Évaluation des vulnérabilités pour VMware

DESCRIPTION GÉNÉRALE DES SERVICES[1]

L'Évaluation de Sécurité VMware est un service d'évaluation de sécurité et de conformité, de nature consultative, fourni par Park Place Technologies (PPT). Ce service utilise un outil d'analyse VMware entièrement automatisé, géré par PPT, ainsi qu'un moteur d'analyse de sécurité pour effectuer une collecte de données de configuration en mode lecture seule, puis générer et livrer des rapports d'évaluation de la sécurité. Toutes les activités d'analyse, de validation et de recommandation sont effectuées par des experts en sécurité de PPT.

Ce service fournit une évaluation complète de l'environnement de virtualisation VMware du Client, incluant les serveurs vCenter, les hôtes ESXi, les clusters, le réseau virtuel, les machines virtuelles et les composants de stockage.

L'évaluation identifie les mauvaises configurations, les lacunes en matière de sécurité et les écarts de conformité en accord avec des cadres d'excellence tels que les CIS Benchmarks, DISA STIGs, les VMware Hardening Guidelines, le NIST Cybersecurity Framework, et les critères SOC 2 Trust Services.

SERVICES ET LIVRABLES

PPT effectue l'identification de vulnérabilités spécifiques à VMware-, l'analyse des configurations et l'évaluation de conformité (« Services »). Tous les services sont réalisés à distance.

Activités d'évaluation

PPT s'appuie sur un script d'analyse VMware automatisé, en mode lecture seule-, et sur un moteur d'analyse gérés par PPT pour :

- Collecter les métadonnées de configuration VMware sans stockage de credentials ni modification de la configuration.
- Évaluer les configurations par rapport à plus de 200 contrôles de sécurité alignés avec VMware-.
- Détecter les mauvaises configurations, les paramètres non sécurisés et les dérives de configuration.
- Mapper les résultats à plusieurs cadres de conformité simultanément.
- Identifier les problèmes concernant vCenter, les hôtes ESXi, les clusters, les machines virtuelles, le réseau, les certificats, l'authentification et la journalisation.
- Valider les résultats et éliminer les faux positifs identifiables.

Livrables

Mise en service

- Implémentation et Évaluation initiale.
- Briefing exécutif résumant le score de sécurité de base, les principales conclusions-, l'état de conformité et les prochaines étapes recommandées.

[1] L'outil d'analyse (« Logiciel ») est un produit propriétaire de Kalosys, sous licence de PPT. Tous les brevets, droits d'auteur, secrets commerciaux et autres droits de propriété intellectuelle appartiennent exclusivement à Kalosys et à ses concédants de licence. Le Client n'acquiert qu'un droit limité d'utilisation du Logiciel, et non un droit de propriété. Le Client s'engage à ne pas : (a) copier, modifier ou créer des œuvres dérivées ; (b) procéder à de l'ingénierie inverse, décompiler ou désassembler ; (c) retirer les mentions ou étiquettes de propriété ; (d) accorder des sous-licences, louer, prêter ou transférer ; (e) utiliser pour fournir des services à des tiers ; ou (f) contourner les mesures de protection. L'Utilisateur final comprend que ce Logiciel est conçu pour l'évaluation de la sécurité et accepte de l'utiliser uniquement sur des systèmes qu'il est autorisé à tester.

Rapport Automatisé Récurrent

Livré automatiquement selon la fréquence choisie par le Client (mensuelle, trimestrielle ou hebdomadaire) :

- Résultats de conformité mappés aux CIS, DISA STIG, VMware Hardening Guides, NIST CSF, SOC 2.
- Inventaire des observations de sécurité classé par gravité.
- Classification des vulnérabilités incluant les CVE et les scores de gravité CVSS.
- Guide de remédiation avec des actions correctives recommandées.
- Plan d'action priorisé en fonction du risque et de l'impact opérationnel.
- Rapports livrés dans divers formats pris en charge.

Portée Consultative

PPT fournit uniquement des analyses et des recommandations. Le Client est entièrement responsable de la mise en œuvre de toutes les actions de remédiation, des changements de configuration, et des actions opérationnelles.

Portée du Support VMware

- VMware vSphere 6.7 et versions ultérieures
- Services vCenter Server, authentification, permissions, journalisation
- Renforcement des hôtes ESXi (services, pare-feu, certificats, NTP, politiques de mot de passe/verrouillage)
- Services des clusters (HA, DRS, EVC, vSAN)
- Configuration des vSwitch/vDS et sécurité des groupes de ports
- Paramètres de configuration des machines virtuelles, VMware Tools, politiques d'isolation
- Configuration des datastores et du vSAN

PROCESSUS ET SLA

Évaluation Initiale et Mise en Œuvre

- Déploiement du script d'analyse sur le système désigné par le Client-.
- Validation des prérequis de l'outil.
- Vérification de la connectivité et des autorisations vCenter.
- Exécution de l'évaluation de base VMware.
- Configuration de la livraison automatisée des rapports.

Briefing Exécutif & Technique

- Aperçu des constats de base.
- Résumé de l'état de conformité.
- Recommandations de remédiation priorisées (consultatives uniquement).

Évaluations Continues

- Analyses automatisées effectuées selon la fréquence définie par le Client-.
- Détection de nouvelles vulnérabilités et régressions.
- Surveillance des dérives de configuration.

Rapports d'Avancement

- Tendances dans la posture de sécurité VMware.
- Détection récurrente des problèmes.
- Visibilité sur l'avancement des remédiations.

LIMITATIONS DU SERVICE

Ce service n'inclut pas :

- La surveillance en temps réel, le SIEM/SOC, ou la réponse aux incidents.
- L'investigation d'incidents ou l'analyse médico-légale.
- Le patching, les mises à jour ou les opérations du cycle de vie de VMware.
- L'exécution des remédiations ou des modifications de configuration.
- Le dépannage de performances (calcul, stockage ou réseau).
- La conception d'architecture, l'ingénierie ou la planification de capacité.
- L'automatisation, la création de scripts ou les intégrations sur-mesure.
- La préparation à la certification de conformité (ISO, PCI, SOC 2).
- Le support ITSM (tickets, flux de travail, CAB).
- L'approvisionnement en licences ou la gestion des droits.
- Les services d'ingénierie sur site ou de matériel.

RESPONSABILITÉS DU CLIENT

Le Client doit :

- Affecter du personnel VMware et sécurité pour soutenir l'exécution du service.
- Fournir des credentials en mode lecture seule- et une autorisation pour les cibles d'évaluation.
- S'assurer que tous les systèmes VMware sont accessibles pendant les fenêtres de scan.
- Assumer la responsabilité de toutes les activités de remédiation et opérationnelles.
- Gérer la classification, la gestion et la rétention des données d'évaluation.
- Reconnaître une charge temporaire des ressources pendant l'évaluation.
- Maintenir la gouvernance et le contrôle des changements pour toutes les configurations VMware.

SÉCURITÉ DE L'OUTIL DE SCAN, PROTECTION DES DONNÉES ET PORTÉE DE COLLECTE

PPT garantit un fonctionnement sécurisé et contrôlé de l'outil de scan. Les éléments clés incluent :

- Collecte de données en mode lecture seule- et non intrusive-.
- Aucun agent installé ; aucune modification de configuration effectuée.
- Les credentials sont utilisés uniquement pendant la session active et ne sont jamais stockés.
- Seules les métadonnées de configuration VMware sont collectées (vCenter, ESXi, cluster, stockage, réseau, authentification, certificats, journalisation, NTP, et détails de licence masqués).
- Aucune collecte de contenu des systèmes d'exploitation invités des machines virtuelles, des données d'applications, des données des utilisateurs, des mots de passe ou des clés de licence complètes.
- Toutes les communications sont chiffrées via HTTPS (443).
- Les artefacts d'évaluation sont chiffrés en transit et au repos.
- L'accès est restreint au personnel autorisé de PPT et du Client.