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

Mis à jour le 30/01/2024

S'inscrire

Formation GrayLog : solution SIEM moderne

3 jours (21 heures)

Présentation

Notre formation GrayLog vous apprendra à centraliser la capture, le stockage, la recherche en temps réel ainsi que l'analyse des logs de machines de toutes les composantes de votre infrastructure informatique. GrayLog est une solution SIEM performante qui vous permettra de mieux comprendre les ensembles de données au sein de votre organisation.

Notre formation couvre l'exploration et l'analyse des données ainsi que leur configuration et leur traitement. Vous apprendrez également l'optimisation de l'exploitation, l'architecture et la scalabilité. Les tâches de maintenance de GrayLog seront également abordées.

Vous découvrirez également les fonctions avancées telles que la gestion des échecs d'indexation, l'administration des utilisateurs et des rôles,

Comme pour toutes nos formations, nous vous présenterons la dernière version du logiciel : GrayLog v5.2.3

Objectifs

- Configurer GrayLog
- Être familier de l'architecture GrayLog
- Pouvoir déployer et administrer la solution
- Traiter et analyser les données

Public visé

- **Analystes cybersécurité**
- Chargé de cybersécurité
- Administrateur réseaux

Pré-requis

- Connaissances de base des réseaux et des systèmes
- Expérience avec les bases de données
- Connaissance de Java

Pré-requis matériel

- Une base de donnée comme Elasticsearch
- Avoir Java OpenJDK installé
- Avoir MongoDB installé

PROGRAMME DE NOTRE FORMATION GRAYLOG

DÉCOUVERTE DE GRAYLOG ET GESTION CENTRALISÉE DES LOGS

- Présentation et objectifs de la gestion centralisée des logs
- Introduction à l'interface utilisateur
- Composants clés
- Interface de recherche
- Syntaxe des requêtes
- Création et personnalisation de tableaux de bord

EXPLORATION ET ANALYSE DES DONNÉES

- Éléments d'action de recherche
- Exploration des logs
- Fonctionnement des événements et des alertes
- Création d'événements corrélés
- Configuration et gestion des notifications d'alerte

CONFIGURATION ET TRAITEMENT DES DONNÉES

- Introduction aux concepts de streams
- Pipelines et indices
- Établissement de règles de pipelines
- Exemples de routage des messages
- Utilisation des entrées (inputs)
- Techniques d'analyse et d'enrichissement des données (GeoIP, renseignements d'entreprise)

AMÉLIORATION DE L'EXPLOITATION DES DONNÉES

- Optimisation des tableaux de bord et widgets interactifs
- Mise en place d'alertes avancées
- surveillance proactive et conditions

- Flexibilité accrue dans le traitement des logs

ARCHITECTURE ET SCALABILITÉ

- Considérations architecturales
- Méthodes d'installation et de configuration de Graylog
- Stratégies de mise à l'échelle et construction d'environnements résilients
- Bonnes pratiques pour la sécurisation de Graylog

EXPLOITATION ET MAINTENANCE DE GRAYLOG

- Techniques de recherche avancée pour l'analyse des données
- Gestion des échecs d'indexation et résolution des problèmes courants
- Administration des utilisateurs et des rôles
- Exploration des plugins et intégration avec Graylog Marketplace
- Réponses aux questions fréquemment posées et résolution de problèmes

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.