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

Mis à jour le 28/05/2024

S'inscrire

Formation Microsoft Sentinel

3 jours (21 heures)

Présentation

Découvrez notre formation exclusive sur Microsoft Sentinel, le système de gestion des informations et des évènements (SIEM) de Microsoft.

Notre formation complète sur Sentinel débutera par une présentation de ce logiciel SIEM populaire, nous vous enseignerons ses différents cas d'usage, ses avantages et ses limites. Par la suite, nous vous apprendrons à connecter vos données et vos logs pour une analyse proactive des menaces.

Grâce à notre formation Microsoft Sentinel, vous pourrez appliquer des techniques de "threat hunting" au sein de votre organisation. Ainsi, vous découvrirez le modèle ASIM, les extensions de l'outil ainsi que les dashboards sur mesure.

Notre formation Microsoft Sentinel vous enseignera par ailleurs le langage Kusto (KQL) pour créer des requêtes performantes, vous saurez également configurer des règles d'analytiques pour une détection proactive.

Objectifs

- Comprendre le rôle et les fonctionnalités de Microsoft Sentinel
- Gérer les incidents et le Threat Hunting efficacement
- Utiliser le langage de requête Kusto (KQL) pour l'analyse des données
- Créer des règles d'analyse et des rapports personnalisés

Public visé

- Analystes Cybersécurité
- Analystes SOC
- Chargé de cybersécurité
- Administrateur Système

- Administrateur Réseau

Pré-requis

Connaissances de base des réseaux et des systèmes.

Pré-requis

- Un accès à Microsoft Sentinel
- Optionnel : un accès à un outil SOAR pour mettre en place des réponses automatisées

PROGRAMME DE NOTRE FORMATION MICROSOFT SENTINEL

INTRODUCTION

- Microsoft Sentinel
  - Son rôle
  - Ses fonctionnalités
  - Pourquoi préférer Sentinel ?
- Les cas d'usage courants
- Explorer l'interface utilisateur
- Les avantages et les inconvénients de la solution

ARCHITECTURE ET DÉPLOIEMENT

- Comprendre l'architecture des espaces de travail et des locataires
- Les méthodes pour collecter les données
- Apprendre à enrichir ses données
- Transformation des logs
- Normalisation des logs
- Le modèle ASIM (Advanced SIEM Information Model)
- Configurer et gérer les connecteurs de données pour l'ingestion de logs
- Utiliser Microsoft 365 Defender
- Intégrer des données syslog/CEF
- Intégrer des solutions tiers

GESTION DES INCIDENTS ET THREAT HUNTING

- Mettre en application le threat hunting
  - Les incidents
  - Le triage
  - L'investigation
- Utiliser les playbooks pour automatiser les réponses aux incidents

KUSTO (KQL)

- Les bases du langage de requête Kusto
- Créer des requêtes avec KQL
- Utiliser KQL pour l'analyse des incidents
- Détection des menaces avec Kusto

LES RÈGLES D'ANALYSE

- Développer des règles d'analyse pour détecter les comportements anormaux
- Implémenter des réponses automatisées avec SOAR
- Analyser le comportement des utilisateurs et des entités avec UEBA (User and Entity Behavior Analytics)
- Surveiller l'intégrité et les performances de Microsoft Sentinel

REPORTING

- Gestion des workbooks
- Personnaliser les modèles de workbooks
- Créer des visualisations avancées et des rapports personnalisés
- Utiliser les tableaux de bord pour le suivi des incidents
- Création de classeurs
- Personnaliser ses classeurs pour la représentation des données
- Générer des rapports en temps réel
- Utiliser les notebooks

ANALYTICS

- Configurer des règles d'analytique pour une détection proactive
- Fusionner les règles
- Appliquer des règles de sécurité
- Créer des règles de requêtes planifiées et en temps réel (NRT)

APPLICATION DES CONNAISSANCES

- Des simulations pour appliquer les compétences acquises
- Configurer et gérer les rôles et permissions dans Microsoft Sentinel
- Études de cas concrets

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.