Fortaleça a segurança cibernética de seu servidor com o Dell CloudIQ

Resumo

As organizações podem levar anos para construir uma boa reputação com seus clientes e apenas alguns minutos com um incidente relacionado à segurança cibernética para arruiná-la. As equipes de segurança cibernética e os administradores de servidor devem usar todas as ferramentas ao seu dispor para fortalecer a infraestrutura. Aqui está um recurso do Dell CloudIQ que todos os clientes do Dell PowerEdge devem conhecer.

Esta nota técnica Direct from Development (DfD) descreve os recursos de segurança cibernética para servidores PowerEdge integrados ao CloudIQ.

O CloudIQ é um aplicativo de monitoramento e análise preditiva baseado em nuvem e IA/ML para o portfólio de produtos de infraestrutura da Dell. Hospedado na segura Dell IT Cloud, o CloudIQ coleta e analisa dados de integridade, desempenho e telemetria para identificar riscos e recomendar ações para resolução rápida de problemas.

Autor

Mark Maclean
Engenharia Técnica de Marketing

Kyle Shannon
Gerenciamento de produtos

Versão 1.1 de julho de 2022

Introdução

O Dell CloudIQ oferece um recurso de segurança cibernética que agora inclui os servidores Dell PowerEdge. O recurso de segurança cibernética integrado ao CloudIQ permite que as equipes de servidores dos clientes criem uma política chamada plano de avaliação. Este plano de avaliação foi criado a partir de vários testes de critérios de configuração prontos para uso. Esta lista de definições de configuração e valores se baseia nas práticas recomendadas da Dell e na estrutura de segurança cibernética do NIST (National Institute of Standards and Technology, Instituto Nacional de Padrões e Tecnologia).

Uma abordagem para resultados rápidos

Um especialista com as habilidades certas que entende as definições exatas de configuração de segurança com os valores corretos pode criar um perfil de configuração do servidor “SCP” e usá-lo diretamente com o recurso de modelo de configuração do iDRAC ou OME para definir as configurações do servidor. No entanto, o CloudIQ oferece um método muito mais rápido e prescritivo para implementar uma política de avaliação de segurança cibernética baseada nas configurações e valores recomendados pela Dell. Para simplificar ainda mais o processo de segurança cibernética, o CloudIQ pode agregar várias instâncias do OME, oferecendo uma visão consolidada dos servidores em diversos locais. Algumas organizações podem optar por usar o OME e o CloudIQ para demonstrar a diferença entre conformidade de configuração e gerenciamento de segurança.

Figura 1 Resumo do status de segurança cibernética da página de visão geral do CloudIQ

A área de segurança cibernética acima encontrada na página de visão geral do CloudIQ fornece uma visão agregada do status do nível de risco, detalhando o número de sistemas em cada categoria de risco e o número total de problemas detectados. O risco é determinado pela severidade e pelo número de problemas por servidor. Por exemplo, um servidor com um ou mais problemas de alto risco é categorizado como de alto risco, mas um servidor com mais de cinco riscos não altos com pelo menos um deles sendo um problema médio também seria categorizado como de alto risco.

Identifique riscos com rapidez

O painel de indicadores de risco do sistema classifica cada servidor com uma política aplicada, exibindo cada servidor em seu próprio cartão com o status do nível de risco de segurança cibernética. Isso ajuda os clientes a priorizar ações com rapidez e acelerar o tempo de resolução.

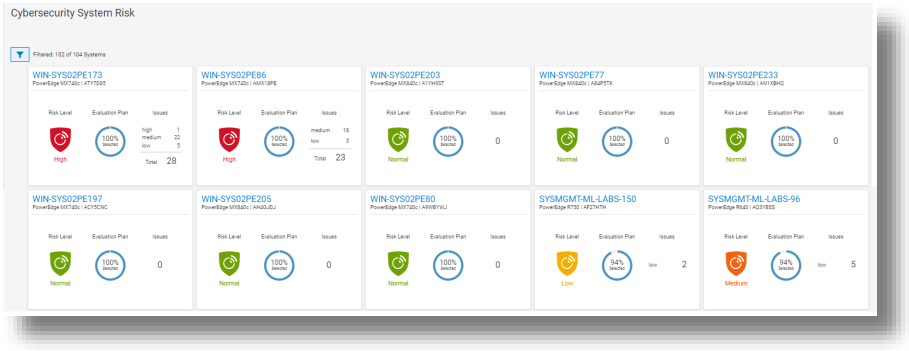

Figura 2 Painel de indicadores de risco do sistema de segurança cibernética de todos os sistemas

Além do painel de indicadores, o status de avaliação de segurança exibe as informações de cada servidor com a ação recomendada para retornar qualquer configuração de segurança modificada ao estado preferencial. O gráfico de rosca exibe a quantidade de regras selecionadas como uma porcentagem do total de testes no plano de avaliação de risco atribuído ao servidor específico.

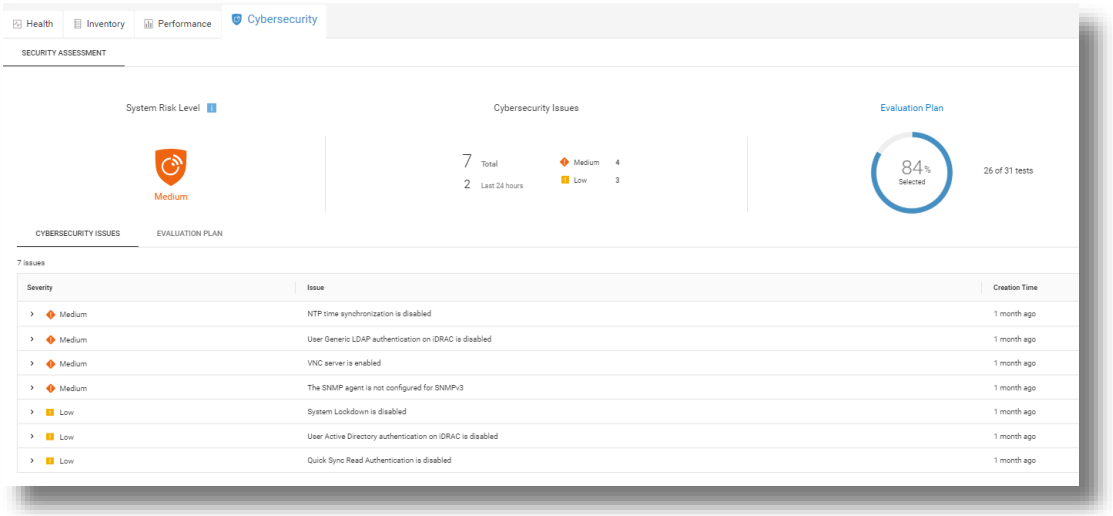

Figura 3 Informações e recomendações sobre os riscos de segurança cibernética

Na página de detalhes do sistema na guia de segurança cibernética, há informações sobre o plano de avaliação e seu status. A parte inferior da página possui duas guias: Problemas de segurança cibernética, que detalha os elementos que não estão em conformidade e sua devida ação corretiva e Plano de avaliação, que exibe todo o plano e o status de seleção de cada teste.

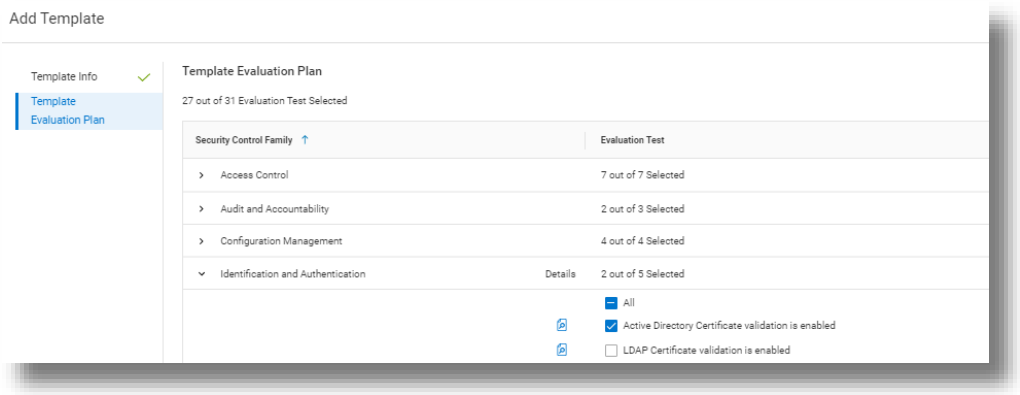

Figura 4 Seleção de teste

Os usuários do CloudIQ também podem optar por receber um e-mail de resumo diário, que inclui um resumo do status de segurança cibernética.

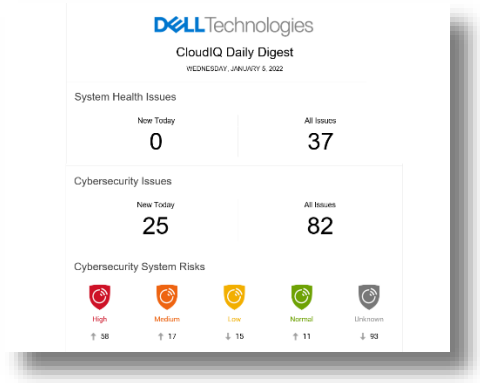

Figura 5 E-mail de resumo diário do CloudIQ

Capacitação e segurança

Como era de se esperar, há vários controles de acesso de segurança integrados ao CloudIQ nas contas de administrador e de usuário para controlar a criação e a geração de relatórios. Há duas funções de segurança cibernética criadas no CloudIQ: Administrador de segurança cibernética e Visualizador de segurança cibernética. Essas funções podem ser atribuídas a partir de contas do CloudIQ com direitos de administrador.

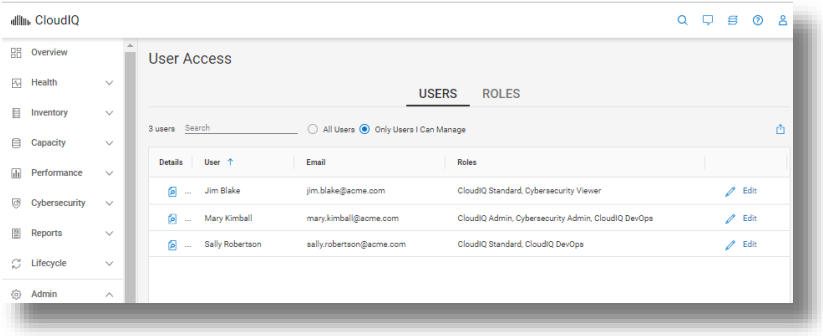

Figura 6 Configuração do RBAC

Para oferecer suporte à segurança cibernética do PowerEdge no CloudIQ, os clientes devem utilizar o OpenManage Enterprise 3.9 ou superior com o plug-in 1.1 ou superior do CloudIQ ativado. Todos os servidores exigem cobertura do Dell ProSupport e já devem ter sido identificados pelo OME.

Elementos de teste do plano de avaliação de segurança cibernética do PowerEdge

A tabela abaixo detalha cada critério de teste e a família do plano de teste à qual pertencem.

Família	Título
Sistema e comunicações	A IPMI na interface LAN está desativada
Sistema e comunicações	A IPMI Serial na LAN está desativada
Sistema e comunicações	A criptografia do console virtual está ativada
Sistema e comunicações	A criptografia de mídia virtual está ativada
Sistema e comunicações	A detecção automática está desativada
Sistema e comunicações	Os recursos da VLAN do iDRAC estão ativados
Sistema e comunicações	O servidor da Web do iDRAC está com o TLS 1.2 ou TLS 1.3 ativado
Sistema e comunicações	As solicitações HTTP do servidor da Web do iDRAC são redirecionadas para solicitações HTTPS
Sistema e comunicações	O tipo de plug-in do console virtual está ativado
Sistema e comunicações	O iDRAC está usando o NIC dedicado
Sistema e comunicações	O servidor da Web do iDRAC está com o TLS 1.2 ou TLS 1.3 ativado
Controle de acesso	O bloqueio de IP está ativado
Controle de acesso	O servidor VNC está desativado
Controle de acesso	O agente SNMP está configurado para SNMPv3
Controle de acesso	A autenticação de leitura do Quick Sync para o servidor está ativada
Controle de acesso	O SSH está desativado
Controle de acesso	A autenticação do LDAP genérico do usuário no iDRAC está ativada
Controle de acesso	A autenticação do Active Directory do usuário no iDRAC está ativada
Gerenciamento de configuração	As portas USB estão desativadas
Gerenciamento de configuração	O protocolo Telnet está desativado[1]
Gerenciamento de configuração	O bloqueio do sistema está ativado
Gerenciamento de configuração	Configurar o iDRAC a partir do POST do BIOS está desativado
Auditoria e responsabilidade	A sincronização de tempo NTP está ativada
Auditoria e responsabilidade	O NTP está protegido
Auditoria e responsabilidade	Syslog remoto está ativado
Integridade do sistema e das informações	Configuração local ativada: a configuração do iDRAC no sistema host está desativada
Integridade do sistema e das informações	A inicialização segura está ativada
Identificação e autenticação	A senha tem a pontuação mínima da proteção forte
Identificação e autenticação	A validação do certificado do LDAP está ativada
Identificação e autenticação	A validação do certificado do Active Directory está ativada
Identificação e autenticação	A criptografia do SSL servidor da Web do iDRAC usando 256 bits ou mais
Identificação e autenticação	Servidor da Web do iDRAC - SCEP ativado

1. A partir da versão 4.40.00.00 do firmware do iDRAC, o recurso Telnet é removido do iDRAC

Resumo

Diferente de um membro de equipe de TI convencional, o CloudIQ não precisa comer, dormir ou sair de férias. Portanto, as organizações podem confiar nas políticas de segurança cibernética do CloudIQ para monitorar continuamente a não conformidade de servidores. A segurança cibernética integrada ao CloudIQ permite que os clientes acelerem a entrega da segurança do servidor por meio da automação de testes predefinidos e visualização de status. Isso proporciona altos níveis de flexibilidade para administradores de servidor, mantendo a governança e o controle que as equipes de segurança cibernética precisam aplicar. O CloudIQ reduz ainda mais os riscos e a melhoria da produtividade da TI ao demonstrar a segurança cibernética, além do status de integridade do sistema de servidores e o portfólio mais amplo de infraestrutura da Dell, tudo isso no mesmo portal conveniente e baseado em nuvem.

Referências

CloudIQ em Dell.com - para obter informações sobre o produto, vídeos de demonstração e muito mais

Blog Assuma o controle da segurança cibernética de servidores com o monitoramento inteligente baseado em nuvem

Vídeo sobre como criar e acompanhar as políticas de segurança cibernética do Dell CloudIQ para servidores PowerEdge

Página de conhecimento técnico do plug-in OpenManage Enterprise do CloudIQ

Soluções adicionais relacionadas à segurança cibernética da Dell