Procédure Opérationnelle sur l’Utilisation de Trend Micro-Vision One

SOMMAIRE

Introduction

Cette procédure a pour objectif de fournir une ligne directrice claire et détaillée pour l'utilisation des solutions Trend Micro-Vision One par les techniciens internes de l'entreprise Inetum. Ce document comporte des sections détaillées sur la gestion des agents, l'administration des configurations, la réponse aux incidents de sécurité et bien plus encore.

Configuration Générale

Accès à la Console Web de Vision One

Pour accéder à la console web de Vision One, utilisez le lien suivant : Trend Vision One™

La console permet de résumer l'état de conformité et de sécurité des serveurs et des agents Vision One ainsi que des systèmes qu'ils protègent.

Vue d'Ensemble de la Solution

Les principaux menus de la solution Vision One comprennent :

- Dashboard : Résumé de l'état de conformité et de sécurité.
- Actions : Gestion des règles de contrôle d'application (non utilisé dans le contexte d'Inetum).
- Alerts : Liste des alertes actuelles et configuration des alertes.
- Events & Reports : Affiche les événements et génère des rapports de conformité et de sécurité.
- Computers : Liste et gestion de toutes les machines gérées par le DSM.
- Policies : Gestion des politiques et des objets associés aux politiques.
- Administration : Administration des propriétés globales de la console et des tâches pour toute la flotte.
- Login : Compte actuellement utilisé, ses propriétés et possibilité de modifier les connexions.
- Help : Accès au guide d'administration de la solution en ligne.
- Support : Accès à la FAQ et menu pour créer des scripts d'installation des agents Vision One (DSA).
- Add/Remove Widgets : Ajouter ou supprimer un widget du tableau de bord.

Nous utilisons Trend Micro pour assurer la sécurité et la conformité de nos systèmes. Le suivi des mises à jour est consultable sur la console d'administration de Trend Micro.

Gestion des Utilisateurs

Administration des Utilisateurs

- Opérations effectuées par l'IT Groupe

Ajout d'un Rôle

- Opérations effectuées par l'IT Groupe

Ajout d'un Contact

Utilisez ce menu pour envoyer des alertes DSM à des contacts n'ayant pas accès à la console.

- Chemin : Administration > User Management > Rôles
- Cliquez sur New
- Entrez les informations de contact
- Sélectionnez un rôle pour définir quelles alertes sont autorisées à être reçues

Gestion des Mises à Jour de Sécurité

- Opérations effectuées par l'IT Groupe

Déploiement des Agents

L'installation de l'agent se fait par script de déploiement. Dans le cas où l'installation échouerait, veuillez-vous rapprocher de votre référent Trend ou ouvrez un ticket auprès de l'IT Groupe.

Configuration des Politiques de Sécurité

Vue d'Ensemble des Politiques

Les politiques définissent les profils de sécurité à appliquer en fonction des types de systèmes et des fonctions qu'ils exploitent.

- Opérations effectuées par l'IT Groupe

Arborescence des Systèmes

La création de groupes de machines est nécessaire pour différencier leur localisation et pouvoir déléguer l'administration.

- Chemin : Computers
- Création d'un groupe de machines :
- Cliquez sur + Add > Create Group(s)
- Entrez un nom de groupe de serveurs
- Choisissez où le placer dans l'arborescence de groupes déjà existante
- Cliquez sur Add
- Cliquez sur Close après avoir créé les différents groupes de serveurs

Remarque : Lors de la synchronisation VCenter, tous les serveurs synchronisés de VCenter ne peuvent pas être déplacés vers les groupes créés. Il est important de créer des Smart Folders pour afficher certains serveurs afin d'appliquer certaines actions spécifiques.

Création des Objets Anti-Malware

Les objets Anti-Malware visent à créer les éléments essentiels pour le bon fonctionnement du module Anti-Malware, y compris les listes d'exclusion des différentes applications en fonction du type de plateforme, le paramétrage des différents types de scan (temps réel, planifié, manuel), et le niveau de sécurité attribué à ces scans pour éviter les problèmes de performance sur les applications métier d'Inetum qui peuvent entraîner des impacts sur la production.

- Opérations effectuées par l’IT Groupe

Gestion des Evénements de Sécurité

Configuration des Tâches Basées sur les Evénements

Les tâches basées sur les événements sont des tâches automatiques et en temps réel basées sur des événements configurés précédemment par l'administrateur.

- Opérations effectuées par l’IT Groupe

Configuration des Tâches Planifiées

Les tâches planifiées peuvent être créées pour automatiser les actions utiles aux opérations Vision One.

- Chemin : Administration > Scheduled Tasks
- Pour configurer une tâche planifiée,

- Cliquez sur New
- Sélectionnez le type de tâche et la période d'exécution
- Liste recommandée des tâches planifiées :
- Check for Security Updates : Vérifie régulièrement les mises à jour de sécurité
- Generate and Send Report : Génère automatiquement des rapports et les envoie éventuellement par email à une liste de destinataires
- Scan for Integrity changes : Le Workload Security analyse l'intégrité pour comparer l'état actuel d'un ordinateur à sa base de référence
- Scan computers for Malware : Planifie une analyse de logiciels malveillants