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

Mis à jour le 24/06/2025

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

- Expliquer en détail l’architecture et le fonctionnement complet de Wazuh
- Installer, configurer et administrer une infrastructure Wazuh
- Personnaliser le ruleset (décodeurs, règles, scénarios personnalisés)
- Surveiller l’intégrité des systèmes et détecter les vulnérabilités
- Automatiser la détection et la réponse aux incidents (Active Response)
- Implémenter des intégrations avancées
- Administrer un environnement Wazuh en mode cluster HA

# 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 16 Go de RAM requis) pour les labs

# Programme de notre formation Wazuh

## Jour 1 : Introduction, Architecture, Déploiement et Configuration

### Introduction à Wazuh

- Introduction à Wazuh
- Architecture et communication sécurisée
- Déploiement et enregistrement des agents
- Découverte du Wazuh Dashboard
- Configuration de Wazuh

### Architecture et communication sécurisée

- Architecture client-serveur de Wazuh
- Communication entre les composants
- Sécurisation des échanges

### Déploiement et enregistrement des agents

- Options de déploiement du serveur Wazuh
- Prérequis d’installation

- Méthodes d’enregistrement des agents
- Mise à niveau des agents
- TP/Lab 1 : Déploiement et enregistrement d’un agent

### Découverte du Wazuh Dashboard

- Connexion au Wazuh Dashboard
- Présentation de l’interface
- Exploration des sections clés
- TP/Lab 2 : Exploration du Wazuh Dashboard

### Configuration de Wazuh

- Fichiers de configuration principaux
- Configuration centralisée d’un agent
- Options de configuration de base
- TP/Lab 3 : Configuration centralisée d’un agent

## Jour 2 : Analyse de logs, règles et décodeurs

### Analyse de logs

- Moteur d’analyse de logs de Wazuh
- Flux des logs dans le pipeline Wazuh
- Phases d’analyse
- Localisation des logs et des alertes
- Surveillance des périphériques réseau via Syslog
- Support de la conformité réglementaire
- TP/Lab 4 : Analyse des logs et suivi des règles

### Wazuh Indexer et Dashboard

- Intégration avec l’indexer OpenSearch
- Utilisation du Wazuh Dashboard comme console de gestion des alertes
- Pipeline événement/alerte détaillé

### Wazuh Ruleset

- Structure du Wazuh Ruleset
- Couverture applicative diverse
- Mise à jour du Ruleset
- Contribution au Ruleset (brève mention si pertinent pour l’audience)
- Exploration approfondie de la hiérarchie des règles

### Décodeurs et règles

- Définition des règles, décodeurs et pré-décodeurs
- Types de règles
- Décodeurs en détail
- Création de règles et décodeurs personnalisés
- Bonnes pratiques pour adapter le Ruleset
- Test des décodeurs et des règles personnalisés
- Décodage dynamique des logs JSON entrants
- TP/Lab 5 : Création d’un décodeur et d’une règle personnalisés

### Listes CDB

- Fonctionnement des listes CDB
- Cas d’utilisation des listes CDB
- Format des fichiers et chemins
- Création de règles utilisant les listes CDB
- TP/Lab 6 : Utilisation des listes CDB

## Jour 3 : Surveillance, détection et réponse

### Surveillance de l’intégrité des fichiers (FIM)

- Fonctionnement du module FIM (Syscheck)
- Options de configuration de Syscheck
- Exclusions FIM
- Alertes FIM
- Cas d’utilisation du FIM
- TP/Lab 7 : Configuration et analyse des résultats du FIM

### Collecte d’inventaire & détection de vulnérabilités

- Collecte d’inventaire (Syscollector)
- Module de détection de vulnérabilités
- Configuration du détecteur de vulnérabilités
- Visualisation des vulnérabilités
- Utilisation de l’inventaire via l’API Wazuh (brève mention)
- TP/Lab 8 : Détection de vulnérabilités

### Détection de rootkits

- Fonctionnement du module Rootcheck
- Méthodes de détection
- Alertes Rootcheck
- TP/Lab 9 : Simulation de rootkit

### Système d’intégration Wazuh

- Présentation du système d’intégration
- Configuration des intégrations
- Exemples d’intégrations fournies par Wazuh

### Réponse active

- Concept de réponse active
- Scripts de réponse active par défaut
- Types de commandes
- Configuration de la réponse active
- Exemples de réponse active
- TP/Lab 10 : Configuration d’une réponse active automatique

### Évaluation de la configuration de sécurité (SCA)

- Fonctionnement du module SCA
- Politiques SCA
- Gestion centralisée des politiques SCA
- Types de vérifications SCA
- Résultats des évaluations SCA
- TP/Lab 11 : Exécution d’une politique SCA

## Jour 4 : Threat Intelligence, intégrations avancées et administration HA

### Techniques MITRE ATT&CK

- Introduction au framework MITRE ATT&CK
- Mapping des alertes Wazuh avec MITRE ATT&CK
- Navigation dans le module MITRE ATT&CK du Dashboard
- Utilisation d’ATT&CK Navigator
- TP/Lab 12 : Exploration du mapping MITRE ATT&CK dans Wazuh

### Intégrations avancées

- Intégration Docker, Trivy et SCA
- Intégration Osquery
- TP/Lab 13 : Exécuter une requête Osquery via Wazuh et analyser les résultats dans le Dashboard
- Intégration Sysmon (Windows)
- TP/Lab 14 : Simuler un événement Sysmon
- Intégration Azure
- Intégration Office 365
- Intégration avec des plateformes de TI (VirusTotal, MISP)
- TP/Lab 15 : Test EICAR et intégration VirusTotal
- Intégration ClamAV et YARA Rules

### Gestion du cluster HA

- Déploiement d’un Wazuh en cluster HA (multi-VMs en utilisant Docker sur les nœuds)
- Rotation des certificats
- Ajout de nouveaux nœuds
- Upgrades en cluster HA (versions Docker et source installée)
- Snapshots

Conclusion & prochaines étapes

## 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.


Organisme de formation enregistré sous le numéro 11 75 54743 75. Cet enregistrement ne vaut pas agrément de l’État.
© Ambient IT 2015-2025. Tous droits réservés. Paris, France - Suisse - Belgique - Luxembourg