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

Mis à jour le 14/11/2025

S'inscrire

Formation SentinelOne

3 jours (21 heures)

Présentation

SentinelOne est une plateforme de cybersécurité moderne conçue pour protéger les postes de travail, serveurs et environnements cloud grâce à l'analyse comportementale et à la Storyline. Cette technologie unifiée d'EDR et de XDR permet de détecter, analyser et remédier automatiquement aux menaces tout en offrant une visibilité complète sur l'activité du système d'information.

Notre formation SentinelOne vous permettra de maîtriser le déploiement des agents, la configuration des politiques, l'investigation avancée, l'exploitation de la Threat Intelligence, ainsi que l'intégration SIEM/SOAR.

Vous apprendrez à automatiser vos workflows, optimiser votre posture de sécurité et superviser efficacement vos environnements.

À la suite de cette formation, vous serez en mesure d'administrer la plateforme, d'investiguer des incidents complexes, d'automatiser la réponse et de construire un runbook opérationnel.

Comme toutes nos formations, celle-ci vous présentera la dernière version stable de SentinelOne disponible.

Objectifs

- Comprendre l'architecture de SentinelOne.
- Déployer et configurer les agents.
- Analyser et investiguer les incidents.
- Exploiter la Threat Intelligence et les IOC.
- Superviser et automatiser la sécurité.

Public visé

- Administrateurs Systèmes
- Analystes SOC
- Ingénieurs Cybersécurité

Pré-requis

- Notions en cybersécurité
- Connaissance Windows / Linux

Formation SentinelOne

[Jour 1 - Matin]

Architecture et fondamentaux de SentinelOne

- Comprendre la plateforme SentinelOne Singularity : EDR, XDR, IA comportementale
- Fonctionnement du moteur comportemental et de la Storyline
- Structure de la solution : agents, console, groupes, politiques
- Composants clés : visibilité, détection, réponse autonome
- Bonnes pratiques de prise en main et organisation du tenant
- Atelier pratique : Exploration guidée de la console et première analyse d’activité.

[Jour 1 - Après-midi]

Déploiement et configuration des agents

- Méthodes de déploiement Windows / macOS / Linux
- Gestion des tokens d’enrôlement et modes de protection
- Création et paramétrage des politiques de sécurité
- Gestion des exclusions et règles contextuelles
- Contrôles intégrés : Device Control, firewall, réseau
- Atelier pratique : Déploiement d’agents + création d’une politique ciblée.

Premiers diagnostics et analyse des événements

- Types d’événements : alertes, incidents, comportements suspects
- Lecture des données enrichies via Deep Visibility
- Arborescence des processus et analyse du comportement
- Identification rapide des menaces et risques potentiels
- Utilisation des filtres et recherches avancées
- Atelier pratique : Diagnostic d’un événement suspect et analyse guidée.

[Jour 2 - Matin]

Investigation avancée

- Exploration complète de la Storyline
- Reconstitution de la chaîne d’attaque
- Corrélation des événements et indicateurs clés
- Analyse MITRE ATT&CK intégrée
- Détection des mouvements latéraux et compromissions avancées
- Atelier pratique : Investigation complète d’un incident complexe.

[Jour 2 - Après-midi]

Réponse à incident et remédiation

- Mécanismes de rollback automatisé
- Quarantaine, isolation réseau et suppression ciblée
- Gestion d’incidents à grande échelle
- Réponse manuelle vs réponse automatisée
- Stratégies de containment rapide
- Atelier pratique : Mise en œuvre d’une stratégie complète de remédiation.

Threat Intelligence et IOC

- Rôle de la Threat Intelligence dans SentinelOne
- Travail avec les IOC : hash, IP, domaine, URL
- Enrichissement automatique et réputation
- Listes d’indicateurs personnalisées
- Détection proactive par signaux comportementaux
- Atelier pratique : Ajout et exploitation d’IOC dans la plateforme.

[Jour 3 - Matin]

Supervision, alerting et reporting

- Construction de tableaux de bord personnalisés
- Analyse des tendances d’attaque et anomalies
- Création d’alertes ciblées
- Rapports automatisés pour équipes SOC / RSSI
- Indicateurs de performance et qualité de détection
- Atelier pratique : Création d’un dashboard opérationnel pour SOC.

[Jour 3 - Après-midi]

Intégration SIEM / SOAR et automatisation

- Connexion à un SIEM : Splunk, Elastic, Sentinel
- Scénarios SOAR : Cortex, Phantom, Shuffle
- Exploitation de l’API SentinelOne
- Webhooks, automatisations et enrichissements
- Construction d’un flux opérationnel SecOps automatisé
- Atelier pratique : Intégration SentinelOne / SIEM + alerting automatisé.

Maintenance, gouvernance et durcissement

- Gestion du cycle de vie des agents
- Stratégies de durcissement de la configuration
- Gestion des logs, stockage et conformité
- Gouvernance : rôles, permissions, audits
- Checklist de mise en production et bonnes pratiques
- Atelier pratique : Création d’un runbook d’exploitation SentinelOne.

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.