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

Mis à jour le 21/11/2023

S'inscrire

Formation Threatlocker : Plateforme Zero Trust de protection des points finaux

2 jours (14 heures)

Présentation

Notre formation ThreatLocker vous présentera cette plateforme de sécurité informatique offrant une approche robuste rentable et granulaire afin de protéger les serveurs, les points de terminaison et les réseaux contre les menaces et attaques informatiques.

Grâce à cette plateforme, vous pourrez interdire l'exécution de toutes les applications, les ransomwares, les scripts et autres logiciels malveillants, à l'exception de ceux qui sont explicitement autorisés.

Durant cette formation, vous serez capable d'utiliser Ringfencing™ pour créer des limites autour des applications afin de dicter la manière dont elles vont interagir avec d'autres applications.

ThreatLocker vous permettra de suivre ainsi que de contrôler l'accès aux données externes et internes. Votre équipe de sécurité pourra voir votre stockage de données et pourra prendre la mesure de bloquer le vol de données pour que cela ne se reproduise plus.

Comme toutes nos formations, celle-ci mettra en lumière les dernières avancées de cette solution, vous assurant d'être à jour avec les nouvelles fonctionnalités de l'outil.

Objectifs

- Savoir installer et configurer ThreatLocker
- Développer des compétences dans la détection de menaces
- Exploiter toutes les fonctionnalités de base de l'outil
- Maîtriser l'outil ThreatLocker

Public visé

- Administrateurs systèmes
- Professionnels IT

Pré-requis

Compétences de base en sécurité informatique.

Programme de notre Formation ThreatLocker

Introduction à l'outil

- Qu'est-ce que ThreatLocker ?
- Compréhension des menaces informatiques
- Sécurité des systèmes
- La sécurisation des applications

Déploiement

- Installation et configuration
- Déploiement manuel
- Déployer ThreatLocker à l'aide d'InTune
- Automatiser le déploiement continu avec ConnectWise
- Déployer ThreatLocker avec N-Central
- Déployer ThreatLocker dans un environnement VDI
- Déploiement de l'agent TL via Kaseya VSA X

Fonctionnalités

- Création automatique de politiques
- Travailler avec un antivirus existant
- Autoriser ThreatLocker à travers son pare-feu
- Configurer la gestion des cyber-héros (Cyber Hero Management)
- Création de stratégies pour surveiller les emplacements de stockage
- Gestion des politiques de sécurité
- Configuration optimale pour se protéger

Gestion des menaces

- Règles d'analyse des e-mails dans ConnectWise Manage
- Stratégies de blocages des attaques
- Identification des menaces potentielles
- Sécurité et confidentialité
- Analyse de l'impact sur les performances

Ringfencing™

- Accès aux fichiers cloisonné
- Interaction avec des applications de cantonnement
- Configuration d'une stratégie de cantonnement IIS
- Séparer une nouvelle application
- Utiliser les exclusions Internet du cloisonnement
- Utiliser des clôtures pour empêcher les mouvements latéraux en cas d'élévation

Administration

- Authentification OTC
- Authentification sans mot de passe
- Création de balises
- Navigation dans la page Administrateurs
- Paramètres de connexion
- Modifier les options de demande de stockage et les noms de stratégie

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.