Dell CloudIQ Cybersecurity für PowerEdge: Die Vorteile der Automatisierung

Zusammenfassung

Infrastrukturteams von Kunden stehen zahlreiche Servereinstellungen zur Verfügung, um Server zu härten und so vor zunehmenden Cyberbedrohungen zu schützen. Wo aber finden sie die von Dell empfohlenen Sicherheitskonfigurationseinstellungen und wie können sie effizient und kontinuierlich überprüfen, ob die Einstellungen falsch konfiguriert oder geändert wurden? Die Antwort auf diese Fragen ist das Cybersicherheitsfeature der AIOps-Lösung „CloudIQ für PowerEdge“. Dieses Feature vergleicht die Konfiguration bereitgestellter PowerEdge-Server mit einer sicherheitsbezogenen Konfigurationsrichtlinie. Wenn CloudIQ eine Abweichung zwischen der tatsächlichen und der empfohlenen Konfigurationseinstellung erkennt, benachrichtigt CloudIQ den/die AdministratorIn und empfiehlt Problembehandlungsschritte.

In diesem technischen Hinweis von Direct from Development (DfD) wird beschrieben, welche Zeiteinsparungen Kunden durch die Verwendung der automatisierten Cybersicherheits-Policy Engine von CloudIQ erzielen können – verglichen mit der manuellen Compliancеprüfung.

Autoren

Mark Maclean
Technical Marketing Engineering

Kyle Shannon
Produktmanagement

Version 1.1, Juli 2022

Einführung

In einer Welt der ständigen Verfügbarkeit und Konnektivität müssen Organisationen ihre Cybersicherheitsstrategie heutzutage kontinuierlich verbessern, um die wachsende Gefahr eines Angriffs zu minimieren. Mit dem integrierten Cybersicherheitsfeature von Dell CloudIQ können Kunden auf einfache Weise Sicherheitsrichtlinien für den Schutz von PowerEdge-Servern erstellen. Eine Richtlinie besteht aus vorgefertigten Tests, die Kunden ganz einfach durch Aktivieren eines Kontrollkästchens aktivieren können. Die Tests enthalten Sicherheitseinstellungen für die Infrastruktur, die auf den Best Practices von Dell sowie auf dem NIST Cybersecurity Framework (National Institute of Standards and Technology) basieren. Dell CloudIQ-Cybersicherheit für PowerEdge ermöglicht sowohl die mühelose Erstellung einer Richtlinie als auch die Automatisierung der Richtlinienüberwachung, was die Lösung einfach, effizient und zuverlässig macht.

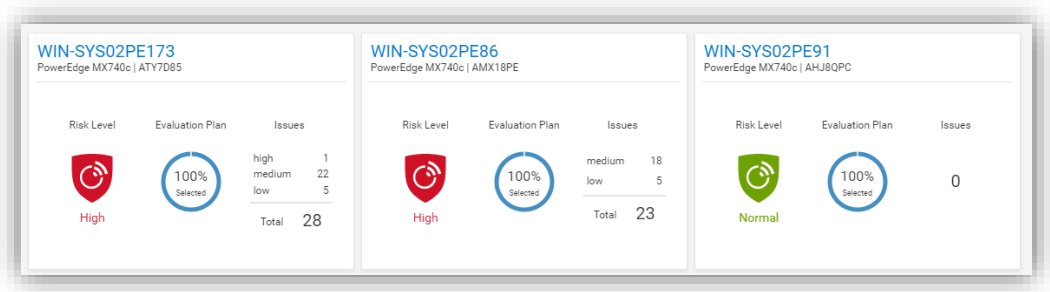


Abbildung 1: Cybersicherheitsdashboard von CloudIQ

CloudIQ ist die proaktive AIOPs-Anwendung für Monitoring und Analysen, die Einblicke in die Systemintegrität gibt und Empfehlungen für Dell Infrastrukturlösungen wie Speicher, Data Protection, Netzwerk und natürlich PowerEdge-Server bereitstellt. Die in CloudIQ integrierte Cybersicherheits-Policy Engine verfügt über mehr als 30 Sicherheitskonfigurationsregeln für PowerEdge, die ganz einfach implementiert werden können. CloudIQ ist Cloud-basiert und kann daher über das OME-CloudIQ-Plug-in mit einer beliebigen Anzahl von OME-Instanzen (OpenManage Enterprise) in verschiedenen Rechenzentren integriert werden. Somit kann CloudIQ die gleiche Richtlinie auf mehrere von OME verwaltete Server anwenden – ganz gleich, wo sich diese befinden. Dieses Feature wird von CloudIQ ohne zusätzliche Konfiguration auf iDRAC- oder OME-Ebene bereitgestellt. Nachdem eine Richtlinie eingerichtet wurde, prüft CloudIQ kontinuierlich den gewünschten Zustand der PowerEdge-Sicherheitskonfigurationseinstellungen anhand des aktuellen Ist-Zustands der Konfiguration. Ergibt die Überprüfung, dass ein Server nicht richtlinienkonform ist, wird er hervorgehoben. Die Ergebnisse werden von CloudIQ bewertet. Besonders anfällige Server erhalten dabei eine hohe Risikostufe. Einzelne Probleme können zusammen mit einer empfohlenen Korrektur angezeigt werden. Diese empfohlenen Korrekturen für die Sicherheitskonfiguration können dann pro Server 1:1 über die grafische iDRAC-Benutzeroberfläche implementiert werden. Sollten mehrere Hosts als nicht richtlinienkonform erkannt werden, kann OME verwendet werden, um eine Vorlagendatei für die Konfigurationsaktualisierung bereitzustellen oder ein RACADM-Skript auszuführen, das die Sicherheitskonfigurationen für mehrere Server korrigiert.

Die Vorteile der Automatisierung

Um die tiefgreifenden Auswirkungen der Automatisierung dieses Prozesses zu verstehen, haben wir ihn einem manuellen Prozess für einen, zehn, 100* und 1.000* Server gegenübergestellt. Basierend auf den Tests des CloudIQ Cybersecurity-Ansatzes für einen Kunden mit 1.000* Servern haben wir Folgendes festgestellt:

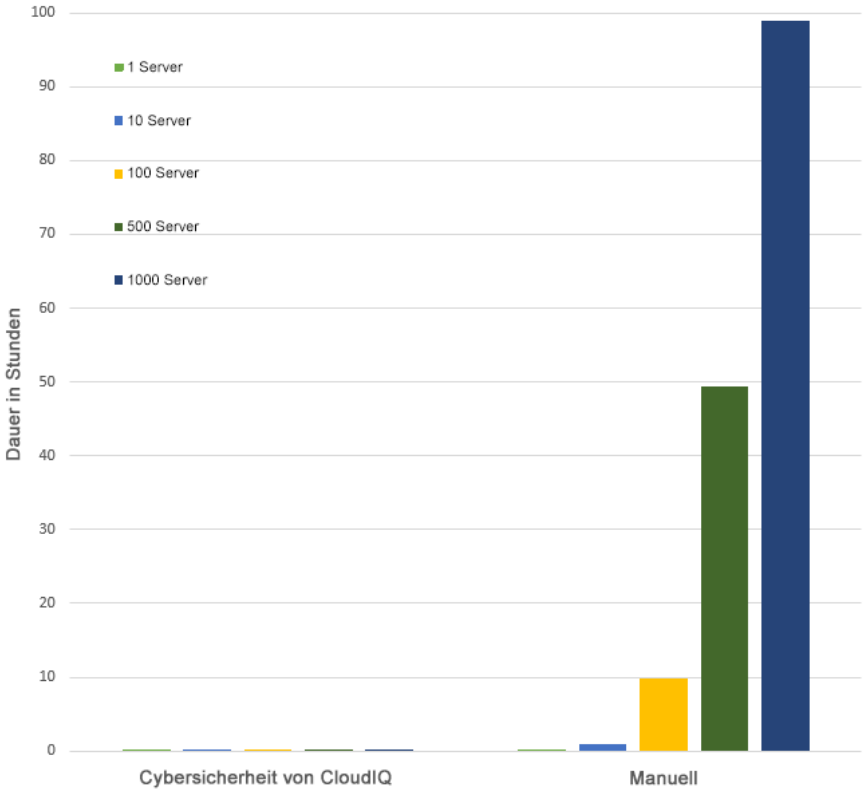
- Sie können in weniger als drei Minuten eine Richtlinie mit 15 Tests erstellen und auf 1.000 Server anwenden.*
- Die CloudIQ-Aufgabe war um 99 Prozent schneller als eine manuelle Überprüfung.*
- Mit CloudIQ hat sich die Zeit für die einmalige Durchführung der Aufgabe um 98 Stunden verkürzt.*
- Durch die Verwendung der Cybersicherheitsautomatisierung von CloudIQ verringert sich der Aufwand im Vergleich zur manuellen Durchführung sofort um über eine Woche.*
- Nach der Aktivierung werden alle diese wichtigen Sicherheitskonfigurationseinstellungen weiterhin regelmäßig von CloudIQ überwacht.

* Prognostizierte Ergebnisse basierend der Analyse der Ergebnisse mit einem Server und zehn Servern. Kundenergebnisse können variieren.

Bei den Labortests haben wir festgestellt, dass die manuelle Überprüfung von 15 Einstellungen über die grafische iDRAC-Benutzeroberfläche fünf Minuten und 56 Sekunden dauerte, während die Erstellung einer CloudIQ-Cybersicherheitsrichtlinie mit 15 aktiven Testelementen und das Auswählen der Zielserver lediglich zwei Minuten und 58 Sekunden dauerte. Darüber hinaus dauerte die Erstellung der Richtlinie für einen, zehn, 100 oder 1.000 Server immer gleich lang. Beim manuellen Prozess kamen dagegen für jeden zusätzlichen Server weitere fünf Minuten und 56 Sekunden hinzu, um die Prüfungen abzuschließen. Nach dem Festlegen der Richtlinie überprüft CloudIQ außerdem weiterhin den Ist-Zustand der Servereinstellungen auf Compliance.

Ergebniszusammenfassung

Schneller ist bekanntlich besser. Das folgende Diagramm hebt die Unterschiede zwischen Automatisierung und manuellem Prozess hervor und veranschaulicht die erhebliche Zeitersparnis durch die Automatisierung.



Die vollständigen Ergebnisdaten finden Sie in Tabelle 1 am Ende dieses Dokuments.

Testübersicht

Zur Veranschaulichung der Benutzerfreundlichkeit und der Auswirkungen der Automatisierung haben wir zwei verschiedene Ansätze getestet: manuell und automatisiert. Um dieses Cybersicherheitsfeature von CloudIQ nutzen zu können, muss mindestens OpenManage Enterprise 3.9 (OME) installiert und das CloudIQ-Plug-in 1.1 (oder höher) aktiviert sein. Außerdem müssen die PowerEdge-Server über Dell ProSupport verfügen und die Zielserver für die Richtlinie bereits von OME erkannt worden sein. Zum Erstellen der Richtlinie müssen NutzerInnen in CloudIQ die CyberSec-Administratorrechte zugewiesen sein. Bei einigen der Konfigurationsregeln, die in der Testsicherheitsrichtlinie verwendet werden, handelt es sich um die iDRAC-Standardwerte. Alle diese Werte können jedoch von AdministratorInnen mit entsprechenden Rechten für einen einzelnen iDRAC geändert werden, wodurch unter Umständen eine Sicherheitslücke entsteht.

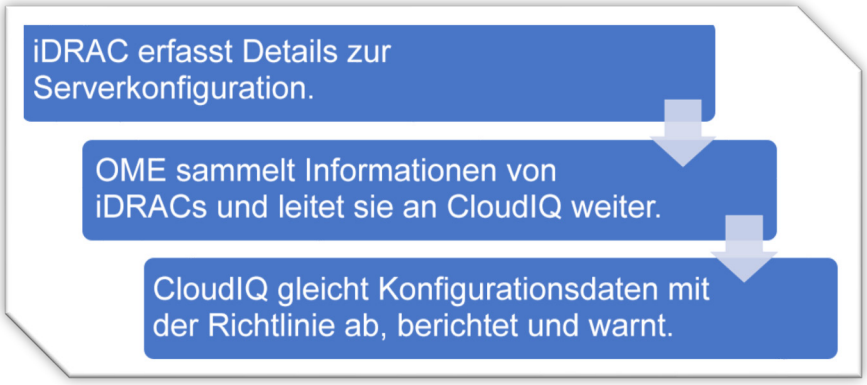


Abbildung 2: Konfigurationsdatenfluss

Testverfahren

Um einen präzisen Vergleich der Testansätze zu ermöglichen, haben wir unsere Tests streng getestet und dokumentiert. Wir haben 15 allgemeine Einstellungen mit einer Mischung aus BIOS- und iDRAC-Konfigurationswerten ausgewählt und 15 Tests in der Testrichtlinie aktiviert. Die Tests wurden intern bei Dell Austin im Labor für technisches Marketing sowie online mithilfe des CloudIQ-Angebots vom 6. Juli 2022 durchgeführt.

I. USB-Anschlüsse: Deaktiviert
II. Aktive iDRAC-NIC: Dediziert
III. Systemsperre: Aktiviert
IV. iDRAC-Konfiguration über Host: Deaktiviert
V. IPMI über LAN: Deaktiviert
VI. Secure Boot: Aktiviert
VII. Kennwortrichtlinie: Sicher
VIII. VNC: Deaktiviert
IX. SNMP-Version 3: Aktiviert
X. SSH: Deaktiviert
XI. Syslog: Aktiviert
XII. Active Directory-Authentifizierung: Aktiviert
XIII. IP-Blockierung: Aktiviert
XIV. Virtuelle Datenträger verschlüsselt: Aktiviert
XV. NTP-Zeitsynchronisation: Aktiviert

Schritte für einen automatisierten Ansatz mit Cybersicherheitsrichtlinie von CloudIQ für PowerEdge

Beginnen Sie auf der Anmeldeseite von CloudIQ https://cloudiq.emc.com:

1. Melden Sie sich bei CloudIQ an.
2. Wählen Sie im Menü auf der linken Seite des Bildschirms die Option „Cybersicherheit“ aus.
3. Wählen Sie „Richtlinie“ aus.
4. Wählen Sie die Registerkarte „Vorlagen“ aus.
5. Wählen Sie „Vorlage hinzufügen“ aus.
6. Benennen Sie die Vorlage.
7. Wählen Sie im Dropdownmenü mit den Produkten die Option „PowerEdge“ aus und klicken Sie auf „Weiter“.
8. Konfigurieren Sie in der Vorlage für den Bewertungsplan Folgendes:
9. Zugriffskontrolle (Häkchen): IP-Blockierung ist aktiviert. SSH ist deaktiviert. SNMP ist für V3 konfiguriert. Active Directory-Authentifizierung ist konfiguriert. VNC ist deaktiviert.
10. Audit und Verantwortlichkeit (Häkchen): NTP-Zeitsynchronisation ist aktiviert. Remote-Syslog ist aktiviert.
11. Konfigurationsmanagement (Häkchen): iDRAC-Konfiguration über POST ist aktiviert. Systemsperre ist aktiviert. USB-Anschlüsse sind deaktiviert.
12. Identifizierung und Authentifizierung (Häkchen): Das Kennwort muss mindestens als sicher eingestuft werden.
13. System- und Kommunikationsschutz (Häkchen): IPMI über LAN ist deaktiviert. Verschlüsselung virtueller Medien ist aktiviert. Dedizierte NIC
14. System und Informationen: Secure Boot ist aktiviert.
15. Wählen Sie „Fertig stellen“ aus.
16. Wählen Sie die Registerkarte „Systeme“ aus.
17. Wählen Sie in der Hostliste die erforderlichen Hosts aus. (In unserem Test haben wir eine Liste mit einem Server bzw. mit zehn, 100 oder 1.000 Servern ausgewählt.)
18. Klicke auf "Assign" (Zuweisen).
19. Wählen Sie im Dropdownmenü mit der Vorlagenliste die benötigte Vorlage aus.
20. Wählen Sie unten im Menü auf der linken Seite des Bildschirms die Option „Systemrisiko“ aus, um die Ergebnisse anzuzeigen.

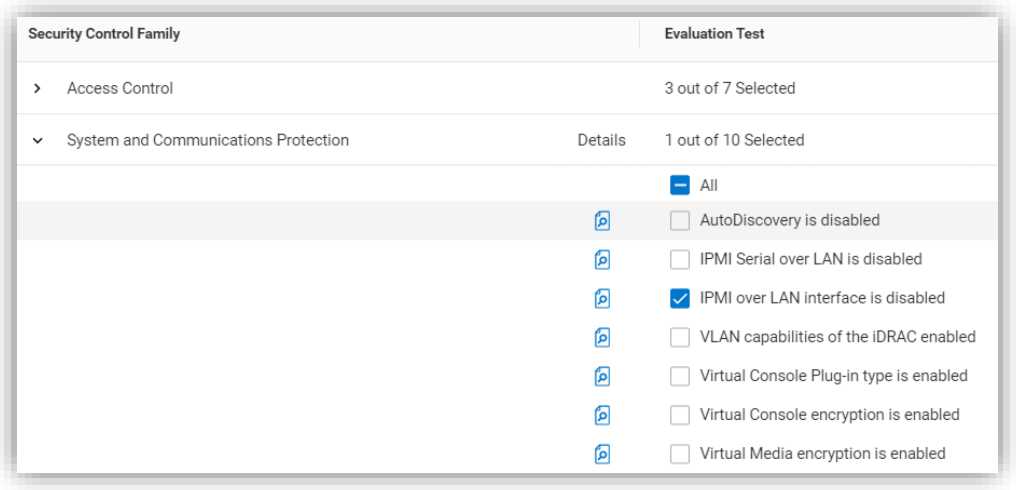


Abbildung 3: Auswählen von Regeln für die Richtlinienerstellung

Schritte für die manuelle Überprüfung von Konfigurationswerten auf der grafischen iDRAC-Benutzeroberfläche

Gehen Sie in einem Browser mit angezeigtem iDRAC-Anmeldebildschirm wie folgt vor:

1. Anmelden
2. USB – Konfiguration/BIOS-Einstellungen/integrierte Geräte/für Nutzer zugängliche USB-Anschlüsse: Alle Anschlüsse deaktiviert
3. Secure Boot – Konfiguration/BIOS-Einstellungen/TPM (erweitert)/Secure Boot: Aktiviert
4. VNC – Konfiguration/virtuelle Konsole/VNC-Server/VNC-Server aktivieren: Deaktiviert
5. SNMPv3 – Konfiguration/Systemeinstellungen/Warnungskonfiguration/SNMP-Trap/SNMP-Einstellung/SNMP-Trap-Format: SNMP v3
6. Syslog – Konfiguration/Systemeinstellungen/Warnungskonfiguration/Einstellungen für Remote-Syslog/Remote-Syslog: Aktiviert
7. Verschlüsselung virtueller Datenträger – Konfiguration/Virtuelle Datenträger/Angeschlossene Datenträger/Verschlüsselung virtueller Datenträger: Aktiviert
8. Dedizierter Port – iDRAC-Einstellungen/Aktive NIC-Schnittstelle: Dediziert
9. Lokale iDRAC-Konfiguration – iDRAC-Einstellungen/Services/lokale Konfiguration/Lokale iDRAC-Konfiguration deaktivieren: Aktiviert
10. IPMI – iDRAC-Einstellungen/Konnektivität/Netzwerk/IPMI-Einstellungen/IPMI über LAN aktivieren: Deaktiviert
11. Kennwortrichtlinie – iDRAC-Einstellungen/Nutzer/globale Nutzereinstellungen/Kennworteinstellung/Richtlinie/Bewertung: Sicher[1]
12. AD-Authentifizierung – iDRAC-Einstellungen/Nutzer/Verzeichnisdienste/Microsoft AD: Aktiviert
13. SSH – iDRAC-Einstellungen/Services/SSH/Aktiviert: Deaktiviert
14. IP-Blockierung – iDRAC-Einstellungen/Konnektivität/Netzwerk/Erweiterte Netzwerkeinstellung/IP-Blockierung/Blockierung: Aktiviert
15. NTP-Zeitsynchronisation – iDRAC-Einstellungen/Einstellungen/Zeitzone/NTP-Server/NTP aktivieren: Aktiviert
16. Sperre – Vergewissern Sie sich, dass das Vorhängeschlosssymbol rechts oben auf dem Bildschirm den gesperrten Modus anzeigt.

Getestet mit Dell PowerEdge R540 BIOS 2.12.2 und iDRAC9 Firmware 5.10.00.00

1. Durch die manuelle Erzwingung der Richtlinie für sichere Kennwörter wird die Konformität neuer Kennwörter mit der Kennwortrichtlinie sichergestellt. Bereits vorhandene Konten können jedoch weiterhin über unsichere Kennwörter verfügen. Von CloudIQ werden iDRACs mit unsicherem Kennwort dagegen entsprechend gekennzeichnet.

Ergebnis

Anzahl der Server	CloudIQ-Cybersicherheitsrichtlinie	Manuelle Prüfung
1	2 Min. und 58 Sek.	5 Min. und 56 Sek.
10	2 Min. und 58 Sek.	59 Min.
100	2 Min. und 58 Sek.	9 Std. und 53 Min.*
500	2 Min. und 58 Sek.	49 Std. und 26 Min.*
1000	2 Min. und 58 Sek.	98 Std. und 53 Min.*

Tabelle 1: Testergebnisse

* Prognostizierte Ergebnisse basierend der Analyse der Ergebnisse mit einem Server und zehn Servern. Kundenergebnisse können variieren.

Zusammenfassung

Unsere Tests haben gezeigt, dass die Automatisierung mit der Cybersicherheits-Policy Engine von Dell CloudIQ für PowerEdge erhebliche Vorteile in puncto zeitliche Effizienz, Wiederholbarkeit, Zuverlässigkeit und natürlich Sorgenfreiheit mit sich gebracht hat. Außerdem hat sich der Nutzen drastisch erhöht, als wir die Serveranzahl aus den Testdaten hochgerechnet haben.

Referenzen

CloudIQ auf Dell.com (Datenblätter und Demovideos)

Behalten Sie stets die Kontrolle über Ihre Cybersicherheit – mit intelligentem Cloud-basiertem Monitoring (Blog)

Erstellen und Nachverfolgen von Dell CloudIQ-Cybersicherheitsrichtlinien für PowerEdge-Server (Video)

Seite mit technischen Informationen für das OpenManage Enterprise-CloudIQ-Plug-in

Weitere Cybersicherheitslösungen von Dell