+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 XSIAM

2 jours (14 heures)

Présentation

Cortex XSIAM est une plateforme AI-driven de sécurité opérationnelle qui unifie XDR,SIEM,SOAR et automatisation pour transformer le SOC. Cette formation vous donne les clés pour exploiter une architecture pensée pour la détection, l'investigation et la réponse, avec des usages orientés production.

Notre formation Cortex XSIAM vous permettra d'aller au-delà des usages de base pour maîtriser les fonctions essentielles rencontrées dans un centre de sécurité moderne.

Vous apprendrez à comprendre l'architecture de la plateforme, à exploiter la collecte et la normalisation des données, à conduire des investigations plus rapides avec XQL et à structurer des workflows d'automatisation adaptés aux besoins du SOC.

À l'issue de la formation, vous serez en mesure d'analyser plus efficacement les alertes, de prioriser les incidents, de réduire le bruit opérationnel et de mieux industrialiser vos activités de détection et de réponse.

Cette formation aborde également les tableaux de bord, les indicateurs, la contextualisation des événements, les bonnes pratiques de pilotage et les réflexes nécessaires pour exploiter Cortex XSIAM dans un environnement réel.

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

Objectifs

- Comprendre le positionnement de Cortex XSIAM dans une stratégie SOC moderne.

- Maîtriser les principaux composants de la plateforme, la collecte de données et la logique de normalisation.
- Exploiter XQL pour rechercher, corréler et analyser les événements de sécurité.
- Structurer des investigations plus rapides et mieux priorisées à partir des alertes et des cas.
- Mettre en place des actions d'automatisation pour accélérer la réponse aux incidents.
- Utiliser les tableaux de bord et les contenus de pilotage pour suivre l'activité de sécurité.

Public visé

- Analyste SOC
- Ingénieur SOC
- Responsable sécurité opérationnelle
- Consultant cybersécurité
- Ingénieur détection et réponse

Pré-requis

- Connaissances de base en cybersécurité et en fonctionnement d'un SOC.
- Pratique des notions d'investigation d'alertes et d'analyse d'événements.
- Compréhension des principes de SIEM,XDR ou SOAR.
- Lecture aisée de logs, d'indicateurs et de données techniques de sécurité.
- Expérience préalable sur une plateforme de supervision ou de réponse à incidents.

Pré-requis techniques

- Un ordinateur portable récent avec navigateur web à jour et ressources suffisantes pour les exercices.
- Une connexion Wi-Fi ou Ethernet stable pour suivre les démonstrations et ateliers.
- Un accès à un environnement de laboratoire ou à un compte de démonstration Cortex XSIAM si fourni.
- Un casque et un micro pour les sessions à distance, si la formation est suivie en visioconférence.
- Un environnement de travail permettant l'ouverture de plusieurs onglets, consoles et tableaux de bord simultanément.

Programme de notre formation Cortex XSIAM

[Jour 1 - Matin]

Fondamentaux de la plateforme

- Positionnement de Cortex XSIAM dans l’écosystème SecOps.
- Architecture fonctionnelle, logique de plateforme unifiée et bénéfices opérationnels.
- Rôle de la donnée dans la détection, l’investigation et la réponse.
- Panorama des briques XDR, SIEM, SOAR et automatisation.
- Lecture des principaux objets, vues et espaces de travail.

- Atelier pratique : prendre en main l’interface, identifier les zones clés et repérer les objets de supervision.

[Jour 1 - Après-midi]

Collecte et exploitation des données

- Sources de données supportées et logique d’ingestion.
- Normalisation, enrichissement et contextualisation des événements.
- Gestion des alertes, signaux et cas dans le flux d’analyse.
- Principes de qualité de données pour améliorer la détection.
- Organisation des vues de suivi pour le travail quotidien du SOC.
- Atelier pratique : analyser un flux d’événements, retrouver les données utiles et qualifier une alerte.

[Jour 2 - Matin]

Investigation avec XQL

- Syntaxe de base de XQL et logique des requêtes.
- Filtrage, agrégation et tri des résultats d’analyse.
- Corrélation d’événements pour reconstituer une séquence d’attaque.
- Recherche d’indicateurs, d’anomalies et de comportements suspects.
- Méthodes pour accélérer le triage et réduire le bruit.
- Atelier pratique : écrire des requêtes XQL pour investiguer un scénario d’incident.

[Jour 2 - Après-midi]

Automatisation et pilotage SOC

- Logique des workflows d’automatisation et des actions guidées.
- Déclenchement de réponses selon le niveau de criticité.
- Tableaux de bord, indicateurs et suivi opérationnel.
- Bonnes pratiques de priorisation et de réduction du temps de traitement.
- Industrialisation des tâches répétitives dans le SOC.
- Atelier pratique : concevoir un scénario de réponse automatisée et le valider sur un cas d’usage.

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.