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

Mis à jour le 17/08/2026

S'inscrire

Formation Wazuh Security Engineer

3 jours (21 heures)

Présentation

Wazuh est une plateforme SIEM et XDR open source permettant de centraliser la détection, la supervision et la réponse aux menaces. Avec le Wazuh manager, les agents, le dashboard et l'indexer, Wazuh offre une chaîne complète pour analyser les événements, renforcer la visibilité et industrialiser les opérations de sécurité.

Notre formation Wazuh Security Engineer vous permettra d'aller au-delà de l'installation pour maîtriser les sujets essentiels d'une plateforme Wazuh exploitable en environnement de production.

Vous apprendrez à structurer une architecture Wazuh, à déployer et administrer les agents, à exploiter les alertes, les logs et les tableaux de bord, puis à piloter la collecte et l'analyse des données de sécurité.

La formation couvre également la création de règles, de décodeurs et de cas d'usage de détection, ainsi que la gestion du caching fonctionnel de la plateforme, la supervision, le contrôle des accès et les bonnes pratiques d'exploitation.

À l'issue de la formation, vous serez en mesure de configurer une plateforme Wazuh robuste, d'améliorer la qualité de détection, de fiabiliser l'administration quotidienne et de préparer un socle production-ready pour vos équipes sécurité.

Cette formation aborde enfin les aspects de durcissement, d'observabilité, de maintenance et de mise en œuvre opérationnelle afin de sécuriser durablement vos environnements.

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

Objectifs

- Comprendre l'architecture Wazuh et le rôle de chaque composant.
- Déployer et administrer les agents, le manager, le dashboard et l'indexer.
- Configurer la collecte de logs, la corrélation et la visibilité opérationnelle.
- Créer et ajuster des règles et des décodeurs pour améliorer la détection.
- Exploiter les tableaux de bord, les alertes et les indicateurs pour piloter la sécurité.
- Appliquer les bonnes pratiques de supervision, de sécurité et de maintien en conditions opérationnelles.

Public visé

- Analyste SOC
- Ingénieur cybersécurité
- Administrateur sécurité
- Ingénieur systèmes et réseaux
- Consultant sécurité

Pré-requis

- Connaissances de base en cybersécurité et en supervision technique.
- Maîtrise des fondamentaux Linux et de l'administration système.
- Notions d'exploitation de logs et d'analyse d'événements.
- Compréhension générale des environnements réseau et des services exposés.
- Pratique d'un outil d'administration ou de supervision de type SIEM ou XDR appréciée.

Pré-requis techniques

- Un ordinateur récent avec au moins 16 Go de mémoire vive et un processeur multicœur.
- Une connexion Wi-Fi ou Ethernet stable pour les manipulations en ligne.
- Un accès à un environnement Linux de laboratoire, local ou virtuel.
- Un navigateur web à jour pour utiliser le Wazuh dashboard.
- Un outil de virtualisation ou d'accès distant selon l'environnement fourni par le formateur.

Programme de notre formation Wazuh Security Engineer

[Jour 1 - Matin]

Fondamentaux de la plateforme

- Comprendre le positionnement de Wazuh dans une architecture de détection et de supervision.
- Identifier les rôles du manager, des agents, du dashboard et de l’indexer.
- Découvrir le flux de données entre collecte, analyse, indexation et visualisation.
- Lire les principaux objets de configuration et les notions de base du ossec.conf.
- Appréhender les usages opérationnels, du suivi des hôtes à la détection d’incidents.

- Atelier pratique : cartographier une architecture Wazuh cible et associer chaque composant à son rôle.

[Jour 1 - Après-midi]

Installation et mise en service

- Préparer un environnement de déploiement cohérent pour une première plateforme.
- Installer et valider les prérequis du Wazuh manager et du dashboard.
- Comprendre les dépendances de l'indexer et la logique de connexion entre services.
- Vérifier les certificats, les comptes d'administration et les services essentiels.
- Diagnostiquer les erreurs fréquentes de démarrage et les problèmes de connectivité.
- Atelier pratique : déployer une instance Wazuh de référence et contrôler l'accès à l'interface d'administration.

[Jour 2 - Matin]

Gestion des agents et collecte

- Enrôler un agent et suivre son cycle de vie dans la console.
- Configurer la remontée des logs, la surveillance de fichiers et les modules de collecte.
- Organiser les agents par groupes pour simplifier l'exploitation à grande échelle.
- Contrôler l'état de santé, la connectivité et les événements de supervision des endpoints.
- Adapter les paramètres de collecte selon les besoins métiers et techniques.
- Atelier pratique : enregistrer plusieurs agents, puis vérifier leur statut et leurs premières alertes.

[Jour 2 - Après-midi]

Détection et normalisation

- Comprendre le rôle des décodeurs dans la lecture des événements bruts.
- Construire et tester des règles de détection adaptées au contexte.
- Utiliser le moteur de test pour valider la correspondance entre logs, décodeurs et règles.
- Affiner les alertes avec des conditions, des niveaux de sévérité et des exceptions.
- Structurer une démarche de détection progressive, du cas simple au cas métier.
- Atelier pratique : créer un décodeur simple et une règle associée à partir d'un journal d'événements.

[Jour 3 - Matin]

Analyse, tableaux de bord et exploitation

- Explorer les tableaux de bord pour suivre les alertes, les tendances et les actifs exposés.

- Lire les indicateurs utiles à l’analyse opérationnelle et au triage.
- Exploiter les fonctions de recherche, de filtrage et de contextualisation des incidents.
- Comprendre la gestion des droits et les principes de contrôle d’accès.
- Mettre en place une routine de supervision pour les équipes sécurité.
- Atelier pratique : construire un tableau de bord orienté SOC pour suivre un scénario de menace.

[Jour 3 - Après-midi]

Industrialisation et bonnes pratiques

- Renforcer la sécurité de la plateforme par le durcissement des composants.
- Appliquer les bonnes pratiques de maintenance, de sauvegarde et d’exploitation.
- Préparer la montée en charge, la supervision et la continuité de service.
- Structurer les tâches récurrentes d’administration et de contrôle.
- Identifier les points de vigilance pour un passage en production maîtrisé.
- Atelier pratique : élaborer un plan d’exploitation Wazuh avec contrôles, maintenance et priorités de mise en production.

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.