Rafforza la sicurezza informatica dei tuoi server con Dell CloudIQ

Riepilogo

Le organizzazioni potrebbero impiegare anni per crearsi una buona reputazione presso i clienti e bastano pochi minuti di un incidente correlato alla sicurezza informatica per comprometterla. I team addetti alla sicurezza informatica e gli amministratori dei server devono utilizzare ogni strumento a disposizione per potenziare l'infrastruttura. Ecco una funzione di Dell CloudIQ che ogni cliente Dell PowerEdge dovrebbe conoscere.

Questa nota tecnica Direct from Development (DfD) descrive le funzionalità di sicurezza informatica per i server PowerEdge integrati in CloudIQ.

CloudIQ è l'applicazione di monitoraggio e di analisi predittiva basati su cloud e AI/ML per il portafoglio di prodotti d'infrastruttura di Dell. In hosting nel cloud sicuro Dell IT, CloudIQ raccoglie e analizza integrità, prestazioni e telemetria per individuare i rischi e consigliare azioni per una risoluzione rapida dei problemi.

Autore

Mark Maclean
Technical Marketing Engineering

Kyle Shannon
Gestione dei prodotti

Versione 1.1 luglio 2022

Introduzione

Dell CloudIQ offre una funzionalità di sicurezza informatica che ora include i server Dell PowerEdge. La funzionalità di sicurezza informatica integrata in CloudIQ consente ai team di server dei clienti di creare una policy definita piano di valutazione. Questo piano di valutazione si basa su una serie di test di criteri di configurazione "click to pick" pronti all'uso. L'elenco di impostazioni e valori di configurazione si basa sulle best practice di Dell e sul framework di sicurezza informatica del NIST (National Institute of Standards and Technology) americano.

Un approccio per risultati rapidi

Uno specialista con le competenze giuste che comprende le esatte impostazioni di configurazione di sicurezza con valori corretti riesce a creare un profilo di configurazione server "SCP" utilizzandolo direttamente con la funzione del modello di configurazione di iDRAC o OME per impostare le configurazioni server. Tuttavia, CloudIQ offre un metodo molto più rapido e prescrittivo per attuare una policy di valutazione della sicurezza informatica basata sulle impostazioni e sui valori consigliati da Dell. Per semplificare ulteriormente il processo di sicurezza informatica, CloudIQ aggrega più istanze OME, offrendo una vista consolidata dei server in più sedi. Alcune organizzazioni decidono di utilizzare OME e CloudIQ per dimostrare la separazione tra conformità della configurazione e security management.

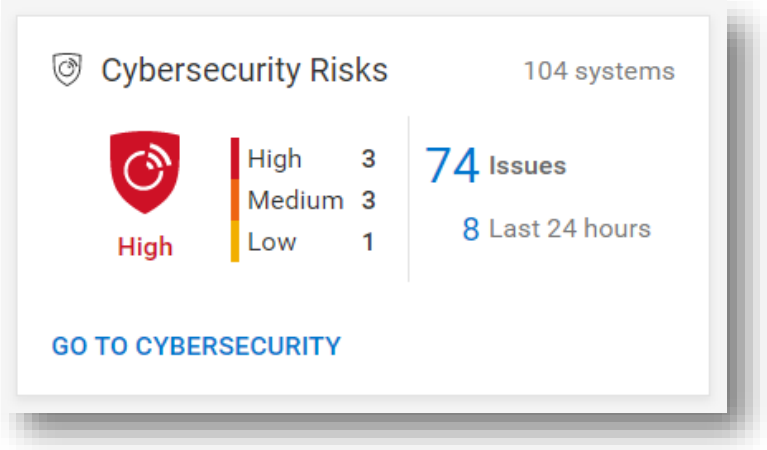

Figura 1 Riepilogo dello stato della sicurezza informatica dalla pagina di panoramica di CloudIQ

Il riquadro sulla sicurezza informatica riportato sopra è nella pagina di panoramica di CloudIQ e offre una visione aggregata dello stato del livello di rischio, suddividendo il numero di sistemi in ciascuna categoria di rischio e il numero totale di problemi rilevati. Il rischio è determinato dalla gravità e dal numero di problemi per server. Ad esempio, un server con uno o più problemi ad alto rischio è classificato come ad alto rischio, ma anche un server con più di cinque rischi non elevati di cui almeno uno come un problema medio verrebbe classificato come rischio elevato.

Identificazione rapida dei rischi

Il dashboard dei rischi di sistema classifica ogni server con una policy applicata, mostrando ogni server nella propria scheda con lo stato del livello di rischio nel settore della sicurezza informatica. In questo modo, i clienti assegnano rapidamente priorità alle azioni e velocizzano il tempo di risoluzione dei problemi.

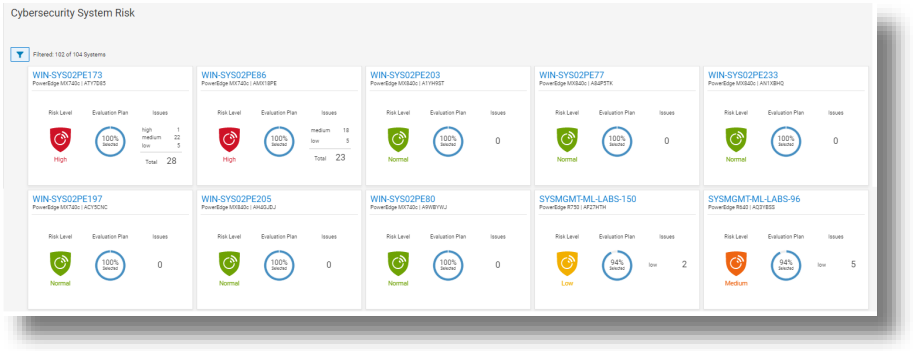

Figura 2 Rischio del sistema di sicurezza informatica Dashboard tutti i sistemi

Oltre al dashboard, lo stato di valutazione della sicurezza mostra i dettagli per ogni server con azione consigliata per riportare qualsiasi configurazione di sicurezza deviata allo stato preferito. Il grafico a torta mostra il numero di regole selezionate come percentuale rispetto ai test totali nel piano di valutazione del rischio assegnato al server specifico.

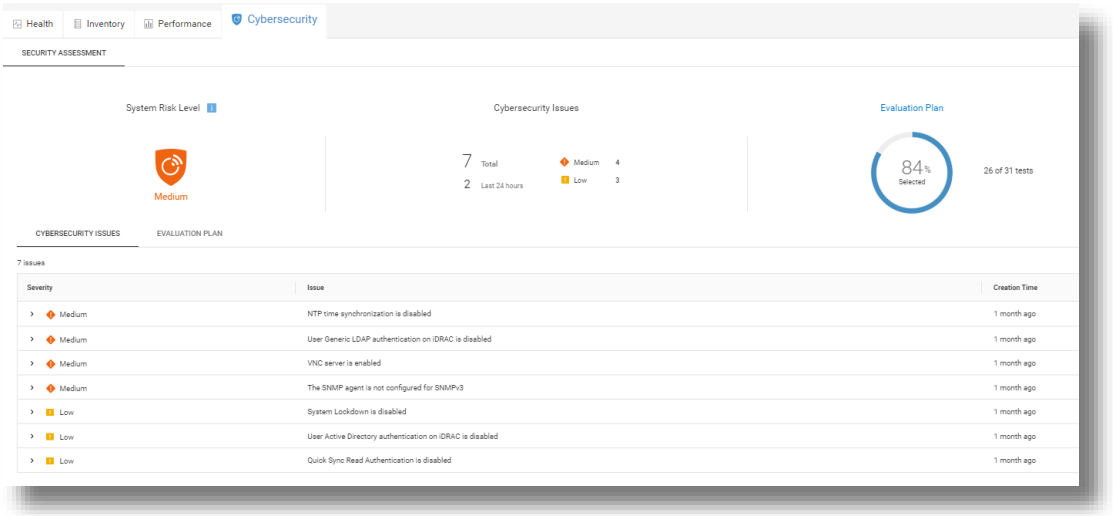

Figura 3 Dettagli e consigli in merito ai rischi per la sicurezza informatica

Nella pagina dei dettagli del sistema, sotto la scheda Sicurezza informatica, sono disponibili dettagli sul piano di valutazione e sul relativo stato. In basso nella pagina sono presenti due schede: Problemi di sicurezza informatica, che descrive in dettaglio gli elementi non conformi con l'azione correttiva, e Piano di valutazione, che mostra l'intero piano e lo stato di selezione di ciascun test.

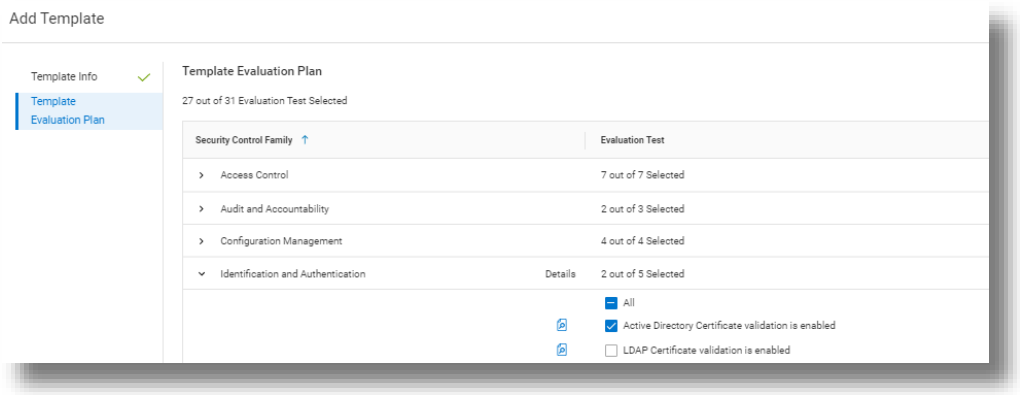

Figura 4 Selezione test

Gli utenti di CloudIQ possono anche scegliere di ricevere un'e-mail Daily Digest, incluso un riepilogo dello stato della sicurezza informatica.

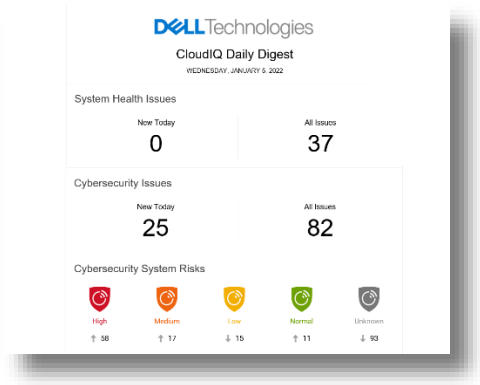

Figura 5 E-mail di CloudIQ Daily Digest

Abilitazione e sicurezza

Come ci si aspetterebbe, in CloudIQ sono integrati vari controlli degli accessi di sicurezza relativi agli account amministratore e utente per controllare creazione e reporting. I ruoli di sicurezza informatica creati per CloudIQ sono due: Cybersecurity Admin e Cybersecurity Viewer. Questi ruoli possono essere assegnati dagli account con diritti di amministratore CloudIQ.

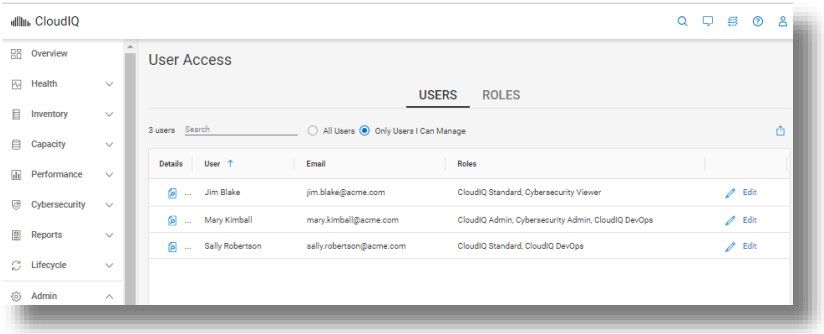

Figura 6 Configurazione RBAC

Per supportare la sicurezza informatica per PowerEdge all'interno di CloudIQ, i clienti devono avere OpenManage Enterpriser 3.9 o versione successiva con il plug-in CloudIQ 1.1 o versione successiva abilitato. Tutti i server richiedono la copertura Dell ProSupport e devono essere già rilevati da OME.

Elementi di test del piano di valutazione della sicurezza informatica PowerEdge

La tabella seguente riporta in dettaglio ogni criterio di test e la relativa famiglia del piano di test.

Famiglia	Qualifica
Sistema e comunicazioni	IPMI su interfaccia LAN disabilitata
Sistema e comunicazioni	IPMI seriale su LAN disabilitata
Sistema e comunicazioni	La crittografia della console virtuale è abilitata
Sistema e comunicazioni	La crittografia dei supporti virtuali è abilitata
Sistema e comunicazioni	Auto-Discovery disabilitata
Sistema e comunicazioni	Funzionalità VLAN di iDRAC abilitate
Sistema e comunicazioni	Server web iDRAC con TLS 1.2 o TLS 1.3 abilitato
Sistema e comunicazioni	Richieste HTTP del server web iDRAC reindirizzate alle richieste HTTPS
Sistema e comunicazioni	Tipo di plug-in della console virtuale abilitato
Sistema e comunicazioni	iDRAC utilizza la scheda di rete dedicata
Sistema e comunicazioni	Server web iDRAC con TLS 1.2 o TLS 1.3 abilitato
Controllo degli accessi	Blocco IP abilitato
Controllo degli accessi	Server VNC disabilitato
Controllo degli accessi	Agent SNMP configurato per SNMPv3
Controllo degli accessi	Autenticazione di lettura Quick Sync per il server abilitata
Controllo degli accessi	SSH disabilitato
Controllo degli accessi	Autenticazione LDAP utente generico su iDRAC abilitata
Controllo degli accessi	Autenticazione utente Active Directory su iDRAC abilitata
Configuration Management	Porte USB disabilitate
Configuration Management	Protocollo Telnet disabilitato[1]
Configuration Management	Blocco del sistema abilitato
Configuration Management	Configurazione iDRAC dal BIOS POST disabilitata
Audit e responsabilità	Sincronizzazione dell'ora NTP abilitata
Audit e responsabilità	NTP protetto
Audit e responsabilità	Syslog remoto abilitato
Integrità del sistema e delle informazioni	Configurazione iDRAC abilitata per la configurazione locale sul sistema host disabilitata
Integrità del sistema e delle informazioni	Avvio sicuro abilitato
Identificazione e autenticazione	La password ha un punteggio minimo di protezione avanzata
Identificazione e autenticazione	Convalida del certificato LDAP abilitata
Identificazione e autenticazione	Convalida del certificato Active Directory abilitata
Identificazione e autenticazione	Crittografia SSL del server web iDRAC a 256 bit o superiore
Identificazione e autenticazione	Server web iDRAC - SCEP abilitato

1. A partire dalla versione del firmware iDRAC 4.40.00.00, la funzione Telnet viene rimossa da iDRAC

Riepilogo

A differenza del tipico membro del team IT, a CloudIQ non occorre mangiare, dormire o andare in vacanza, quindi le organizzazioni si affidano alle policy di sicurezza informatica di CloudIQ per monitorare costantemente i server non conformi. La sicurezza informatica integrata in CloudIQ consente ai clienti di accelerare la distribuzione della sicurezza dei server attraverso l'automazione di test predefiniti e visualizzazione dello stato. Questo approccio fornisce elevati livelli di flessibilità per gli amministratori dei server, mantenendo al contempo la governance e il controllo che i team addetti alla sicurezza informatica devono applicare. CloudIQ riduce ulteriormente i rischi e migliora la produttività IT mostrando la sicurezza informatica, lo stato di integrità del sistema dei server e il più ampio portafoglio di infrastrutture Dell, il tutto nello stesso comodo portale basato su cloud.

Riferimenti

CloudIQ su Dell.com: per informazioni sui prodotti, video dimostrativi e altro ancora

Blog sull'assunzione del controllo della sicurezza informatica dei server grazie al monitoraggio intelligente basato su cloud

Video su creazione e monitoraggio delle policy di Dell CloudIQ Cybersecurity per i server PowerEdge

Pagina delle conoscenze tecniche per il plug-in OpenManage Enterprise CloudIQ

Ulteriori soluzioni correlate alla sicurezza informatica di Dell