Renforcez la cybersécurité de vos serveurs avec Dell CloudIQ

Synthèse

Plusieurs années peuvent être nécessaires aux organisations pour se bâtir une bonne réputation auprès de leurs clients, mais quelques minutes suffisent après un incident lié à la cybersécurité pour la réduire à néant. Les équipes de cybersécurité et les administrateurs de serveurs doivent utiliser tous les outils à leur disposition pour renforcer leur infrastructure. Voici une fonctionnalité Dell CloudIQ que chaque client équipé de Dell PowerEdge doit connaître.

Cette note technique Direct from Development (DfD) décrit les fonctionnalités de cybersécurité destinées aux serveurs PowerEdge intégrées dans CloudIQ.

CloudIQ est l'application Cloud de surveillance et d'analytique prédictive basée sur l'intelligence artificielle/l'apprentissage automatique dédiée à la gamme de produits d'infrastructure Dell. Hébergée dans la solution sécurisée Cloud Dell IT, CloudIQ collecte et analyse les informations sur l'intégrité, les performances et la télémétrie pour localiser les risques et recommander des actions en vue de résoudre rapidement les problèmes.

Auteur

Mark Maclean
Ingénierie marketing technique

Kyle Shannon
Gestion de produits

Version 1.1, juillet 2022

Introduction

Dell CloudIQ offre une fonctionnalité de cybersécurité qui inclut désormais les serveurs Dell PowerEdge. Cette fonctionnalité de cybersécurité intégrée à CloudIQ permet aux équipes chargées des serveurs des clients de créer une stratégie appelée plan d'évaluation. Ce plan d'évaluation repose sur plusieurs tests des critères de configuration prêts à l'emploi « cliquer pour sélectionner ». Cette liste de paramètres et de valeurs de configuration s'appuie sur les bonnes pratiques Dell et le cadre de cybersécurité du NIST (National Institute of Standards and Technology) américain.

Une approche assurant des résultats rapides

Un spécialiste disposant des compétences appropriées qui connaît les paramètres de configuration de sécurité exacts ainsi que les valeurs adéquates peut créer un profil de configuration de serveur « SCP » et l'utiliser directement avec le modèle de configuration de l'iDRAC ou d'OME pour définir les configurations de serveur. Toutefois, CloudIQ offre une méthode beaucoup plus rapide et prescriptive pour mettre en œuvre une politique d'évaluation de la cybersécurité reposant sur les paramètres et valeurs recommandés par Dell. Pour rationaliser davantage le processus de cybersécurité, CloudIQ peut agréger plusieurs instances OME, offrant ainsi une vue consolidée des serveurs sur plusieurs sites. Certaines organisations peuvent choisir d'utiliser OME et CloudIQ pour justifier la séparation entre la conformité de la configuration et la gestion de la sécurité.

Figure 1 Récapitulatif de l'état de cybersécurité sur la page de présentation CloudIQ

La section dédiée à la cybersécurité ci-dessus disponible sur la page de présentation CloudIQ indique l'état du niveau de risque, en précisant le nombre de systèmes dans chaque catégorie de risque et le nombre total de problèmes détectés. Le risque est déterminé par la gravité et le nombre de problèmes par serveur. Par exemple, un serveur présentant un ou plusieurs problèmes graves est classé dans la catégorie des risques très élevés. Si un serveur présente plus de cinq risques peu graves, sachant qu'au moins l'un d'entre eux est un problème moyennement grave, il serait également classé dans la catégorie des risques très élevés.

Identifier rapidement les risques

Le tableau de bord des risques système classe chaque serveur en y appliquant une politique et en l'affichant dans sa propre carte accompagnée de l'état du niveau de risque de cybersécurité. Cela permet aux clients de hiérarchiser rapidement les actions et d'accélérer le délai de résolution.

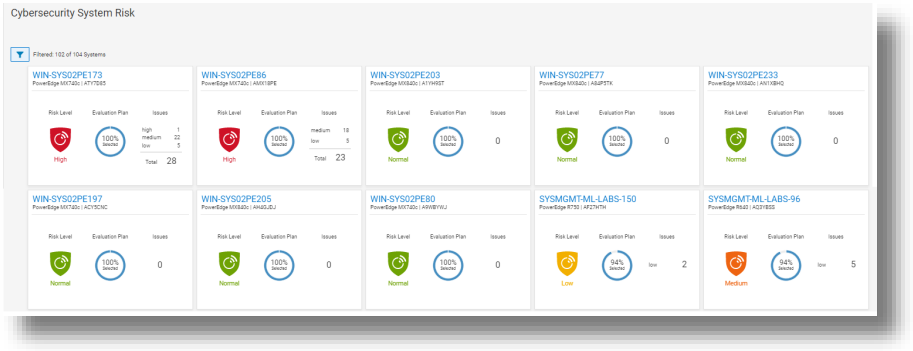

Figure 2 Tableau de bord répertoriant les risques liés à la cybersécurité de tous les systèmes

En plus du tableau de bord, l'état de l'évaluation de la sécurité affiche les informations relatives à chaque serveur avec l'action recommandée pour rétablir toute configuration de sécurité obsolète à l'état souhaité. Le graphique circulaire affiche le nombre de règles sélectionnées sous la forme du pourcentage du nombre total de tests dans le plan d'évaluation des risques attribué au serveur en question.

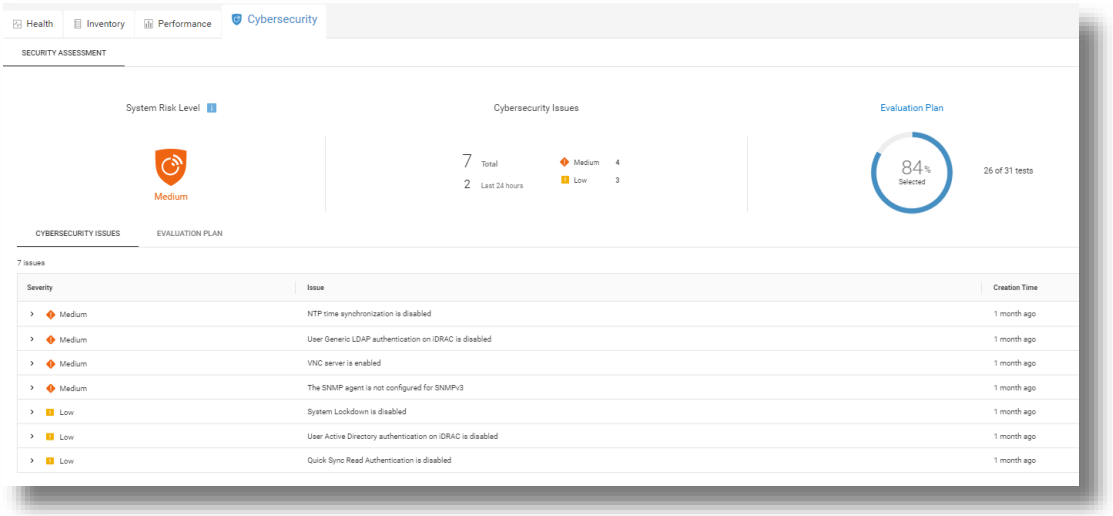

Figure 3 Détails et recommandations sur les risques liés à la cybersécurité

Sur la page des détails du système, sous l'onglet Cybersécurité, vous trouverez des informations sur le plan d'évaluation et son état. En bas de la page se trouvent deux onglets : Problèmes de cybersécurité, indiquant les éléments non conformes avec l'action corrective et Plan d'évaluation, affichant l'ensemble du plan et l'état de sélection de chaque test.

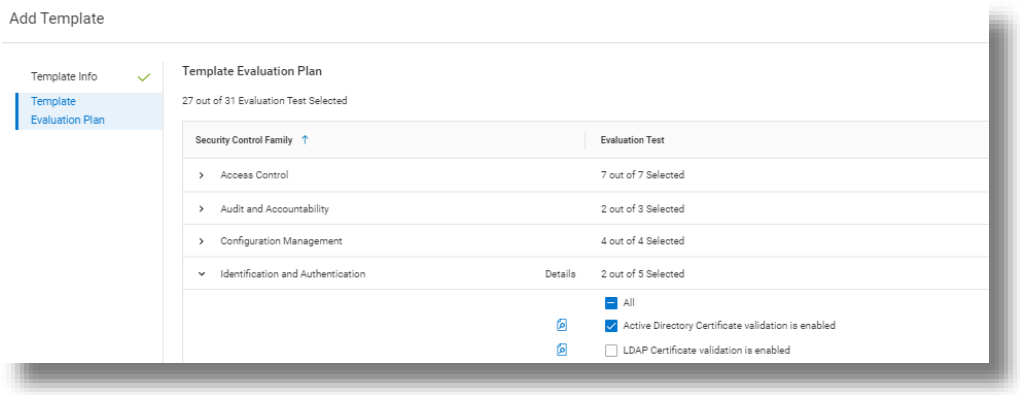

Figure 4 Sélection du test

Les utilisateurs CloudIQ peuvent également choisir de recevoir un e-mail Daily Digest comprenant un récapitulatif de l'état de cybersécurité.

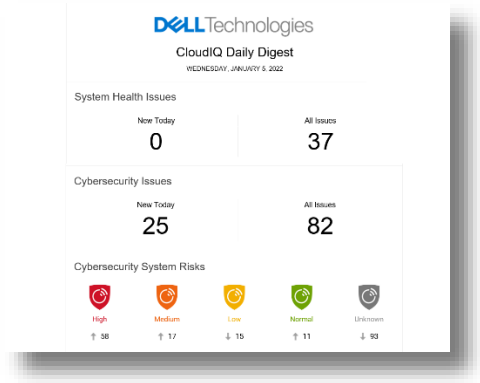

Figure 5 E-mail Daily Digest CloudIQ

Habilitation et sécurité

Comme vous pouvez vous en douter, il existe un certain nombre de contrôles d'accès de sécurité intégrés dans CloudIQ au niveau des comptes d'administrateur et d'utilisateur qui permettent de gérer la création de rapport. Il existe deux rôles de cybersécurité intégrés à CloudIQ : administrateur de cybersécurité et observateur de cybersécurité. Ces rôles peuvent être attribués à partir de comptes disposant de droits d'administrateur CloudIQ.

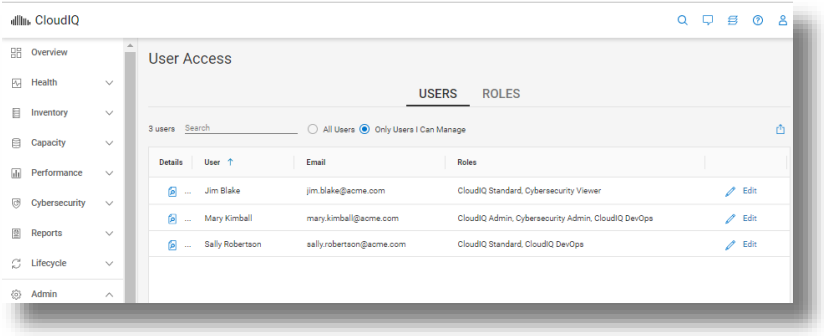

Figure 6 Configuration RBAC

Pour prendre en charge la cybersécurité pour PowerEdge dans CloudIQ, les clients doivent exécuter OpenManage Enterprise version 3.9 ou supérieure alors que le plug-in CloudIQ 1.1 ou version supérieure est activé. Tous les serveurs nécessitent une couverture Dell ProSupport et doivent déjà avoir été détectés par OME.

Éléments de test du plan d'évaluation de la cybersécurité PowerEdge

Le tableau ci-dessous présente chaque critère de test et la famille de plans de test auquel il appartient.

Famille	Titre
Système et communications	L'interface IPMI sur LAN est désactivée
Système et communications	L'interface IPMI série sur LAN est désactivée
Système et communications	Le chiffrement de la console virtuelle est activé
Système et communications	Le chiffrement des supports virtuels est activé
Système et communications	La détection automatique est désactivée
Système et communications	Les fonctionnalités VLAN de l'iDRAC sont activées
Système et communications	TLS 1.2 ou TLS 1.3 est activé sur le serveur Web de l'iDRAC
Système et communications	Les demandes HTTP du serveur Web de l'iDRAC sont redirigées vers les demandes HTTPS
Système et communications	Le type de plug-in de console virtuelle est activé
Système et communications	L'iDRAC utilise la carte NIC dédiée
Système et communications	TLS 1.2 ou TLS 1.3 est activé sur le serveur Web de l'iDRAC
Contrôle d'accès	Le blocage IP est activé
Contrôle d'accès	Le serveur VNC est désactivé
Contrôle d'accès	L'agent SNMP est configuré pour SNMPv3
Contrôle d'accès	L'authentification de lecture Quick Sync sur le serveur est activée
Contrôle d'accès	SSH est désactivé
Contrôle d'accès	L'authentification LDAP générique de l'utilisateur sur l'iDRAC est activée
Contrôle d'accès	L'authentification Active Directory de l'utilisateur sur l'iDRAC est activée
Gestion de la configuration	Les ports USB sont désactivés
Gestion de la configuration	Le protocole Telnet est désactivé[1]
Gestion de la configuration	System Lockdown est activé
Gestion de la configuration	La configuration de l'iDRAC à partir du test POST du BIOS est désactivée
Audit et responsabilité	La synchronisation de l'heure NTP est activée
Audit et responsabilité	Le protocole NTP est sécurisé
Audit et responsabilité	Le journal syslog distant est activé
Intégrité du système et des informations	La configuration de l'iDRAC compatible avec la configuration locale sur le système hôte est désactivée
Intégrité du système et des informations	Secure Boot est activé
Identification et authentification	Le mot de passe respecte les critères minimaux de protection forte
Identification et authentification	La validation du certificat LDAP est activée
Identification et authentification	La validation du certificat Active Directory est activée
Identification et authentification	Le chiffrement SSL du serveur Web de l'iDRAC utilise 256 bits au moins
Identification et authentification	Serveur Web de l'iDRAC – SCEP est activé

1. À partir de la version 4.40.00.00 du firmware de l'iDRAC, la fonctionnalité Telnet est supprimée de l'iDRAC

Synthèse

Contrairement aux collaborateurs IT classiques, CloudIQ n'a pas besoin de manger, de dormir ou de partir en vacances. Les organisations peuvent donc s'appuyer sur les politiques de cybersécurité CloudIQ pour surveiller en permanence les serveurs non conformes. La cybersécurité intégrée à CloudIQ permet aux clients d'accélérer la mise en place de la sécurité des serveurs par l'intermédiaire de l'automatisation des tests prédéfinis et de la visualisation de l'état. Leurs administrateurs de serveurs bénéficient ainsi de niveaux élevés de flexibilité, tout en conservant la gouvernance et le contrôle indispensables aux équipes de cybersécurité. CloudIQ réduit davantage les risques et améliore la productivité IT en affichant le niveau de cybersécurité ainsi que l'état d'intégrité système des serveurs et de la gamme d'infrastructures Dell dans le même portail pratique et basé sur le Cloud.

Références

CloudIQ on Dell.com : pour obtenir des informations sur les produits, regarder des vidéos de démo et bien plus encore

Blog : Prenez le contrôle de la cybersécurité des serveurs avec une solution de surveillance intelligente basée sur le Cloud

Vidéo : Création et suivi des politiques de cybersécurité Dell CloudIQ pour les serveurs PowerEdge

Page de connaissances techniques sur le plug-in OpenManage Enterprise CloudIQ

Solutions Dell supplémentaires liées à la cybersécurité

En savoir plus sur les serveurs PowerEdge

Contactez-nous pour tout commentaire et toute demande

Suivez-nous pour les actualités PowerEdge