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

Mis à jour le 26/04/2024

S'inscrire

Formation Alienvault OSSIM

2 jours (14 heures)

Présentation

Notre formation Alienvault OSSIM vous permettra de maîtriser la gestion unifiée des informations et des événements de sécurité (SIEM) pour votre infrastructure.

OSSIM est une solution robuste qui intègre la détection d'intrusion, la gestion des vulnérabilités, la surveillance des journaux et bien plus encore, offrant ainsi une vision complète de la sécurité de votre environnement informatique.

Cette formation couvre en détail la configuration, la gestion et l'analyse des journaux de sécurité, ainsi que l'optimisation des fonctionnalités avancées d'Alienvault OSSIM.

Vous apprendrez à interpréter les données générées par OSSIM pour identifier les menaces potentielles, à configurer des alertes personnalisées et à mettre en place des mesures correctives efficaces.

Nous mettons également l'accent sur la compréhension de l'architecture d'Alienvault OSSIM, la gestion des utilisateurs et des rôles, ainsi que les bonnes pratiques de maintenance et de mise à jour du système.

Comme pour toutes nos formations, nous vous présenterons la dernière version du logiciel.

Objectifs

- Configurer et déployer Alienvault OSSIM
- Comprendre l'architecture d'OSSIM
- Administrer la solution OSSIM
- Analyser et répondre aux événements de sécurité

Public visé

- Analystes en cybersécurité
- Responsables de la cybersécurité
- Administrateurs réseau

Pré-requis

- Connaissances de base en sécurité informatique et en gestion des risques
- Familiarité avec les concepts de détection d'intrusion et de gestion des vulnérabilités
- Expérience dans l'administration de systèmes et de réseaux
- Compréhension des principes fondamentaux des bases de données relationnelles
- Connaissance de base de Linux

PROGRAMME DE NOTRE FORMATION ALIENVAULT OSSIM

INTRODUCTION À ALIENVAULT OSSIM

- Présentation d'AlienVault OSSIM et de ses capacités
- Exploration des composants clés du système OSSIM
- Avantages d'utiliser AlienVault OSSIM pour la gestion des informations et événements de sécurité (SIEM)
- Vue d'ensemble de l'architecture OSSIM
- Distinction entre AlienVault OSSIM et d'autres solutions SIEM sur le marché

PRÉREQUIS LOGICIELS ET INSTALLATION D'OSSIM

- Énumération des logiciels nécessaires pour l'installation d'OSSIM
- Préparation de l'environnement d'installation (systèmes d'exploitation et outils compatibles)
- Processus détaillé d'installation d'un serveur AlienVault OSSIM
- Vérification de l'installation et résolution des problèmes courants
- Aperçu de l'installation de Kali Linux en tant qu'outil de test de pénétration

CONFIGURATION DU SERVEUR OSSIM ET INSTALLATION DES CAPTEURS

- Navigation et configuration initiale via l'interface web d'OSSIM
- Installation et configuration de capteurs pour la collecte de données
- Importance et rôle des capteurs dans le réseau
- Meilleures pratiques pour le déploiement des capteurs
- Configuration d'un serveur web pour interagir avec OSSIM

GESTION DES ÉVÉNEMENTS ET LOG FORWARDING

- Comprendre le rôle et la configuration du transfert de logs (Log Forwarding)

- Configuration du transfert de logs via Syslog
- Formatage et gestion des logs pour une analyse efficace
- Utilisation des outils intégrés pour visualiser et analyser les événements
- Création de règles de corrélation et de notifications

CONFIGURATION AVANCÉE ET GESTION DES INCIDENTS

- Configuration avancée du serveur via la console web d'OSSIM
- Utilisation des directives et des politiques dans OSSIM
- Réponse aux incidents et gestion des alertes
- Personnalisation des tableaux de bord et des rapports pour un suivi optimal
- Intégration d'OSSIM avec d'autres outils de cybersécurité

CONCLUSION ET ÉTAPES SUIVANTES

- Récapitulatif des compétences et connaissances acquises durant la formation
- Discussion sur les meilleures pratiques et les stratégies d'exploitation d'OSSIM
- Identifier les opportunités d'approfondissement et de spécialisation post-formation
- Conseils pour la mise en œuvre d'OSSIM dans un environnement de production
- Ressources et communauté pour le support continu et l'apprentissage

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.