident plus large.
- Atelier pratique : mise en œuvre d’actions de containment et validation du retour à un état maîtrisé.

[Jour 3 - Après-midi]

Exploitation avancée et bonnes pratiques

- Consolider les usages avancés pour fiabiliser l’exploitation quotidienne.
- Revoir les méthodes d’optimisation du triage, de la supervision et du suivi.
- Identifier les indicateurs utiles pour piloter l’activité de détection.
- Appliquer les bonnes pratiques de gouvernance, de maintien en condition et d’amélioration continue.
- Préparer une montée en autonomie sur les cas d’usage les plus fréquents.
- Atelier pratique : étude de cas complète, de la détection initiale à la réponse finale.

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.