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

Mis à jour le 24/01/2025

S'inscrire

Formation splunk SOAR

3 jours (21 heures)

Présentation

Notre formation Spluk SOAR vous enseignera les compétences nécessaires pour automatiser, gérer et sécuriser votre environnement informatique. Notre programme couvre l'ensemble des fonctionnalités de l'outil afin que vous puissiez efficacement analyser et traiter les cyberattaques.

Dans ce cours, vous apprendrez tout d'abord les fonctionnalités premières de Splunk SOAR, telles que sa configuration, la création de playbooks et l'optimisation de performance. À travers une démonstration pratique, vous apprendrez à manipuler l'interface et à configurer vos alertes.

À la fin de la formation, vous maîtriserez la gestion des incidents, l'utilisation avancée de Splunk SOAR pour la gestion du Workflow, ainsi que la gestion et la sécurisation des données sensibles.

Comme pour toutes nos formations, nous vous présenterons la dernière version du logiciel : Splunk SOAR 6.3

Objectifs

- Comprendre le rôle de Splunk SOAR dans la cybersécurité
- Intégration avancée avec Splunk
- Création des playbooks
- gestion des **playbooks**
- Analyse et visualisation avec Splunk SOAR
- Optimisation des performances

Public visé

- **Analystes Cybersécurité**
- Analystes SOC

- Ingénieur en sécurité
- Administrateur Réseau

Pré-requis

Connaissances de base des réseaux et des systèmes.

Pré-requis matériel

Un accès à Splunk SOAR

Programme de la formation Splunk SOAR

INTRODUCTION À PLUNK SOAR

- Comprendre le rôle de splunk SOAR dans la cybersécurité
- Concepts clés
  - orchestration
  - automatisation
  - réponse
- Architecture de Splunk SOAR flux de données et composants
- Pré-requis techniques pour une implémentation efficace
- SOC modernes

Intégrations Avancées avec Splunk SOAR

- Intégration de Splunk SOAR avec un SIEM
- Connexion d'outils tiers via les Webhooks et les API
- Intégration avec des systèmes de ticketing
- Synchronisation avec des threats intelligence
- Automatisation des flux avec des outils réseau IDS/IPS et pare-feux

Création et Gestion des Playbooks

- Structure des playbooks dans Splunk SOAR
  - logiques conditionnelles
  - boucles
- Création de playbooks avancés avec le visual builder
- Personnalisation des actions avec Python
- Débogage des playbooks et gestion des erreurs
- Création de workflows complexes
- Gestion des versions et partage des playbooks au sein d’un SOC

Gestion des Incidents

- Collecte et centralisation des données d’incidents
- Catégorisation et priorisation des alertes
- Collaboration d’équipe dans Splunk SOAR
  - gestion des rôles
  - accès
- Automatisation des réponses pour les incidents critiques
- Création de rapports détaillés sur les incidents
- Intégration des IOCs

Analyse et Visualisation avec Splunk SOAR

- Utilisation des tableaux de bord pour surveiller les KPI de sécurité
- Analyse des performances des playbooks
- Création de rapports automatisés
- Utilisation des logs Splunk SOAR pour diagnostiquer les problèmes
- Personnalisation des visualisations
- Mesure de l’efficacité des processus automatisés

Optimisation des Performances

- Techniques pour réduire les faux positifs dans les alertes
- Ajustements pour accélérer les workflows
- Optimisation des ressources système
- Stratégies pour prioriser les menaces critiques
- Mise à jour et maintenance des intégrations et des playbooks
- Amélioration de l’évolutivité

Sécurité et Conformité de Splunk SOAR

- Meilleures pratiques pour sécuriser Splunk SOAR
- Gestion des accès et des permissions des utilisateurs
- RGPD
- ISO 27001
- Audits des actions automatisées
- Protection des données sensibles dans les workflows
- Préparation des systèmes pour les audits de sécurité

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.

Organisme de formation enregistré sous le numéro 11 75 54743 75. Cet enregistrement ne vaut pas agrément de l’État.
© Ambient IT 2015-2025. Tous droits réservés. Paris, France - Suisse - Belgique - Luxembourg