Dell CloudIQ Cybersecurity per PowerEdge: i vantaggi dell'automazione

Riepilogo

Per proteggere i server dalle crescenti minacce informatiche, i team addetti all'infrastruttura dei clienti possono scegliere di rafforzarne varie impostazioni. Tuttavia, come individuano la best practice da utilizzare per le impostazioni di configurazione della sicurezza di Dell? Inoltre, di quali strumenti dispongono per verificare con efficienza e continuità se le impostazioni sono configurate o modificate in modo errato? La risposta è la funzionalità della sicurezza informatica in CloudIQ per la soluzione PowerEdge AIOps, che confronta la configurazione dei server PowerEdge implementati con una policy di configurazione relativa alla sicurezza. Quando CloudIQ identifica una deviazione tra l'impostazione di configurazione effettiva e quella consigliata, avvisa l'amministratore e raccomanda correzioni per risolvere i problemi.

Questa nota tecnica di Direct from Development (DfD) descrive in dettaglio il risparmio di tempo che i clienti ottengono utilizzando il policy engine automatizzata di sicurezza informatica CloudIQ rispetto all'esame di conformità manuale.

Autori

Mark Maclean
Technical Marketing Engineering

Kyle Shannon
Gestione dei prodotti

Versione 1.1 luglio 2022

Introduzione

Nell'ambiente di oggi, sempre attivo e connesso, tutte le organizzazioni devono costantemente migliorare la propria strategia di sicurezza informatica per mitigare la crescente minaccia di attacco. Utilizzando la funzionalità di sicurezza informatica integrata di Dell CloudIQ, i clienti sono in grado di creare facilmente policy di sicurezza per la protezione dei server PowerEdge. Una policy è costituita da test pronti all'uso che i clienti abilitano limitandosi a selezionare una casella. I test contengono impostazioni di sicurezza dell'infrastruttura basate sulle best practice di Dell e sul framework di sicurezza informatica del NIST (National Institute of Standards and Technology) americano. Dell CloudIQ Cybersecurity per PowerEdge consente di creare facilmente una policy e di automatizzarne il controllo, rendendola semplice, efficiente e prevedibile.

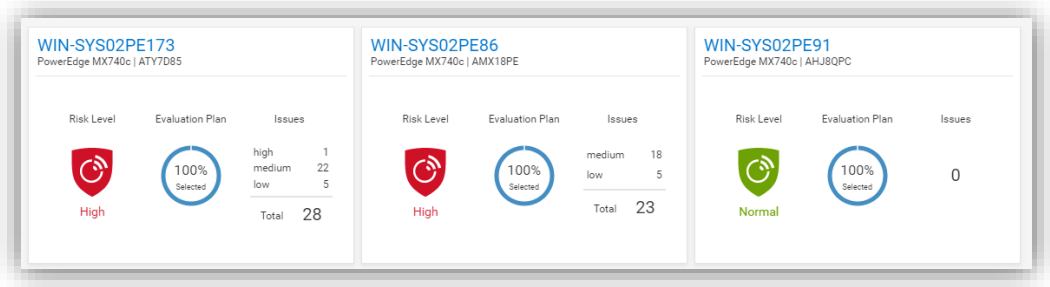


Figura 1 Dashboard CloudIQ Cybersecurity

CloudIQ è l'applicazione di monitoraggio e analisi proattivi AIOP che fornisce suggerimenti e informazioni sull'integrità dei sistemi per le soluzioni di infrastruttura Dell, tra cui storage, protezione dei dati, rete e, naturalmente, server PowerEdge. Il policy engine di sicurezza informatica integrato in CloudIQ vanta oltre 30 regole di configurazione di sicurezza per PowerEdge di semplice attuazione. CloudIQ è basato su cloud; pertanto può integrarsi con un numero qualsiasi di istanze OpenManage Enterprise (OME) su più data center tramite il plug-in OME CloudIQ. Questo significa che CloudIQ applica la stessa policy a più server gestiti da OME indipendentemente dalla loro posizione. Si tratta di una funzione che CloudIQ offre senza alcuna configurazione aggiuntiva a livello di iDRAC o OME. Una volta stabilita la policy, CloudIQ verifica continuamente lo stato desiderato delle impostazioni di configurazione della sicurezza di PowerEdge rispetto all'attuale configurazione effettiva. Se un server non è conforme alle policy, viene evidenziato. CloudIQ classifica i risultati con i server più vulnerabili, dato un livello di rischio "elevato". I singoli problemi vengono visualizzati con la correzione consigliata. È quindi possibile eseguire le correzioni della configurazione di sicurezza consigliate a livello individuale per server utilizzando l'interfaccia grafica utente di iDRAC o, se più host risultano non conformi, utilizzare OME per fornire un file di modello di aggiornamento della configurazione o eseguire uno script RACADM per correggere le configurazioni di sicurezza per più server.

I vantaggi dell'automazione

Per comprendere il profondo impatto dell'automazione di questo processo, lo abbiamo testato rispetto a un processo manuale per 1, 10, 100* e 1.000* server. In base ai test dell'approccio CloudIQ Cybersecurity per un cliente con 1.000* server, abbiamo riscontrato quanto segue:

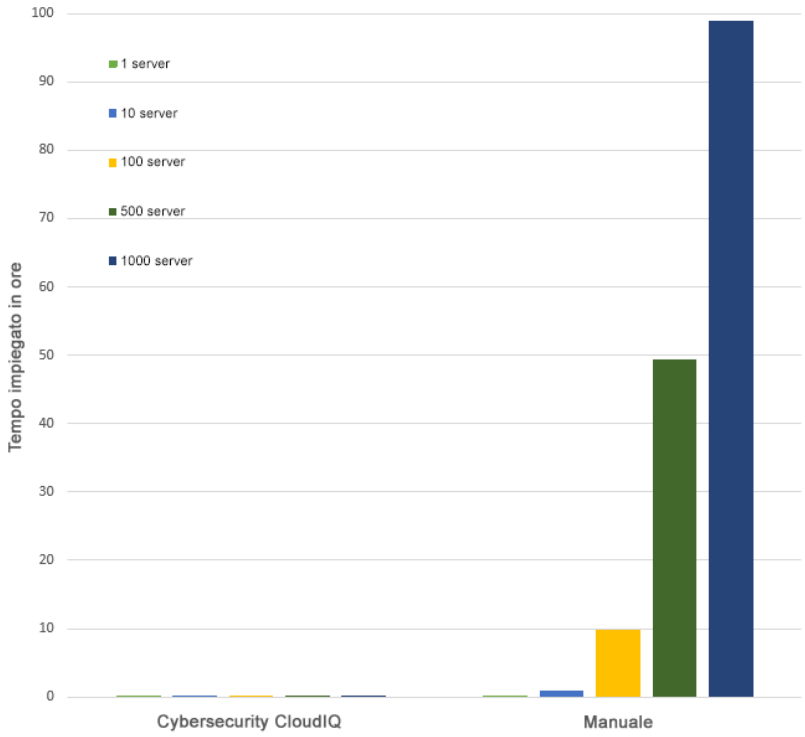
- Creazione di una policy di 15 test e sua applicazione a 1.000 server in meno di 3 minuti*
- L'attività CloudIQ è stata completata il 99% più velocemente rispetto a una revisione manuale*.
- CloudIQ ha ridotto il tempo di 98 ore per completare l'attività una volta*.
- L'utilizzo dell'automazione di CloudIQ Cybersecurity consente di risparmiare subito oltre una settimana di lavoro rispetto alla procedura manuale*
- Una volta abilitato, CloudIQ continua a monitorare regolarmente tutte queste impostazioni chiave di configurazione della sicurezza

*Risultati previsti in base all'analisi dei risultati di 1 e 10 server, i risultati dei clienti possono variare

Nel test di laboratorio abbiamo rilevato che il controllo manuale di 15 impostazioni nell'interfaccia grafica utente di iDRAC ha richiesto 5 minuti e 56 secondi, contro i soli 2 minuti e 58 secondi necessari per la creazione di una policy di sicurezza informatica CloudIQ costituita da 15 elementi di test attivi e la selezione dei server di destinazione. Inoltre, l'attività di creazione della policy ha richiesto la stessa quantità di tempo per 1, 10, 100 o 1.000 server. Tuttavia, utilizzando il processo manuale, ogni ulteriore server ha aggiunto altri 5 minuti e 56 secondi per completare i controlli. Inoltre, dopo aver impostato la policy, CloudIQ continua a controllare le impostazioni effettive dei server per verificarne la conformità.

Riepilogo dei risultati

Dato che il tempo impiegato è inferiore, il grafico seguente evidenzia le differenze tra automazione e processo manuale, rilevando il notevole risparmio di tempo grazie all'automazione.



Per vedere i dati completi dei risultati fare riferimento alla Tabella 1 alla fine del documento.

Panoramica dei test

Per dimostrare la facilità d'uso e l'impatto dell'automazione abbiamo testato due approcci diversi, procedendo a un confronto tra manuale e automazione. Per utilizzare questa funzionalità di sicurezza informatica di CloudIQ occorre che OpenManage Enterprise 3.9 "OME" o versione successiva sia installato con il plug-in CloudIQ 1.1 o versione successiva abilitato, i server PowerEdge siano coperti da Dell Pro Support e che OME abbia già rilevato i server di destinazione per la policy. Per creare la policy, l'utente deve disporre dei diritti di amministratore CyberSec assegnati in CloudIQ. Alcune delle regole di configurazione utilizzate nella policy di protezione del test sono i valori predefiniti di iDRAC. Tuttavia, agli amministratori con i diritti corretti è possibile modificare uno qualsiasi di questi valori in un singolo iDRAC, aprendo un punto debole a livello di sicurezza.

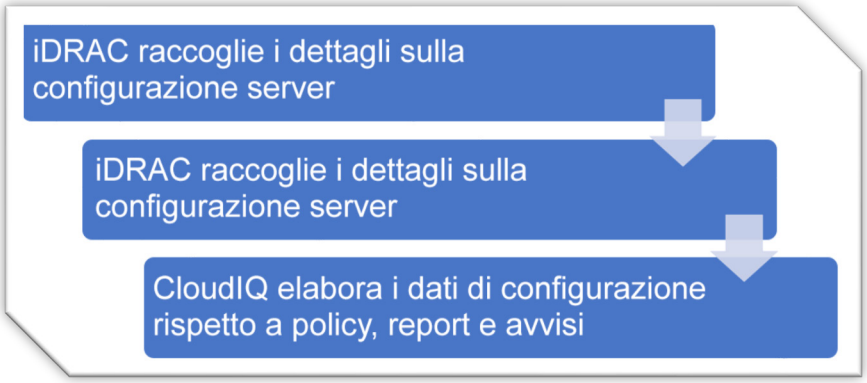


Figura 2 Flusso di dati di configurazione

Procedura di test

Per garantire un confronto accurato degli approcci ai test abbiamo provato e documentato con estremo rigore i nostri test. Abbiamo selezionato 15 impostazioni comuni, una combinazione di valori di configurazione del BIOS e dell'iDRAC e abilitato 15 test nella policy di prova. I test sono stati condotti il 6 luglio 2022 all'interno di Dell Austin nella struttura del laboratorio di marketing tecnico e online utilizzando l'offerta CloudIQ di Dell.

I. Porte USB: disabilitate
II. Scheda di rete attiva per iDRAC: dedicata
III. Blocco del sistema: abilitato
IV. Configurazione iDRAC dall'host: disabilitata
V. IPMI su LAN: disabilitata
VI. Avvio sicuro: abilitato
VII. Policy password: efficace
VIII. VNC: disabilitato
IX. SNMP versione 3: abilitato
X. SSH: disabilitato
XI. Syslog: abilitato
XII. Autenticazione Active Directory: abilitata
XIII. Blocco IP: abilitato
XIV. Supporti virtuali crittografati: abilitati
XV. Sincronizzazione dell'ora NTP: abilitata

Passaggi per un approccio automatizzato con la policy di sicurezza informatica di CloudIQ PowerEdge

A partire dalla "pagina di accesso" di CloudIQ https://cloudiq.emc.com:

1. Effettua l'accesso a CloudIQ
2. Dal menu in basso a sinistra della schermata seleziona Sicurezza informatica
3. Seleziona Policy
4. Seleziona la scheda Modelli
5. Seleziona Aggiungi modello
6. Nome modello
7. Seleziona PowerEdge dal menu a discesa del prodotto, quindi clicca su Avanti
8. Nel piano di valutazione del modello, configura quanto segue
9. Controllo degli accessi - selezionato: il blocco IP è abilitato/SSH è disabilitato/L'SNMP configurato per l'autenticazione V3/Active Directory è abilitato/VNC disabilitato
10. Responsabilità e verifica - selezionato: sincronizzazione dell'ora NTP abilitata/ Syslog remoto abilitato
11. Configuration Management - selezionato: configurare iDRAC da Post/blocco del sistema abilitato/porte USB disabilitate
12. Identificazione e autenticazione - selezionato: la password ha un punteggio minimo di complessità
13. Protezione del sistema e delle comunicazioni - selezionato: IPMI su LAN disabilitata/crittografia dei supporti virtuali abilitata/scheda di rete dedicata
14. Sistema e informazioni - avvio sicuro abilitato
15. Seleziona fine
16. Seleziona scheda sistemi
17. Seleziona gli host richiesti dall'elenco degli host (nel nostro test abbiamo selezionato un elenco di 1, 10, 100 o 1.000)
18. Clicca su Assegna
19. Seleziona il modello necessario dal menu a discesa dell'elenco dei modelli
20. Dal menu in basso a sinistra della schermata seleziona il rischio di sistema per visualizzare i risultati

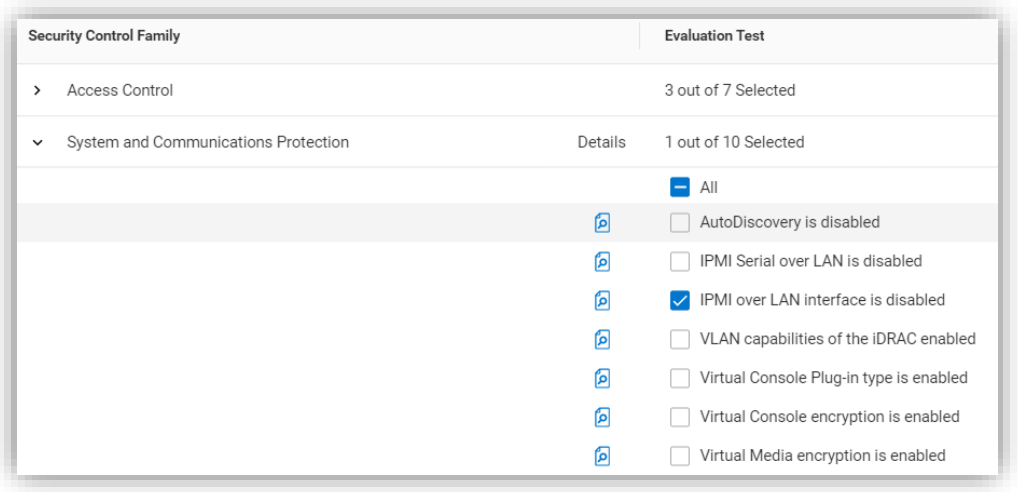


Figura 3 Selezione delle regole per creare una policy

Passaggi per la procedura manuale per il controllo dei valori di configurazione nella GUI iDRAC

Da un browser che mostra la schermata di accesso iDRAC:

1. Accedi
2. USB – Configurazione/impostazioni BIOS/dispositivi integrati/porte USB accessibili dall'utente: tutte le porte disattivate
3. Avvio sicuro – Configurazione/impostazioni BIOS/TPM avanzato /avvio sicuro: abilitato
4. VNC – Configurazione/Console virtuale/Server VNC/Abilita server VNC: disabilitato
5. SNMPv3 – Configurazione /Impostazione di sistema/Configurazione avvisi/Trap SNMP/Impostazione SNMP/Formato trap SNMP: SNMP v3
6. Syslog – Configurazione/Impostazioni di sistema/Configurazione avvisi/Impostazioni syslog remoto/Syslog remoto: abilitato
7. Crittografia dei supporti virtuali – Configurazione/Supporti virtuali/Supporti collegati/Crittografia dei supporti virtuali: abilitata
8. Porta dedicata – Impostazioni iDRAC: interfaccia scheda di rete attiva: dedicata
9. Configurazione iDRAC locale: Impostazioni iDRAC/Servizi/Configurazione locale/Disabilita configurazione iDRAC locale: abilitata
10. IPMI – Impostazioni iDRAC/Connettività/Rete/Impostazioni IPMI/Abilita IPMI su LAN: disabilitata
11. Policy password – Impostazioni iDRAC/Utenti/Impostazioni utenti globali/Punteggio/policy/impostazione password: di tipo complesso[1]
12. Autenticazione AD – Impostazioni iDRAC/Utenti/Servizi directory/Microsoft AD: abilitata
13. SSH – Impostazioni iDRAC/Servizi/SSH/Abilitato: disabilitato
14. Blocco IP – Impostazioni iDRAC/Connettività/Rete/Impostazione di rete avanzata/Blocco IP/Blocco: abilitato
15. Sincronizzazione dell'ora NTP – Impostazioni iDRAC/Impostazioni/Fuso orario/Server NTP/Abilita NTP: abilitata
16. Blocco – l'icona del lucchetto in alto a destra dello schermo mostra la modalità di blocco

Testato utilizzando il BIOS 2.12.2 e il firmware iDRAC9 di Dell PowerEdge R540: 5.10.00.00

1. L'applicazione manuale della policy efficace per le password garantisce la conformità delle nuove password con la policy delle password; tuttavia, gli account preesistenti potrebbero comunque avere password vulnerabili che contrassegnano cloudIQ come qualsiasi iDRAC con password debole.

Risultati

Numero di server	Policy di CloudIQ Cybersecurity	Controllo manuale
1	2 min e 58 sec	5 min e 56 sec
10	2 min e 58 sec	59 min
100	2 min e 58 sec	9 ore e 53 minuti*
500	2 min e 58 sec	49 ore e 26 minuti*
1000	2 min e 58 sec	98 ore e 53 minuti*

Tabella 1 – Risultati dei test

*Risultati previsti in base all'analisi dei risultati di 1 e 10 server, i risultati dei clienti possono variare

Riepilogo

I nostri test hanno dimostrato che l'automazione con Dell CloudIQ per il policy engine di sicurezza informatica PowerEdge ha apportato importanti vantaggi in termini di efficienza del tempo, ripetibilità, prevedibilità e, naturalmente, tranquillità. I vantaggi hanno evidenziato un netto aumento anche quando abbiamo estrapolato il numero di server nei dati di test.

Riferimenti

CloudIQ su Dell.com: per data sheet e video demo

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