Verbessern der Cybersicherheit von Servern mit Dell CloudIQ

Zusammenfassung

Ein über mehrere Jahre aufgebauter guter Ruf bei Kunden kann durch einen Cybersicherheits-Incident innerhalb weniger Minuten zunichte gemacht werden. Cybersicherheitsteams und ServeradministratorInnen müssen jedes ihnen zur Verfügung stehende Tool nutzen, um die Infrastruktur zu härten. Hier finden Sie Informationen zu einem Feature von Dell CloudIQ, das jeder Dell PowerEdge-Kunde kennen sollte.

In diesem technischen Hinweis von Direct from Development (DfD) werden die in CloudIQ integrierten Cybersicherheitsfunktionen für PowerEdge-Server beschrieben.

CloudIQ ist eine Cloud- und KI-/ML-basierte Anwendung für Monitoring und vorausschauende Analysen für das Infrastrukturproduktportfolio von Dell. CloudIQ wird in der Dell IT-Cloud gehostet und erfasst und analysiert die Integrität und Leistung sowie Telemetriedaten, um Risiken zu ermitteln und Maßnahmen für eine schnelle Problemlösung zu empfehlen.

Autor

Mark Maclean
Technical Marketing Engineering

Kyle Shannon
Produktmanagement

Version 1.1, Juli 2022

Einführung

Dell CloudIQ bietet ein Cybersicherheitsfeature, das jetzt auch Dell PowerEdge-Server umfasst. Mit dem in CloudIQ integrierten Cybersicherheitsfeature können Serverteams von Kunden eine als Bewertungsplan bezeichnete Richtlinie erstellen. Diesem Bewertungsplan liegt eine Reihe vorgefertigter Tests für Konfigurationskriterien zugrunde, die mit nur einem Klick ausgewählt werden können. Die Liste der Konfigurationseinstellungen und -werte basiert auf den Best Practices von Dell sowie auf dem NIST Cybersecurity Framework (National Institute of Standards and Technology).

Ein Ansatz für schnelle Ergebnisse

SpezialistInnen mit den richtigen Fähigkeiten, der die exakten Sicherheitskonfigurationseinstellungen mit korrekten Werten verstehen, können ein Serverkonfigurationsprofil (Server Configuration Profile, SCP) erstellen und es direkt mit dem iDRAC- oder OME-Konfigurationsvorlagenfeature verwenden, um Serverkonfigurationen festzulegen. CloudIQ bietet jedoch eine viel schnellere vorgefertigte Methode zum Implementieren einer Cybersicherheitsbewertungsrichtlinie, die auf den von Dell empfohlenen Einstellungen und Werten basiert. Zur weiteren Optimierung des Cybersicherheitsprozesses kann CloudIQ mehrere OME-Instanzen aggregieren und eine konsolidierte Serveransicht für zahlreiche Standorte bereitstellen. Organisationen können eine Kombination von OME und CloudIQ nutzen, um Konfigurationscompliance und Sicherheitsverwaltung getrennt zu behandeln.

Abbildung 1: Zusammenfassung des Cybersicherheitsstatus auf der CloudIQ-Übersichtsseite

Die oben gezeigte Cybersicherheitskachel auf der CloudIQ-Übersichtsseite bietet eine Statusansicht mit aggregierter Risikostufe sowie eine Aufschlüsselung der Anzahl von Systemen in den einzelnen Risikokategorien und der Gesamtanzahl erkannter Probleme. Das Risiko wird anhand des Schweregrads und der Anzahl von Problemen pro Server bestimmt. Ein Server mit einem oder mehreren hochriskanten Problemen wird also beispielsweise als hohes Risiko kategorisiert. Gleiches gilt für einen Server mit mehr als fünf nicht hohen Risiken, von denen mindestens eines ein mittelschweres Problem ist.

Schnelles Identifizieren von Risiken

Auf dem Systemrisiko-Dashboard wird jeder Server mit einer angewendeten Richtlinie klassifiziert und jeweils auf einer eigenen Karte mit dem Status der Cybersicherheitsrisikostufe angezeigt. Das hilft Kunden dabei, Maßnahmen schnell zu priorisieren und die Problemlösung zu beschleunigen.

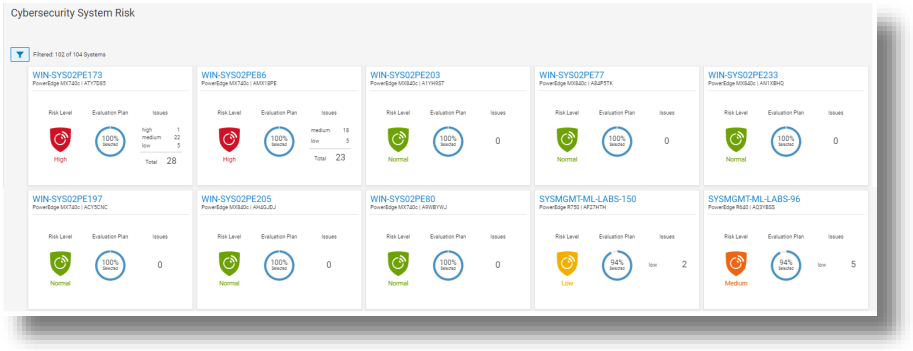

Abbildung 2: Dashboard „Cybersicherheitsrisiko für Systeme“: Alle Systeme

Zusätzlich zum Dashboard zeigt der Status der Sicherheitsbewertung die Details für jeden Server mit empfohlener Maßnahme an, um abweichende Sicherheitskonfigurationen wieder in den bevorzugten Zustand zu versetzen. Das Ringdiagramm zeigt, wie viele Regeln (in Prozent) aus den Gesamttests in dem Risikobewertungsplan ausgewählt wurden, der dem betreffenden Server zugewiesen ist.

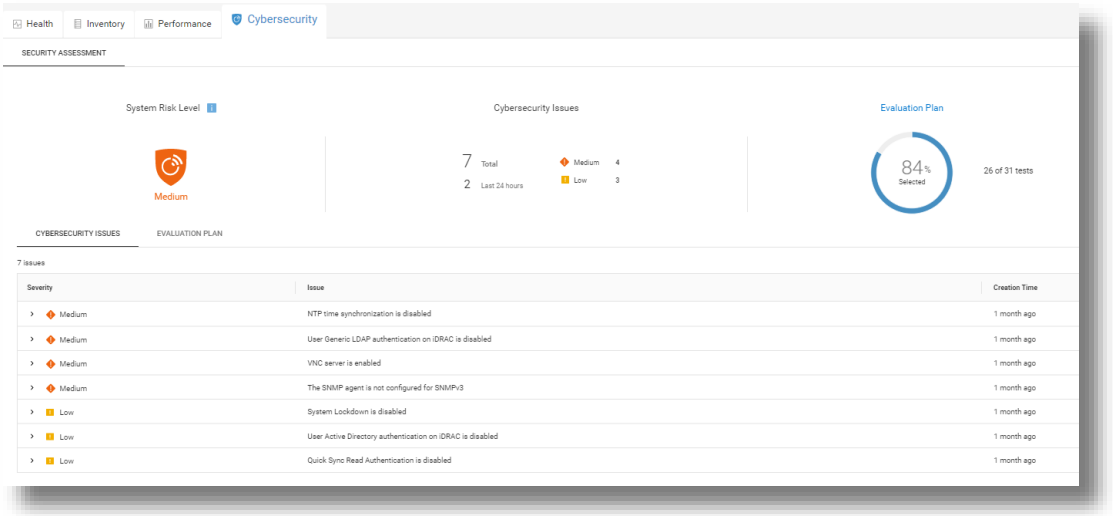

Figure 3: Details und Empfehlungen zu Cybersicherheitsrisiken

Auf der Seite mit den Systemdetails unter der Registerkarte „Cybersicherheit“ finden Sie Details zum Evaluierungsplan sowie dessen Status. Am unteren Rand der Seite befinden sich zwei Registerkarten. Die Registerkarte „Cybersicherheitsprobleme“ enthält Details zu den nicht konformen Elementen sowie Korrekturmaßnahmen und auf der Registerkarte „Bewertungsplan“ werden der gesamte Plan sowie der Auswahlstatus der einzelnen Tests angezeigt.

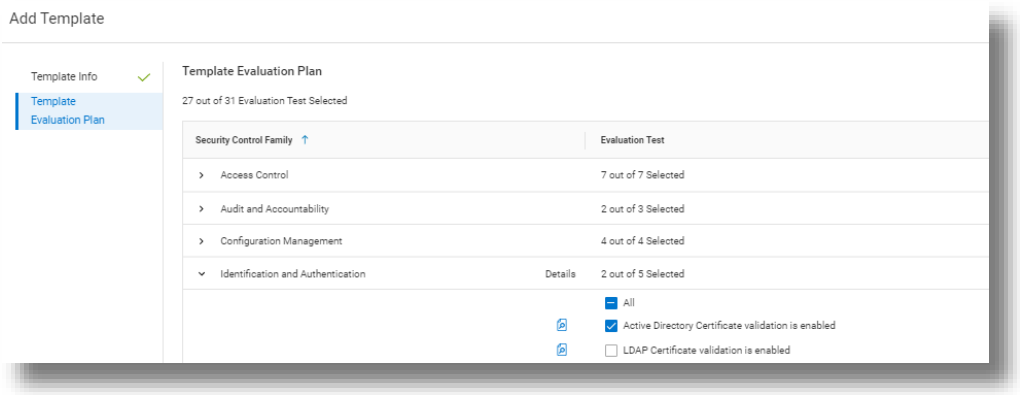

Abbildung 4: Testauswahl

CloudIQ-NutzerInnen können auch festlegen, dass sie täglich eine E-Mail mit einer Übersicht über den Cybersicherheitsstatus erhalten möchten.

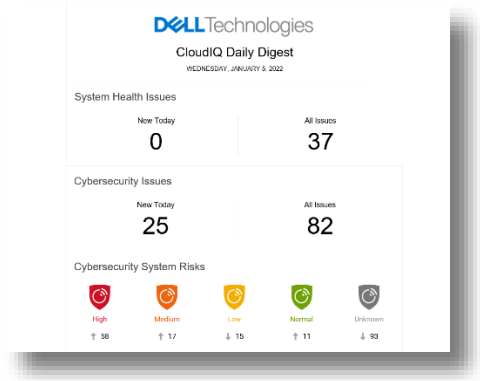

Abbildung 5: Tägliche Übersichts-E-Mail von CloudIQ

Möglichkeiten und Sicherheit

In CloudIQ sind erwartungsgemäß einige Kontrollen für sicheren Zugriff integriert. Diese basieren auf Administrator- und Benutzerkonten und dienen zur Steuerung von Erstellung und Reporting. CloudIQ verfügt über zwei integrierte Cybersicherheitsrollen: „CybersicherheitsadministratorIn“ und „CybersicherheitsviewerIn“. Diese Rollen können über Konten mit CloudIQ-Administratorrechten zugewiesen werden.

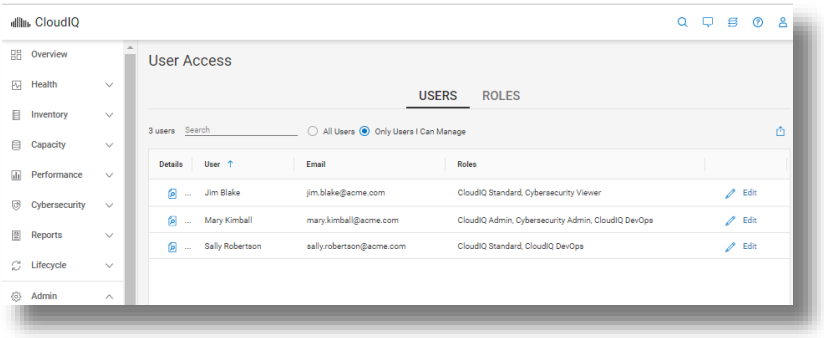

Abbildung 6: RBAC-Einrichtung

Zur Unterstützung der Cybersicherheit für PowerEdge in CloudIQ müssen Kunden mindestens über OpenManage Enterpriser 3.9 mit aktiviertem CloudIQ-Plug-in 1.1 verfügen. Alle Server benötigen Dell ProSupport-Abdeckung und müssen bereits von OME erkannt worden sein.

Testelemente des Bewertungsplans für die Cybersicherheit von PowerEdge

Die folgende Tabelle enthält die einzelnen Testkriterien sowie die Testplanfamilie, zu der sie gehören:

Produktreihe	Titel
System und Kommunikation	IPMI über LAN-Schnittstelle ist deaktiviert.
System und Kommunikation	IPMI seriell über LAN ist deaktiviert.
System und Kommunikation	Verschlüsselung der virtuellen Konsole ist aktiviert.
System und Kommunikation	Verschlüsselung virtueller Datenträger ist aktiviert.
System und Kommunikation	Automatische Erkennung ist deaktiviert.
System und Kommunikation	VLAN-Funktionen des iDRAC sind aktiviert.
System und Kommunikation	Für den iDRAC-Webserver ist TLS 1.2 oder TLS 1.3 aktiviert.
System und Kommunikation	HTTP-Anforderungen des iDRAC-Webservers werden zu HTTPS-Anforderungen umgeleitet.
System und Kommunikation	Der Plug-in-Typ „Virtuelle Konsole“ ist aktiviert.
System und Kommunikation	iDRAC verwendet die dedizierte NIC.
System und Kommunikation	Für den iDRAC-Webserver ist TLS 1.2 oder TLS 1.3 aktiviert.
Zugriffskontrolle	IP-Blockierung ist aktiviert.
Zugriffskontrolle	VNC-Server ist deaktiviert.
Zugriffskontrolle	Der SNMP-Agent ist für SNMPv3 konfiguriert.
Zugriffskontrolle	Quick Sync-Leseauthentifizierung gegenüber dem Server ist aktiviert.
Zugriffskontrolle	SSH ist deaktiviert.
Zugriffskontrolle	Generische LDAP-Benutzerauthentifizierung für iDRAC ist aktiviert.
Zugriffskontrolle	Active Directory-Benutzerauthentifizierung für iDRAC ist aktiviert.
Konfigurationsmanagement	USB-Anschlüsse sind deaktiviert.
Konfigurationsmanagement	Telnet-Protokoll ist deaktiviert.[1]
Konfigurationsmanagement	Systemsperre ist aktiviert.
Konfigurationsmanagement	Konfigurieren von iDRAC über den BIOS POST ist deaktiviert.
Audit und Verantwortlichkeit	NTP-Zeitsynchronisation ist aktiviert.
Audit und Verantwortlichkeit	NTP ist geschützt.
Audit und Verantwortlichkeit	Remote-Syslog ist aktiviert.
System- und Informationsintegrität	iDRAC-Konfiguration zum Aktivieren der lokalen Konfiguration auf dem Hostsystem ist deaktiviert.
System- und Informationsintegrität	Secure Boot ist aktiviert.
Identifizierung und Authentifizierung	Kennwort muss mindestens als sicheres Kennwort eingestuft werden.
Identifizierung und Authentifizierung	LDAP-Zertifikatvalidierung ist aktiviert.
Identifizierung und Authentifizierung	Active Directory-Zertifikatvalidierung ist aktiviert.
Identifizierung und Authentifizierung	iDRAC-Webserver: SSL-Verschlüsselung mit mindestens 256 Bit
Identifizierung und Authentifizierung	iDRAC-Webserver: SCEP aktiviert

1. Ab der iDRAC-Firmwareversion 4.40.00.00 wird die Telnet-Funktion für iDRAC entfernt.

Zusammenfassung

Im Gegensatz zu Mitgliedern des IT-Teams benötigt CloudIQ weder Schlaf noch Essenspausen oder Urlaub. Organisationen können sich also darauf verlassen, dass die Cybersicherheitsrichtlinien von CloudIQ kontinuierlich die Konformität ihrer Server überwachen. Mit der in CloudIQ integrierten Cybersicherheit können Kunden die Serversicherheit durch Automatisierung vordefinierter Tests und Statusvisualisierung beschleunigen. Dadurch erhalten ServeradministratorInnen ein hohes Maß an Flexibilität bei gleichzeitiger Gewährleistung der Governance und Kontrolle, die Cybersicherheitsteams benötigen. CloudIQ trägt zur weiteren Risikosenkung bei und verbessert die IT-Produktivität. Hierzu werden der Cybersicherheits- und der Systemintegritätsstatus der Server und des allgemeinen Dell Infrastrukturportfolios im gleichen praktischen Cloud-basierten Portal angezeigt.

Referenzen

CloudIQ auf Dell.com (Produktinformationen, Demovideos und mehr)

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