Refuerce la seguridad cibernética de sus servidores con Dell CloudIQ

Resumen

A las organizaciones les cuesta años construir una buena reputación con sus clientes y unos pocos minutos para que un incidente relacionado con la seguridad cibernética la arruine. Los equipos de seguridad cibernética y los administradores de servidores deben usar todas las herramientas de su arsenal para reforzar la infraestructura. Esta es una característica de Dell CloudIQ que todos los clientes de Dell PowerEdge deben conocer.

En esta nota técnica de Direct from Development (DfD), se describen las funcionalidades de seguridad cibernética para los servidores PowerEdge incorporadas en CloudIQ.

CloudIQ es la aplicación para análisis predictivo y monitoreo proactivo basado en la nube y en IA/ML del portafolio de productos de infraestructura de Dell. CloudIQ, alojado en la nube de TI segura de Dell, recopila y analiza el estado, el rendimiento y la telemetría para identificar los riesgos y recomendar acciones para una rápida resolución de los problemas.

Autor

Mark Maclean
Ingeniería de marketing técnico

Kyle Shannon
Administración de productos

Versión 1.1 julio de 2022

Introducción

Dell CloudIQ ofrece una característica de seguridad cibernética que ahora incluye servidores Dell PowerEdge. La característica de seguridad cibernética incorporada en CloudIQ permite a los equipos de servidores de los clientes construir una política que se denomina plan de evaluación. Este plan de evaluación se crea a partir de una serie de pruebas listas para usar sobre criterios de configuración con "clic para elegir". Esta lista de valores y ajustes de configuración se basa en las prácticas recomendadas de Dell y en la infraestructura de seguridad cibernética del NIST estadounidense (Instituto Nacional de Estándares y Tecnología).

Un enfoque para obtener resultados rápidos

Un especialista con las habilidades correctas que entienda los ajustes de configuración de seguridad exactos con los valores correctos podría crear un perfil de configuración del servidor "SCP" y usarlo directamente con la característica de plantilla de configuración de iDRAC u OME para establecer configuraciones de servidor. Sin embargo, CloudIQ ofrece un método mucho más rápido y prescriptivo para implementar una política de evaluación de seguridad cibernética basada en los valores y la configuración recomendados de Dell. Para agilizar aún más el proceso de seguridad cibernética, CloudIQ puede agregar múltiples instancias de OME, y ofrecer una vista consolidada de los servidores en muchas ubicaciones. Algunas organizaciones deciden utilizar tanto OME como CloudIQ para demostrar la separación del cumplimiento de la configuración y la administración de la seguridad.

Figura 1 Resumen del estado de seguridad cibernética en la página de visión general de CloudIQ

El mosaico de seguridad cibernética anterior, que se encuentra en la página de visión general de CloudIQ, proporciona una vista del estado del nivel de riesgo agregado y desglosa el número de sistemas en cada categoría de riesgo y el número total de problemas detectados. El riesgo está determinado por la gravedad y la cantidad de problemas por servidor. Por ejemplo, un servidor con uno o más problemas de alto riesgo se clasifica como de alto riesgo, pero un servidor con más de cinco riesgos que no son altos y que al menos uno de ellos sea un problema medio también se clasificaría como de alto riesgo.

Identifique los riesgos rápidamente

El tablero de riesgos del sistema clasifica cada servidor con una política aplicada, y muestra a cada uno de ellos en su propia tarjeta con el estado del nivel de riesgo de seguridad cibernética. Esto permite que los clientes prioricen las acciones con rapidez y aceleren el tiempo de resolución.

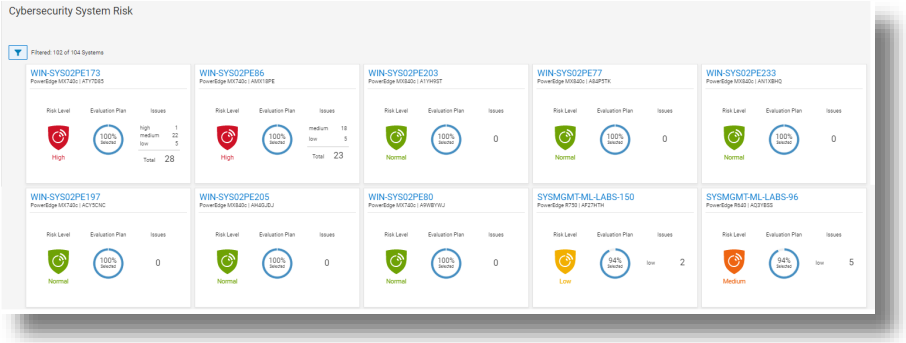

Figura 2 Riesgo del sistema de seguridad cibernética Tablero de control de todos los sistemas

Más allá del tablero, el estado de la evaluación de seguridad muestra los detalles de cada servidor con la acción recomendada para devolver cualquier configuración de seguridad desviada al estado recomendado. El gráfico de anillo muestra cuántas reglas se seleccionaron como un porcentaje de las pruebas totales en el plan de evaluación de riesgos asignado al servidor en particular.

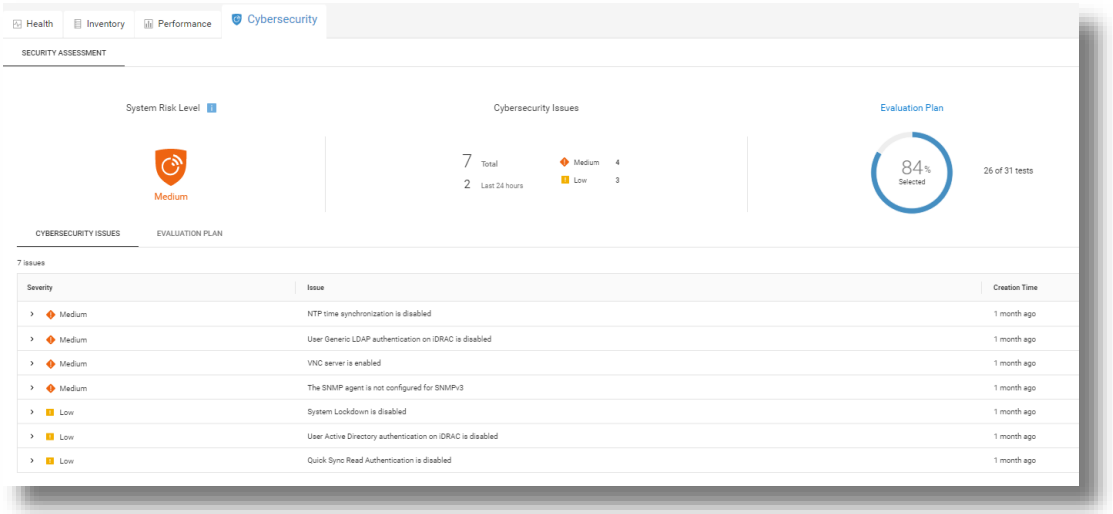

Figura 3 Detalles y recomendaciones sobre riesgos de seguridad cibernética

En la página de detalles del sistema en la pestaña seguridad cibernética, hay detalles sobre el plan de evaluación y su estado. Al final de la página hay dos pestañas: Problemas de seguridad cibernética, en la que se detallan los elementos de incumplimiento con la acción correctiva, y Plan de evaluación, en la que se muestra todo el plan y el estado de selección de cada prueba.

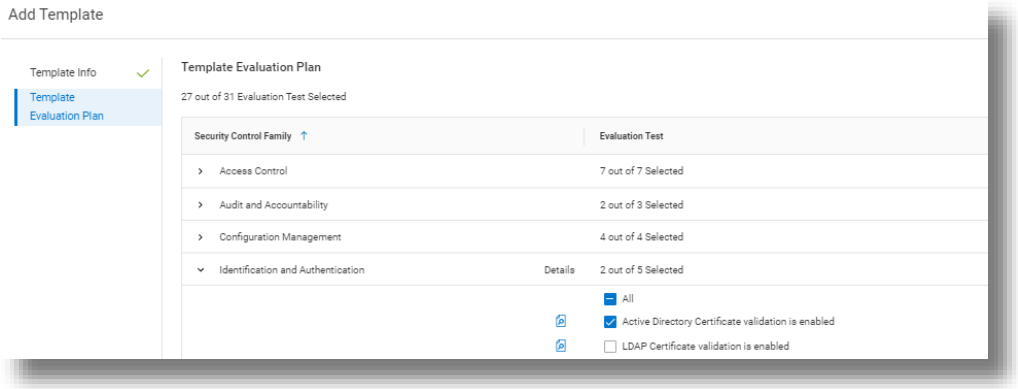

Figura 4 Selección de prueba

Los usuarios de CloudIQ también pueden optar por recibir un correo electrónico a diario con un resumen del estado de seguridad cibernética.

Figura 5 Correo electrónico diario de CloudIQ

Activación y seguridad

Como es de esperar, hay una serie de controles de acceso de seguridad incorporados en CloudIQ para las cuentas de administrador y de usuario que controlan la creación y los informes. Existen dos roles de seguridad cibernética incorporados en CloudIQ: Administrador de seguridad cibernética y Visor de seguridad cibernética. Estas funciones se pueden asignar desde cuentas con derechos de administrador de CloudIQ.

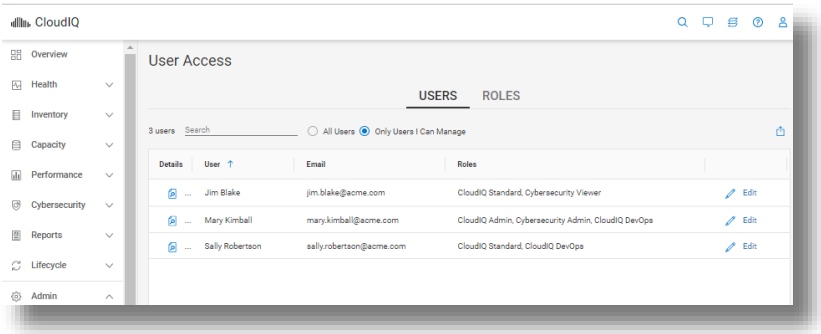

Figura 6 Configuración de RBAC

Para admitir la seguridad cibernética de PowerEdge dentro de CloudIQ, los clientes deben ejecutar OpenManage Enterpriser 3.9 o superior con el plug-in de CloudIQ 1.1 o superior habilitado. Todos los servidores requieren la cobertura de Dell ProSupport y que OME los haya detectado.

Elementos de prueba del plan de evaluación de la seguridad cibernética de PowerEdge

En la siguiente tabla, se detallan todos los criterios de prueba y la familia de planes de pruebas a los que pertenecen.

Familia	Título
Sistema y comunicaciones	La interfaz IPMI en la LAN está deshabilitada
Sistema y comunicaciones	La comunicación en serie IPMI en la LAN está deshabilitada
Sistema y comunicaciones	El cifrado de la consola virtual está habilitado
Sistema y comunicaciones	El cifrado de medios virtuales está habilitado
Sistema y comunicaciones	El descubrimiento automático está deshabilitado
Sistema y comunicaciones	Las funcionalidades de VLAN de iDRAC están habilitadas
Sistema y comunicaciones	El servidor web de iDRAC tiene TLS 1.2 o TLS 1.3 habilitado
Sistema y comunicaciones	Las solicitudes HTTP del servidor web de iDRAC se redirigen a las solicitudes HTTPS
Sistema y comunicaciones	El tipo de plug-in de la consola virtual está habilitado
Sistema y comunicaciones	iDRAC utiliza la NIC dedicada
Sistema y comunicaciones	El servidor web de iDRAC tiene TLS 1.2 o TLS 1.3 habilitado
Control de acceso	El bloqueo de IP está habilitado
Control de acceso	El servidor VNC está deshabilitado
Control de acceso	El agente SNMP está configurado para SNMPv3
Control de acceso	La autenticación de lectura de Quick Sync en el servidor está habilitada
Control de acceso	SSH está deshabilitado
Control de acceso	La autenticación LDAP genérico del usuario en iDRAC está activada
Control de acceso	La autenticación de usuario de Active Directory en iDRAC está activada
Administración de la configuración	Los puertos USB están deshabilitados
Administración de la configuración	El protocolo Telnet está deshabilitado[1]
Administración de la configuración	El bloqueo del sistema está habilitado
Administración de la configuración	La configuración de iDRAC desde la POST del BIOS está desactivada
Auditoría y responsabilidad	La sincronización de hora de NTP está habilitada
Auditoría y responsabilidad	NTP está protegido
Auditoría y responsabilidad	Registro del sistema remoto está habilitado
Integridad del sistema y de la información	La configuración local habilitada de iDRAC en el sistema host está deshabilitada
Integridad del sistema y de la información	El arranque seguro está habilitado
Identificación y autenticación	La contraseña tiene un puntaje mínimo de protección sólida
Identificación y autenticación	La validación del certificado LDAP está habilitada
Identificación y autenticación	La validación del certificado de Active Directory está activada
Identificación y autenticación	Cifrado SSL del servidor web de iDRAC con 256 bits o superior
Identificación y autenticación	Servidor web de iDRAC: SCEP está habilitado

1. A partir de la versión de firmware de iDRAC 4.40.00.00, la función telnet se elimina de iDRAC

Resumen

A diferencia del típico miembro del equipo de TI, CloudIQ no necesita comer, dormir o irse de vacaciones, de modo que las organizaciones pueden confiar en las políticas de seguridad cibernética de CloudIQ para supervisar continuamente los servidores que no cumplen las normas. La seguridad cibernética incorporada en CloudIQ permite a los clientes acelerar la entrega de seguridad del servidor a través de la automatización de pruebas predefinidas y visualización de estado. Esto proporciona altos niveles de flexibilidad para los administradores de servidores, sin dejar de mantener la supervisión y el control que los equipos de seguridad cibernética necesitan aplicar. CloudIQ reduce aún más el riesgo y mejora la productividad de TI, ya que muestra la seguridad cibernética y el estado del sistema de los servidores y de todo el portafolio de la infraestructura de Dell, todo junto en el mismo portal práctico basado en la nube.

Referencias

CloudIQ en Dell.com: para obtener información sobre productos, videos de demostración y más

Tome el control de la seguridad cibernética de los servidores con un blog de supervisión inteligente basado en la nube

Video sobre creación y seguimiento de políticas de seguridad cibernética de Dell CloudIQ para servidores PowerEdge

Página de conocimientos técnicos para el plug-in de OpenManage Enterprise CloudIQ

Soluciones adicionales relativas a la seguridad cibernética de Dell