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

Mis à jour le 15/03/2024

S'inscrire

Formation Huntress Managed Security Platform

3 jours (21 heures)

PRÉSENTATION

Notre formation Huntress vous permettra de protéger efficacement votre entreprise en simulant au travers de votre organisation les nombreuses cyberattaques.

Découvrez l'une des plateformes de cybersécurité les plus appréciées. Progressivement, nous vous présenterons ses diverses fonctionnalités afin que vous puissiez les utiliser pour la protection de votre infrastructure.

Vous saurez interpréter le tableau de bord de Huntress. Accédez aux alertes de sécurité en temps réel, gérez les incidents ou les enquêtes et utilisez les outils de remédiation pour résoudre vos problèmes efficacement.

Dans cette formation, nous approfondirons le simulateur de phishing. Vous saurez ainsi mettre en place une campagne de phishing pour tester les défenses de votre organisme. Nous vous apprendrons également à utiliser le RMM (Remote Monitoring and Management) grâce à ConnectWise et Datto.

Nous vous enseignerons par ailleurs l'implémentation de l'host isolation pour isoler en masse et de manière autonome les hôtes, et l'application du ransomware Canaries, un service parfait pour détecter de potentiels incidents.

Objectifs

- Comprendre les fonctionnalités de Huntress et ses avantages en cybersécurité
- Savoir interpréter et analyser les chiffres du tableau de bord
- Maîtriser les outils de remédiation, y compris l'auto-remédiation, la remédiation manuelle et la remédiation assistée
- Se familiariser avec la simulation de phishing, le ransomware canaries et la gestion des antivirus

Public visé

- Ingénieurs infrastructure
- Administrateurs système
- Administrateurs sécurité
- Responsables en Sécurité Informatique
- Analyste Cybersécurité

Pré-requis

Connaissances en cybersécurité.

Programme de notre formation Huntress Managed Security Platform

Introduction à Huntress

- Présentation
- Pourquoi choisir une plateforme de sécurité gérée ?
- Comment Huntress protège votre entreprise ?
- Présentation des features
- Ajouter Huntress aux listes d'exclusion
- Ajouter Huntress aux listes autorisées
- Résoudre les problèmes réseaux
- Installer l'agent Huntress

Dashboard

- Vue d’ensemble du tableau de bord
- Accès aux alertes de sécurité, incidents actifs et enquêtes
- Utilisation des outils de remédiation
- Auto remédiation
  - Remédiation manuelle
  - Remédiation assistée
  - Reporting en temps réel
- Présentation et paramétrage des rapports
- Envoi des rapports vers d'autres services
- Résoudre les problèmes de panne

Administration

- Gérer plusieurs organisations
- La gestion des utilisateurs
- SAML SSO
- Mise en place de la MFA (Multi Factor Authentification)
- Les méthodes de récupération d'identifiants

Simulation de Phishing

- Présentation du SAT
- L'intérêt d'un simulateur de phishing
- Présentation des différents scénarios
- Créer une campagne de phishing
- Le rapport de phishing

Gestion des antivirus

- Pouvons-nous utiliser d'autres antivirus avec Huntress ?
- Configurer Microsoft Defender pour Huntress
- Les scans complets

RMM

- Présentation de ConnectWise
- Automatisation avec ConnectWise
  - Service Agent
  - Facturation
  - Moniteur interne
  - Moniteur à distance
- Installer les policy avec Datto

Ransomware Canaries

- Ce qu'il faut savoir avant d'utiliser le ransomware Canaries
- Les limitations et les détails techniques
- Lancement et désactivation du ransomware

Host Isolation

- Le fonctionnement de l'isolation
- Isolation en masse
- Self managed isolation
- Séquences des évènements
- Exclusion

Troubleshooting

- Vérifier les statuts agent
- Utiliser le safe mode
- Les erreurs de script
- Mesurer la performance du disque
- Réinstaller la MFA sans backup
- Supprimer les antivirus tiers

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.