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

Mis à jour le 16/02/2024

S'inscrire

Formation Cloud SIEM Enterprise

4 jours (28 heures)

Présentation

Avec cette formation Cloud SIEM (Security Information and Event Management) Enterprise, vous serez capable d'exploiter les fonctionnalités de base comme la collecte de données, le stockage, la veille sur les menaces et l'ingestion.

Révolutionnez votre sécurité en utilisant cette solution SIEM. Améliorez votre visibilité à travers votre entreprise pour comprendre en profondeur le contexte et la portée d'une cyberattaque.

Vous pourrez choisir entre des centaines d'intégrations et de playbooks qui seront prêts à l'emploi ou d'écrire les vôtres. Cet outil vous permettra d'exécuter des playbooks automatiquement ou manuellement lorsqu'un insight est créé ou fermé.

Avec la protection multi-cloud, sécurisez vos efforts d'adoption du cloud hybride et de transformation numérique grâce à la collecte et la détection cloud natives sur les nouvelles surfaces de menaces.

Comme pour toutes nos formations, celle-ci vous présentera la toute dernière version de la plateforme (à la date de rédaction de l’article).

Objectifs

- Audit et examen des journaux
- Analyser en temps réel des alertes de sécurité
- Gestion des identités et des accès
- Compréhension de l'intégration et des playbooks
- Comprendre le fonctionnement des outils SIEM

Public visé

- Analyste Cybersécurité
- Auditeur Cybersécurité
- Pentester

Pré-requis

- Connaissance de base dans le milieu du Cloud
- Avoir de l'expérience dans la sécurité des entreprises

PROGRAMME DE NOTRE FORMATION CLOUD SIEM ENTERPRISE

INTRODUCTION AU CLOUD SIEM

- Qu'est-ce qu'un SIEM et pourquoi est-il essentiel dans le cloud ?
- Comprendre le rôle et l'importance de l'ingestion des données dans le Cloud SIEM
- Configurer l'environnement Cloud SIEM pour une performance optimale
- Parcourir l'interface principale du Cloud SIEM et découvrir ses fonctionnalités clés
- Établir une liste de vérification pour les administrateurs Cloud SIEM lors de l'intégration

ARCHITECTURE ET INFRASTRUCTURE CLOUD SIEM

- Comprendre les composants clés d'un Cloud SIEM
- L'importance de l'élasticité et de la scalabilité
- Intégration avec d'autres services et applications Cloud
- Sécurité et conformité
- Bonnes pratiques pour concevoir une architecture Cloud SIEM robuste

GESTION DES RECORDS, SIGNAUX, ENTITÉS ET INSIGHTS

- Configurer et personnaliser les paramètres de génération d'insights
- Utiliser l'intelligence globale pour améliorer la qualité des insights de sécurité
- Gérer efficacement les entités : visualisation, criticité et personnalisation
- Explorer les tables de recherche d'entités et les types d'entités personnalisés
- Rechercher et analyser les records associés aux signaux et gérer les suppressions

CAPTEURS

- Emplacement de téléchargement des capteurs
- Déployer et dépanner les capteurs réseau et de logs pour une collecte de données efficace
- Ingestion des journaux Zeek

- Utiliser l'éditeur de parser pour la personnalisation et le dépannage

INTÉGRATIONS

- ThreatQ Source
- Serveur d'enrichissement Insight
- Activer l'enrichissement VirusTotal
- Flux TAXII
- Réponse aux incidents de sécurité (SIR)
- Enrichissements et indicateurs de menace

LISTES DE CORRESPONDANCE ET AUTOMATISATION

- Créer une liste de concordance
- Colonnes personnalisées de la liste de concordance
- Référence des champs de correspondance
- Tags d'entités et listes de correspondances standard
- Listes supprimées
- Automatisations dans Cloud SIEM
- Exemples d'automatisation

INGESTION ET SCHÉMAS

- Pipeline de traitement des enregistrements
- Mappage du journal
- Comprendre et configurer les mappages de logs pour une intégration de produits
- Explorer le pipeline de traitement des records et les attributs mappables
- Visualisation des Log Mappers
- Configurer un mappage d'ingestion

DÉTECTION ET ENQUÊTE SUR LES MENACES

- Surveiller l'activité des utilisateurs avec un tableau de bord
- Créer des variables de modèle
- Surveiller la géolocalisation des connexions à la console
- Surveiller les tentatives de connexion ayant échoué
- Détecter les attaques par force brute
- CrowdStrike

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.