Harden Your Server Cybersecurity With Dell CloudIQ

Summary

It can take years for an organization to build a good reputation with its customers and few minutes of a cybersecurity related incident to ruin it. Cybersecurity teams and server administrators must use every tool in their armory to harden infrastructure. Here is a feature of Dell CloudIQ that every Dell PowerEdge customer should know about.

This Direct from Development (DfD) tech note describes the cybersecurity capabilities for PowerEdge servers that are built into CloudIQ.

CloudIQ is a cloud AI/ML-based monitoring and predictive analytics application for the Dell infrastructure product portfolio. Hosted in the secure Dell IT Cloud, CloudIQ collects and analyzes health, performance, and telemetry to pinpoint risks and to recommend actions for fast problem resolution.

Authors

Mark Maclean
Technical Marketing Engineering

Kyle Shannon
Product Management

Introduction

Dell CloudIQ offers a cybersecurity feature that now includes Dell PowerEdge servers. The cybersecurity feature built into CloudIQ lets customer server teams build a policy called an evaluation plan. This evaluation plan is built from a number of ready to use “click to pick” configuration criteria tests. This list of configuration settings and values is based on Dell Technologies best practices and the American NIST (National Institute of Standards and Technology) cybersecurity framework.

An approach for rapid results

A specialist with the right skills who understands the exact security configuration settings with correct values could build a server configuration profile “SCP” and use it directly with the iDRAC or OME configuration template feature to set server configurations. However, CloudIQ offers a much quicker and prescriptive method to implement a cybersecurity assessment policy that is built on Dell’s recommended settings and values. To further streamline the cybersecurity process, CloudIQ can aggregate multiple OME instances, offering one consolidated view of servers across many locations. Some organizations may choose to use both OME and CloudIQ to demonstrate the separation of configuration compliance and security management.

Figure 1. **Cybersecurity status summary from the CloudIQ Overview page**

This cybersecurity tile on the CloudIQ overview page provides an aggregated risk level status view, breaking down the number of systems in each risk category and the total number of detected issues. The risk is determined by the severity and the number of issues per server.

For example, a server with one or more high risk problems is categorized as high risk. Another server with more than five non-high risks, of which one is a medium issue, would also be categorized as high risk.

Identify risks fast

The system risk dashboard classifies each server with a policy applied, displaying each server in its own card with the cybersecurity risk level status. This helps customers quickly prioritize actions and speed time to resolution.

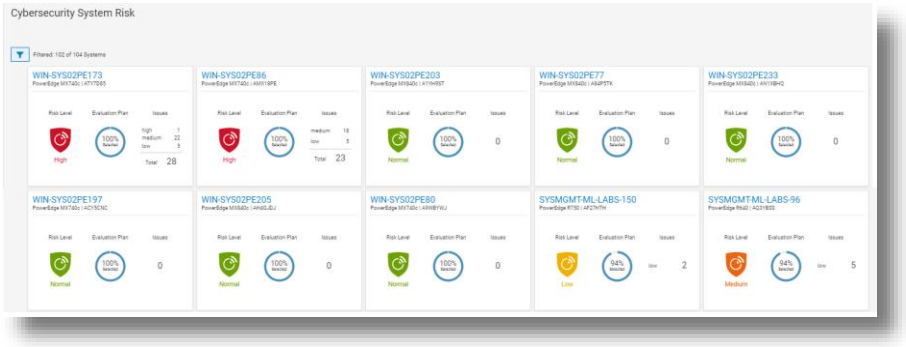

Figure 2. **Cybersecurity System Risk all systems dashboard**

Beyond the dashboard, the security assessment status displays the details for each server, with recommended action to return any deviated security configuration to the preferred state. The donut chart displays how many rules been selected as a percentage from total tests in the risk evaluation plan that are assigned to the particular server.

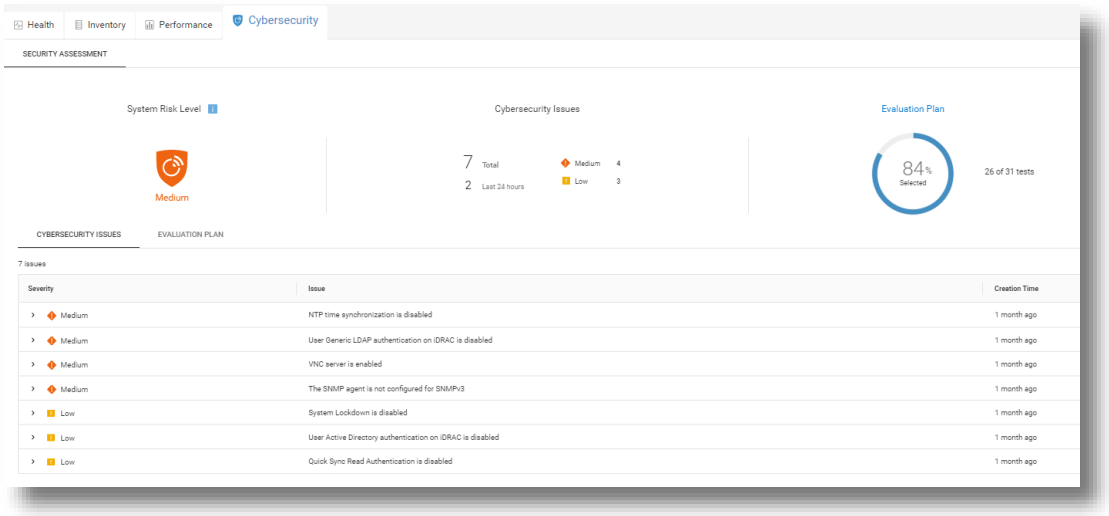

Figure 3. **Cybersecurity Risk details and recommendations**

On the system detail page, under the cybersecurity tab, are details about the evaluation plan and its status. The bottom of the page has two tabs: Cybersecurity Issues, detailing each non-compliant element with its corrective action, and Evaluation Plan, displaying the entire plan and the selection status of each test.

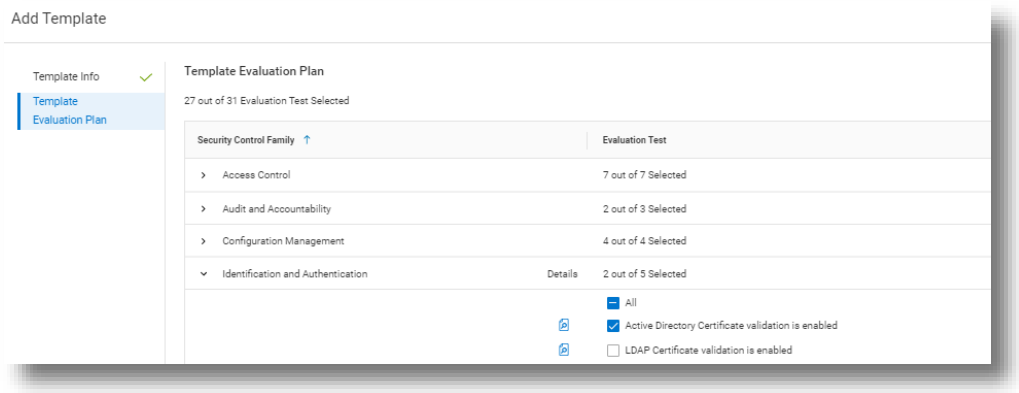

Figure 4. **Test selection**

CloudIQ users can also select to receive a Daily Digest email, including a Cybersecurity status summary.

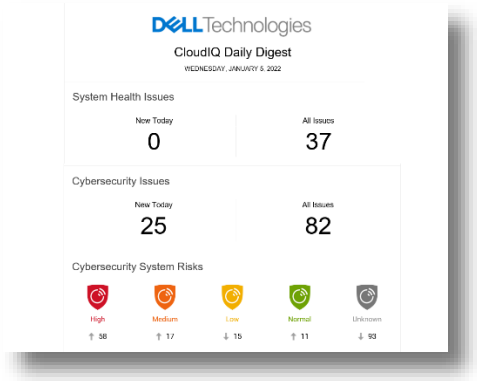

Figure 5. **CloudIQ Daily Digest email**

Enablement and security

As you would expect, many security access controls are built into CloudIQ around administrator and user accounts. There are two Cybersecurity roles built to CloudIQ: Cybersecurity Admin and Cybersecurity Viewer. These roles can be assigned from accounts that have CloudIQ administrator rights.

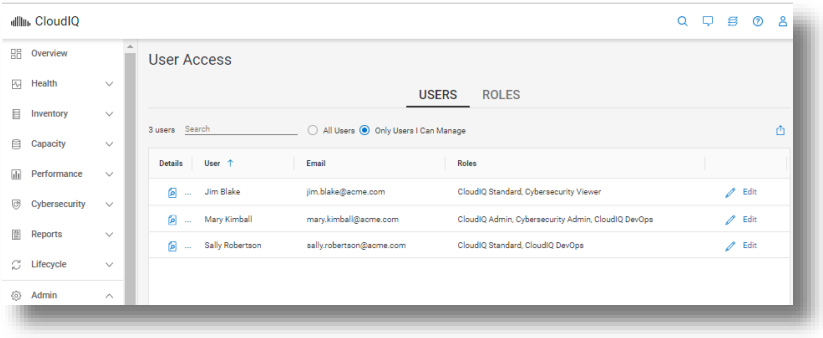

Figure 6. **RBAC setup**

To support cybersecurity for PowerEdge within CloudIQ, customers must be running OpenManage Enterprise 3.9 or higher, with the CloudIQ plugin 1.1 or higher enabled. All servers require Dell ProSupport coverage and must already be discovered by OME.

PowerEdge cybersecurity evaluation plan test elements

The following table lists each test criteria and the test plan family to which it belongs.

Family	Title
System & Communications	IPMI over LAN interface is disabled
System & Communications	IPMI Serial over LAN is disabled
System & Communications	Virtual Console encryption is enabled
System & Communications	Virtual Media encryption is enabled
System & Communications	Auto-Discovery is disabled
System & Communications	VLAN capabilities of the iDRAC are enabled
System & Communications	iDRAC Web Server has TLS 1.2 or TLS 1.3 enabled
System & Communications	iDRAC Web Server HTTP requests are redirected to HTTPS requests
System & Communications	Virtual Console Plug-in type is enabled
System & Communications	iDRAC is using the dedicated NIC
System & Communications	iDRAC Web Server has TLS 1.2 or TLS 1.3 enabled
Access Control	IP Blocking is enabled
Access Control	VNC server is disabled
Access Control	The SNMP agent is configured for SNMPv3
Access Control	Quick Sync Read Authentication to the server is enabled
Access Control	SSH is disabled
Access Control	User Generic LDAP authentication on iDRAC is enabled
Access Control	User Active Directory authentication on iDRAC is enabled
Configuration Management	USB Ports are disabled
Configuration Management	Telnet protocol is disabled[1]
Configuration Management	System Lockdown is enabled
Configuration Management	Configure iDRAC from the BIOS POST is disabled
Audit & Accountability	NTP time synchronization is enabled
Audit & Accountability	NTP is secured
Audit & Accountability	Remote Syslog is enabled
System & information integrity	Local Config Enabled iDRAC configuration on Host system is disabled
System & information integrity	Secure Boot is enabled
Identification & Authentication	Password has a minimum score of Strong Protection
Identification & Authentication	LDAP Certificate validation is enabled
Identification & Authentication	Active Directory Certificate validation is enabled
Identification & Authentication	iDRAC Webserver SSL Encryption using 256 bit or higher
Identification & Authentication	iDRAC Web Server - SCEP is enabled

[1] Starting with iDRAC firmware release version 4.40.00.00, the telnet feature is removed from iDRAC.

Summary

Unlike the typical IT team member, CloudIQ doesn't need to eat, sleep, or go on holiday, so organizations can rely on CloudIQ cybersecurity policies to continuously monitor for non-compliant servers. Cybersecurity built into CloudIQ lets customers speed up the delivery of server security through automation of pre-defined tests and status visualization. This provides high levels of flexibility for server administrators, all while maintaining the governance and control that cybersecurity teams need to enforce. CloudIQ further reduces risk and improves IT productivity by displaying cybersecurity, plus the system health status of servers, and the wider Dell infrastructure portfolio—all together in the same convenient, cloud-based portal.

References

CloudIQ on Dell.com - for product information, demo videos and more

Take Control of Server Cybersecurity with Intelligent Cloud-Based Monitoring Blog

Building and Tracking Dell CloudIQ Cybersecurity Policies for PowerEdge Servers Video

Technical Knowledge Page For OpenManage Enterprise CloudIQ Plugin

Additional Cybersecurity Related Solutions from Dell

Learn more about PowerEdge servers

Contact us for feedback and requests

Follow us for PowerEdge news