O lado humano da segurança cibernética

Imagine o pior cenário.

Todo o seu data center foi desligado por um sofisticado ataque de ransomware. Vendas, atendimento ao cliente e finanças não podem operar. Você é um líder sênior de TI, responsável pela restauração dos sistemas, mas encontrar uma solução tem se mostrado difícil.

Sua equipe, já com poucos recursos, tem trabalhado por semanas, com pouquíssimos intervalos ou tempo de descanso. Alguns profissionais ***chegaram a ficar 36 horas seguidas*** sem dormir. Há a preocupação de que o cansaço esteja levando a decisões equivocadas, potencialmente comprometendo o próprio esforço de recuperação.

Você precisa desesperadamente de recursos adicionais que possam intervir imediatamente e ajudar a resolver o problema, mas onde encontrá-los?

Este cenário pode parecer o começo de uma novela, mas é baseado em experiências reais de clientes da Dell. Ele destaca um problema significativo no ambiente de segurança cibernética atual: O elemento humano.

Dados recentes indicam que o setor sofre com uma escassez de quase 5 milhões de profissionais de segurança. Embora a demanda de recursos seja mais crítica durante um incidente, as soluções começam muito antes.

Comece com a criação e a expansão de um pipeline de talentos

O primeiro passo para garantir que você tenha os recursos necessários é criar um pipeline de talentos:

Estágios e recrutamento universitário

Parcerias com universidades e escolas técnicas podem garantir um fluxo contínuo de novos talentos. Esses profissionais podem ser desenvolvidos ao longo do tempo até se tornarem membros de equipe de alto impacto.

Treinamento e desenvolvimento contínuos

Embora o tempo e o orçamento estejam sob pressão constante, os profissionais de segurança cibernética devem acompanhar as mudanças nas ferramentas e nas ameaças.

Foco na retenção

Há uma alta demanda por bons profissionais, principalmente se tiverem experiência em lidar com ataques. Se você não retiver os melhores, outra empresa o fará.

Mesmo uma equipe forte pode não ser suficiente para lidar com o estresse de gerenciar um ataque, portanto planeje com antecedência, identificando suporte adicional antes que seja necessário:

Avaliar recursos de terceiros

As empresas de consultoria em segurança cibernética e de aumento de equipe podem ajudar sua equipe durante operações contínuas e incidentes. Estabeleça relacionamentos com essas empresas, mesmo que você não precise delas agora, para ter acesso a esses recursos quando necessário.

A Dell oferece uma série de serviços que podem ampliar as equipes existentes, incluindo CISO virtual (vCISO), resposta a incidentes e consultoria em segurança cibernética.

Aproveite a IA

Aproveite os novos recursos de IA incorporados às ferramentas de segurança cibernética, como análise de logs, detecção de anomalias, triagem de alertas de baixo nível ou treinamento especializado para ajudar a suprir lacunas de recursos e atender às necessidades operacionais, liberando potencialmente os membros da equipe para se concentrarem em tarefas mais importantes.

Desafios de recursos são maiores durante um ataque cibernético

Como o cenário inicial ilustrou, um grande ataque cibernético pode prejudicar sua organização, paralisando os principais sistemas e operações comerciais. Cada minuto custa dinheiro para a empresa, e a equipe de segurança cibernética enfrentará uma enorme pressão para corrigir o problema.

Garantir que suas equipes estejam o mais atualizadas possível terá um impacto direto na resposta a incidentes e no estresse relacionado na equipe.

Lembre-se de que o treinamento deve se estender além dos profissionais de segurança e abranger todos os funcionários, pois eles são a primeira linha de defesa.

Esta história destaca um desafio central: os defensores cibernéticos são, em última análise, humanos. Eles têm limites, e quando esses limites são excedidos, até os profissionais mais fortes podem falhar. Fadiga mental, estresse e esgotamento são agora fatores críticos na postura de segurança cibernética.

Copyright © 2025 Dell Inc. ou suas subsidiárias. Todos os direitos reservados.

Embora não exista uma única solução para esse desafio, as seguintes estratégias podem contribuir significativamente:

Criando uma equipe forte e um pipeline de talentos

A solução mais fundamental para esse problema é não deixar que ele se torne uma emergência: monte uma equipe resiliente com redundâncias adequadas.

Planejando o lado humano de um ataque

Os planos de resposta a incidentes são essenciais e DEVEM incluir planos para gerenciar equipe, agendar e lidar com o tempo de inatividade dos funcionários.

Aproveite recursos de terceiros

Consultores externos de segurança cibernética podem ajudar a aumentar sua equipe. Os serviços de resposta a incidentes da Dell, por exemplo, podem ter uma equipe de especialistas no local em poucas horas, pronta para avaliar, conter e iniciar a correção imediatamente. Ajudamos muitos clientes a superar ataques cibernéticos.

A IA pode ajudar, mas não é uma solução mágica

A IA oferece uma enorme promessa de aprimorar ferramentas e programas de segurança cibernética. Em última análise, suas capacidades vão abranger desde análise preditiva até desenvolvimento de programas de treinamento personalizados, e até mesmo abordar proativamente as ameaças antes que elas se espalhem.

Talvez ainda mais importante, a IA pode fornecer aos defensores um sistema de suporte em tempo real durante um incidente. Os modelos de aprendizado de máquina treinados em dados de ataques históricos podem recomendar ações com base em eventos anteriores semelhantes.

À medida que o processamento de linguagem natural avança nas ferramentas de segurança cibernética, os analistas terão a capacidade de interagir diretamente com seus sistemas, identificar ameaças e implementar soluções.

A IA também pode monitorar padrões de comportamento e identificar quando um analista humano está cometendo erros repetitivos, possivelmente devido à exaustão, e sugerir uma troca de turno ou uma segunda revisão.

Embora as ferramentas de segurança cibernética estejam integrando rapidamente ferramentas de IA mais sofisticadas, muitos dos recursos mais poderosos ainda estão em desenvolvimento. Lembre-se de que neste momento, a IA não pode substituir as habilidades de um profissional experiente, ***especialmente alguém que já tenha passado por um ataque anteriormente***.

Recomendações para aproveitar a IA:

Entenda como as ferramentas podem ajudar suas operações de segurança

Faça uma análise detalhada das ferramentas de IA e implemente-as onde elas podem ser mais eficazes. Possíveis conquistas incluem detecção de ameaça avançada, automatização de tarefas repetitivas e uso de IA no gerenciamento de identidades.

> Ter um parceiro de confiança para resposta a incidentes, correção e recuperação sob contrato é uma prática recomendada."
>
> ***Jason Rosselot***
> *Vice-presidente, diretor de segurança cibernética e segurança de unidade de negócios, Dell Technologies*

Planeje o futuro da IA

Entenda quando novos recursos estarão disponíveis, como eles beneficiarão sua equipe e desenvolva um plano para implementá-los.

Incorpore a IA no planejamento da força de trabalho

À medida que a automação reduz as tarefas manuais, a composição da sua equipe de segurança pode precisar evoluir. Você pode precisar de recursos de nível mais alto para analisar e agir com base em informações de segurança, em vez de compilá-las. Ajuste suas estratégias de contratação e desenvolvimento adequadamente.

A IA se tornará uma parte significativa de suas operações de segurança cibernética, se ela já não for. Mas lembre-se de que não há substituto para um profissional qualificado e experiente. O objetivo deve ser usar a IA para automatizar operações e tornar os recursos humanos mais eficazes, prevenindo ataques e minimizando seu impacto quando ocorrerem.

Maturidade da segurança cibernética avançada: Um passo de cada vez

Como tudo em segurança cibernética, abordar o elemento humano é uma jornada, não um destino. O esforço incremental e até mesmo pequenos passos em direção ao progresso fazem a diferença e se somam ao longo do tempo. O importante é lembrar que mesmo as melhores ferramentas de segurança e de tecnologia são, em última análise, tão boas quanto as pessoas que as executam.

Copyright © 2025 Dell Inc. ou suas subsidiárias. Todos os direitos reservados.

DELL Technologies

Produtos e soluções da Dell que podem ajudar

Solução Dell em destaque	Descrição
Serviços de resposta a incidentes	Uma equipe de especialistas em segurança cibernética certificados pelo setor está à disposição para uma resposta rápida em caso de um ataque cibernético. Trabalhamos lado a lado com você para eliminar as ameaças até que as operações normais sejam retomadas.
Cybersecurity Advisory Services	Orientação especializada que pode ajudar você a encontrar e abordar pontos cegos em sua estratégia de segurança, proteger seus ativos e dados, e permitir vigilância e governança contínuas.
vCISO	Diretor virtual de segurança das informações (vCISO) e especialista em segurança cibernética que pode ajudar a identificar e gerenciar riscos, bem como orientar a tomada de decisões estratégicas.
Managed Detection and Response	Reduz os esforços manuais e simplifica as operações diárias de segurança, fornecendo monitoramento, detecção de ameaças, investigação e resposta rápida em endpoints, rede e nuvem. Os clientes escolhem sua plataforma XDR preferida (Secureworks® Taegis™ XDR, CrowdStrike Falcon® XDR ou Microsoft Defender XDR) e recebem orientação especializada, relatórios trimestrais e até 40 horas anuais de resposta a incidentes.

Saiba como enfrentar alguns dos principais desafios atuais de segurança cibernética em **dell.com/cybersecuritymonth**

Copyright © 2025 Dell Inc. ou suas subsidiárias. Todos os direitos reservados.