Jamf 370

Référence Agnosys	JAMF370
Durée	4 jours
Certification	Jamf Certified Admin - Jamf Protect
Support de cours	En anglais

Description

La formation Jamf 370 permet d'approfondir les principes de la sécurité terminaux et des réseaux pour Mac et mobiles avec Jamf Pro et Jamf Protect. Notre environnement de formation pratique, basé sur des scénarios et des exemples, est le meilleur moyen de poursuivre l'étude de la protection des appareils avec Jamf.

Objectifs

• Mettre en œuvre des workflows d'analyse et de collecte de preuves
• Exploiter les renseignements sur les menaces et personnaliser la prévention
• Détecter et corriger les menaces avancées
• Concevoir et déployer un accès réseau Zero Trust (ZTNA)
• Maîtriser la configuration et l'intégration avancées de Jamf Pro et Jamf Protect
• Appliquer des modèles et normes de sécurité avancés pour renforcer la posture défensive
• Se préparer au passage de la certification Jamf Certified Admin - Jamf Protect

Qui peut s'inscrire ?

Cette formation s'adresse aux administrateurs système responsables du déploiement et de la gestion d'appareils Apple avec la solution MDM Jamf Pro et la solution de sécurité Jamf Protect.

Prérequis

- Connaissance de base des scripts (zsh), des variables et des instructions
- Être certifié Jamf Certified Tech - Jamf Pro
- Facultatif, mais fortement encouragé : certification Jamf Certified Associate - Jamf Protect, basée sur l'achèvement du cours Jamf 170
- Facultatif, mais fortement encouragé : certification Jamf Certified Tech - Jamf Protect, basée sur l'achèvement du cours Jamf 270

Participants et matériels sous la responsabilité d'Agnosys

Cette formation est limitée à 12 participants maximum.

Chaque participant accédera aux solutions Jamf Pro et Jamf Protect pour la réalisation des exercices.

Matériels sous la responsabilité exclusive des participants

Chacun des participants devra être équipé sous sa responsabilité :
- d'une connexion Internet fiable avec un débit descendant de 10 Mbps et un débit montant de 5 Mbps
- d'un Mac de test (pas de production) avec n'importe quelle version de macOS Tahoe 26 et une caméra en état de marche
- d'un iPad de test (pas de production) avec n'importe quelle version de iPadOS 26
- facultatif, mais fortement recommandé : d'un ordinateur supplémentaire (production) ou un moniteur externe.

Hors production signifie que le Mac ou l'iPad peut être utilisé pour des tests en classe. Le Mac ou l'iPad ne doit pas être actuellement inscrit dans un serveur MDM, ne doit pas être attribué dans Apple Business Manager ou Apple School Manager et ne doit pas se trouver dans le périmètre d’une inscription PreStage.

Les machines virtuelles macOS ne peuvent pas se substituer à un ordinateur de test physique.

Sujets traités

- Workflows d’analyse et de collecte de preuves
- Renseignements sur les menaces et prévention sur mesure
- Détection et correction des menaces avancées
- Mise en place et déploiement de l’accès réseau Zero Trust (ZTNA)
- Configuration et intégration avancées de Jamf Pro et Jamf Protect

- Modèles de sécurité avancés, critères et normes de référence pour renforcer la protection contre les méthodes des attaquants

Cette formation met en œuvre comme moyens pédagogiques :
- un diaporama présenté par le formateur
- des démonstrations réalisées par le formateur tout au long des leçons
- des travaux pratiques (exercices) réalisées par les participants à la fin de chaque leçon.

AGNOSYS
Conseil - Audit - Formation

Premium Technical Partner

jamf SERVICES Partner

01 64 53 25 25 **www.agnosys.com** **contact@agnosys.fr**