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

Durée de la Formation :3 jours (21heures)

Prix de la Formation :2850 euros TTC

PROGRAMME 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