+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 avancé

2 jours (14 heures)

Présentation

Wazuh est une plateforme XDR et SIEM open source permettant de centraliser la détection, la corrélation et la réponse aux menaces sur vos endpoints, serveurs et environnements hybrides. Avec les agents, les règles, les décodeurs, la vulnérabilité, la FIM et le SCA, Wazuh permet de bâtir une supervision sécurité robuste et industrialisée.

Notre formation Wazuh avancé vous permettra d'aller au-delà des fondamentaux pour maîtriser les sujets critiques rencontrés lors du déploiement et de l'exploitation d'une plateforme Wazuh en production.

Vous apprendrez à structurer une architecture Wazuh server,Wazuh indexer et Wazuh dashboard, à affiner les règles et les décodeurs, à exploiter la File Integrity Monitoring, la Security Configuration Assessment et la vulnerability detection.

À l'issue de la formation, vous serez en mesure d'optimiser la qualité des alertes, de réduire le bruit opérationnel, de mieux prioriser les incidents et de préparer une supervision sécurité prête pour la production.

Cette formation aborde également les active response, l'intégration avec le dashboard, l'administration des agents, les bonnes pratiques de durcissement et les éléments essentiels pour fiabiliser vos usages en environnement réel.

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.

- Configurer et administrer les agents et leur supervision centralisée.
- Exploiter les modules FIM,SCA et vulnerability detection.
- Créer et ajuster des règles et décodeurs pour améliorer la détection.
- Mettre en œuvre des active response et des tableaux de bord pertinents.
- Préparer une exploitation production-ready avec des bonnes pratiques de sécurité.

Public visé

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

Pré-requis

- Connaissances de base en Linux et en administration système.
- Pratique des concepts de sécurité informatique et de supervision.
- Notions sur les logs, les alertes et l'analyse d'événements.
- Expérience avec des outils de SIEM ou de collecte de journaux, souhaitée.
- Capacité à lire de la documentation technique en anglais.

Pré-requis techniques

- Un ordinateur récent avec au moins 16 Go de RAM recommandé pour les manipulations.
- Une connexion Wi-Fi ou Ethernet stable pour accéder aux environnements de test.
- Un navigateur moderne à jour, comme Google Chrome ou Mozilla Firefox.
- Un client SSH et un terminal disponibles sur votre poste de travail.
- Un environnement de virtualisation, comme VirtualBox ou VMware Workstation, si les ateliers sont réalisés en local.

Programme de notre formation Wazuh avancé

[Jour 1 - Matin]

Architecture et flux de données

- Rappel des composants clés de Wazuh et de leur rôle dans la chaîne de détection.
- Compréhension du flux entre agent, server, indexer et dashboard.
- Lecture des ports, services et échanges nécessaires au fonctionnement de la plateforme.
- Différences entre déploiement all-in-one, distribué et clusterisé.
- Gestion des premiers points de contrôle pour valider une architecture opérationnelle.
- Atelier pratique : cartographier une architecture Wazuh cible et identifier les flux à sécuriser.

[Jour 1 - Après-midi]

Agents, collecte et supervision

- Enrôlement et administration des agents Wazuh.
- Paramétrage de la collecte des journaux, événements système et données de sécurité.
- Suivi de l’état des agents, des versions et de la connectivité.
- Gestion des cas agentless pour certains équipements réseau.
- Bonnes pratiques pour structurer la supervision par parc, rôle ou environnement.
- Atelier pratique : enregistrer un agent, vérifier sa remontée et contrôler les données collectées.

[Jour 2 - Matin]

Détection avancée et conformité

- Exploitation des modules FIM et SCA pour renforcer la posture de sécurité.
- Compréhension des mécanismes de vulnerability detection et d’enrichissement des alertes.
- Création et adaptation de règles et décodeurs pour réduire le bruit.
- Lecture des alertes et priorisation selon le contexte métier et technique.
- Approche méthodique pour relier les événements à des scénarios de menace concrets.
- Atelier pratique : ajuster une règle et une politique SCA pour produire une détection plus pertinente.

[Jour 2 - Après-midi]

Réponse, tableaux de bord et exploitation

- Construction de tableaux de bord utiles pour le suivi opérationnel et le pilotage SOC.
- Paramétrage des active response pour automatiser certaines actions de remédiation.
- Exploration des usages avancés du dashboard pour l’analyse et le diagnostic.
- Bonnes pratiques de sécurisation, de durcissement et de maintenance de la plateforme.
- Organisation de l’exploitation quotidienne, des contrôles et des points de vigilance en production.
- Atelier pratique : concevoir un scénario de réponse automatisée et le tester sur un cas simple.

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.