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

Mis à jour le 31/03/2025

S'inscrire

Formation Wazuh

4 jours (28 heures)

PRÉSENTATION

Notre formation Wazuh vous permettra de sécuriser vos infrastructures informatiques de manière efficace et de surveiller en temps réel les menaces potentielles. Contrairement à d'autres outils de sécurité, Wazuh offre une plateforme unifiée pour différents environnements tels que les centres de données, les infratructures cloud et les applications.

Dans cette formation, destinée aux ingénieurs et aux consultants en sécurité responsables de la mise en œuvre, de la configuration et de l'exploitation d'un système Wazuh HIDS/SIEM. Il couvre tous les principaux composants du Wazuh et comment en tirer le meilleur parti.

Vous obtiendrez une expérience directe avec de nombreuses fonctionnalités de Wazuh et apprendrez de nombreuses façons de réunir ces fonctionnalités en synergie à des fins avancées.

Ce cours se compose de conférences et d'exercices pratiques effectués pour comprendre le fonctionnement de la technologie. Ces exercices vous apprennent à effectuer des tâches de configuration et d'exploitation afin d'exercer les fonctionnalités mises au point tout au long de la formation.

Comme dans toutes nos formations, celle-ci vous présentera la dernière version stable de Wazuh (à la date de rédaction de l'article : Wazuh 4.11).

Objectifs

- Installer, configurer et gérer efficacement l’infrastructure Wazuh (Manager, Agents, Indexer, Dashboard).
- Personnaliser le ruleset en développant des décodages, des règles et des scénarios avancés adaptés à leur environnement spécifique.
- Automatiser la détection et la réponse aux incidents (via les scripts Active Response) et assurer la conformité aux politiques de sécurité.
- Surveiller l’intégrité des systèmes (FIM) et détecter les vulnérabilités ainsi que les rootkits.

- Mettre en œuvre des intégrations avancées avec des solutions tierces (Docker, AWS, Osquery, Sysmon, MITRE ATT&CK).
- Administrer un environnement Wazuh en cluster afin d'assurer la haute disponibilité et la résilience.
- Expliquer en détail l'architecture et le fonctionnement complet de Wazuh.

Public visé

- Professionnels iT
- Administrateurs systèmes
- Administrateurs réseau
- Ingénieurs DevOps
- Architectes de solution Cloud

Pré-requis

- Avoir de l'expérience sur les concepts de base de la sécurité informatique
- Connaissance de base de la ligne de commande Linux
- Tester Mes Connaissances

Pré-requis techniques

- Un PC capable de faire tourner des conteneurs Docker (minimum 8 Go de RAM requis) pour les labs

Programme de notre formation Wazuh

DÉCOUVERTE & INSTALLATION

- Introduction à Wazuh et cas d'usage
- Architecture et communication sécurisée
- Installation d'un cluster Wazuh (Manager, Indexer, Dashboard)
- Méthodes de déploiement et d'enregistrement des agents
- Tableau de bord Wazuh : découverte des fonctionnalités
- Mise à niveau push de l'agent
- Configuration de base de Wazuh
- Atelier 1 : Déploiement d'un environnement complet
- Atelier 2 : Enregistrement et supervision d'agents

ANALYSE & DÉTECTION

- Analyse des journaux de sécurité
- Fonctionnement du Wazuh Indexer et du Dashboard
- Ensemble de règles Wazuh
- Décodeurs, règles et Listes CDB

- Pipeline Wazuh : compréhension et optimisation
- Atelier 3 : Création de règles personnalisées
- Atelier 4 : Analyse d’alertes et filtrage avancé

SURVEILLANCE & RÉACTION

- Surveillance de l’intégrité des fichiers
- Collecte de l’inventaire des agents
- Détection des vulnérabilités
- Détection des rootkits
- Réponse active et remédiation
- Évaluation de la configuration de sécurité (CIS, PCI, GDPR…)
- Atelier 5 : Simulation d’une attaque et détection
- Atelier 6 : Mise en place d’une réponse active

INTÉGRATION & CAS CONCRETS

- Techniques MITRE ATT&CK appliquées à Wazuh
- Intégration d’Osquery pour l’inventaire avancé
- Intégration de Sysmon pour Windows Events
- Présentation de l’intégration Amazon CloudTrail
- Automatisation du traitement des alertes
- Visite du cluster Wazuh Manager & bonnes pratiques
- Optimisation et dépannage
- Atelier 7 : Intégration d’un outil externe (Osquery ou Sysmon)
- Atelier 8 : Cas concret de détection d’incident & remédiation

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.