SERVIÇOS DE SEGURANÇA CIBERNÉTICA

PROTEGENDO SUAS OPERAÇÕES DE MISSÃO CRÍTICA

MOTOROLA SOLUTIONS

ATAQUES CIBERNÉTICOS SÃO UMA REALIDADE. E OS RISCOS SÃO ALTOS.

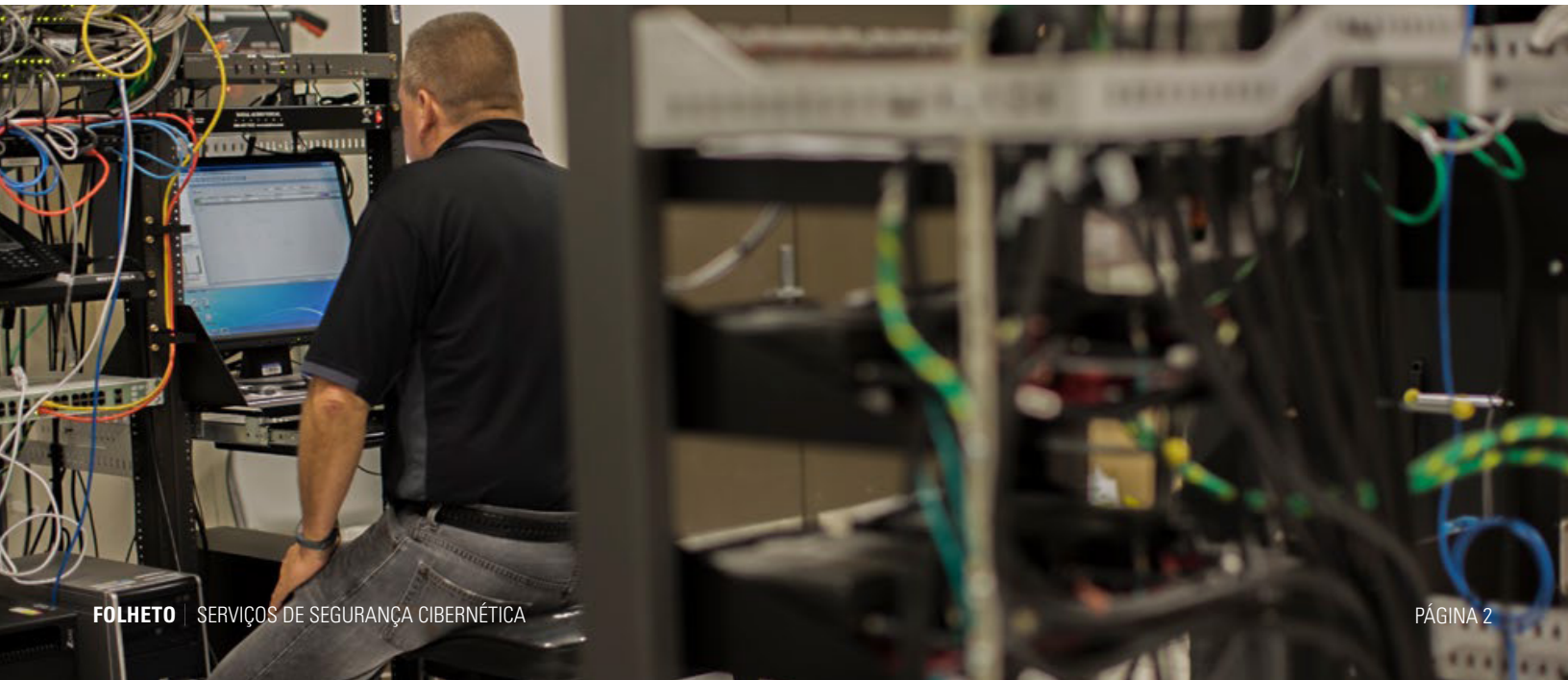
Para organizações encarregadas de operações de missão crítica, o tempo de inatividade do sistema coloca vidas em risco e o fracasso simplesmente não é uma opção. Mas os ataques cibernéticos continuam aumentando em número, frequência e impacto. De fato, o custo anual dos danos globais por crimes cibernéticos deve atingir US$ 5 trilhões em 2020.[1]

Malware, ransomware, phishing, ataques man-in-the-middle, ataques de negação de serviço distribuídos, injeções de SQL e explorações de dia zero são alguns dos ataques comuns que podem interromper operações de missão crítica sem aviso prévio. Muitas vezes, estratégias de segurança são criadas para "verificar a caixa" sobre a conformidade de segurança ou como uma reação a um ataque específico. Claramente, as estratégias de ontem para proteger operações de missão crítica são inadequadas para se proteger contra as ameaças cibernéticas avançadas e aceleradas de hoje.

A incerteza e as implicações financeiras de um ataque cibernético tornaram a segurança cibernética uma das principais preocupações para as organizações. O avanço das técnicas contra ataques cibernéticos e um sistema baseado em IP em constante evolução estão pressionando incansavelmente os recursos internos. Há uma necessidade constante de atualizar habilidades e conhecimentos para gerenciar um ambiente complexo e reforçar a resiliência cibernética. Além disso, os investimentos em ferramentas de segurança de última geração para prevenir e combater ameaças sofisticadas continuam representando um desafio, à medida que as organizações enfrentam orçamentos cada vez menores.

O que é necessário? Uma abordagem holística para a segurança cibernética centrada em torno de uma mentalidade de risco, que se concentra em opções de mitigação, monitoramento contínuo, diagnóstico e remediação. Nós podemos ajudar!

Oferecemos uma gama de produtos e serviços de segurança que abrangem seu ecossistema de missão crítica - redes, software de centro de comando, vídeo e rádios. Estamos continuamente evoluindo nosso portfólio para garantir que você tenha a resiliência cibernética para ficar um passo à frente dos ataques cada vez mais sofisticados. Com a orquestração perfeita de talentos altamente especializados, processos de segurança líderes do setor e ferramentas de ponta, ajudamos a gerenciar a complexidade da segurança cibernética para que você possa se concentrar em sua missão principal.



PROTEGIDO PELA MOTOROLA SOLUTIONS: SERVIÇOS PARA RESILIÊNCIA CIBERNÉTICA

Nossa abordagem para a segurança cibernética inclui um conjunto holístico de serviços que abrange Avaliação e Consultoria de Risco, Patches de Segurança e Monitoramento de Segurança. Além disso, estamos expandindo o portfólio para incluir serviços de Resposta e Recuperação e Treinamento em Segurança Cibernética. Todas as nossas ofertas seguem rigorosamente a Estrutura de Segurança Cibernética do Instituto Nacional de Padrões e Tecnologia (NIST), que visa ajudar as organizações a gerenciar a conscientização, detecção, resposta e recuperação de riscos cibernéticos.

ESTRUTURA DE SEGURANÇA CIBERNÉTICA DO NIST LÍDER DO SETOR

IDENTIFICAR	PROTEGER	DETECTAR	RESPONDER	RECUPERAR
Avaliar os riscos Inventariar ativos e sistemas críticos Fornecer uma análise de risco completa	**Desenvolver proteções** Desenvolver políticas, procedimentos; introduzir ferramentas de proteção Implementar controles apropriados de acesso e auditoria	**Fazer descobertas oportunas** Monitoramento contínuo 24/7/365 Ativar recursos de auditoria	**Entrar em ação** Estabelecer um plano de resposta robusto Criar, analisar, classificar e responder aos eventos detectados	**Restaurar funcionalidade** Instituir um plano de recuperação Criar melhorias para evitar ataques futuros

SERVIÇOS DE SEGURANÇA CIBERNÉTICA

- AVALIAÇÃO DE RISCO E CONSULTORIA
- PATCH DE SEGURANÇA
- MONITORAMENTO DE SEGURANÇA
- RESPOSTA E RECUPERAÇÃO CIBERNÉTICA
- TREINAMENTO DE SEGURANÇA CIBERNÉTICA

AVALIAÇÃO DE RISCO E CONSULTORIA

Com base em décadas de experiência trabalhando em estreita colaboração com clientes de segurança pública, governo e empresas, refinamos uma avaliação de gerenciamento de risco sistemática e reproduzível que ajuda você a entender melhor seu ambiente de segurança específico. Isso abrange seu ecossistema de tecnologia, incluindo o centro de comando, redes LMR, rádios e câmeras de vídeo.

Começamos com uma pré-avaliação para entender seus requisitos e necessidades específicos, aplicando uma combinação de observação física, entrevistas pessoais e ferramentas disponíveis comercialmente e personalizadas. Em seguida, realizamos uma avaliação no local para garantir o alinhamento com a Estrutura de Segurança Cibernética NIST, avaliamos possíveis cenários de ameaças e avaliamos os riscos potenciais à confidencialidade, integridade e disponibilidade do sistema de comunicação da sua organização. Após a avaliação, entregamos um roteiro claro das etapas de mitigação, como mudanças na arquitetura de segurança, integração de produtos específicos ou implementação de novos controles processuais. Todos os riscos são identificados, claramente compreendidos e priorizados.

Na conclusão da avaliação, você recebe um relatório de scorecard de risco que prioriza cada descoberta com base na gravidade baixa, moderada, alta e crítica. Uma recomendação de remediação ou aceitação de risco segue cada descoberta. Por fim, com base nas lacunas identificadas, podemos introduzir novas tecnologias e fornecer serviços que ajudam você a enfrentar ameaças de segurança continuamente.

PATCH DE SEGURANÇA

O patch de segurança é uma das ferramentas mais importantes, mas muitas vezes negligenciado, para se defender contra ataques cibernéticos. Todos os softwares, sistemas e dispositivos precisam de patches contínuos para permanecer seguros. Trabalhamos com você em três fases - identificação, teste e instalação - para garantir que seus procedimentos de patches sejam o mais eficientes e seguros possível.

Primeiro, nosso Laboratório de Garantia de Informações dedicado identifica e valida as atualizações de segurança necessárias para identificar quaisquer lacunas nos patches do seu sistema. Todos os ativos de hardware e software, fluxos e dependências de rede e comunicação são identificados, mapeados, classificados e gerenciados de acordo com a criticidade. Embora seja importante aplicar os patches o mais rápido possível após o lançamento, para sistemas de missão crítica é absolutamente essencial testá- los completamente antes da implantação. O Serviço de Atualização de Segurança da Motorola Solutions realiza pré-testes das definições antimalware mais recentes e todos os patches de software aplicáveis em laboratórios de teste dedicados. Uma vez validado como seguro, trabalhamos em estreita colaboração com você na fase de instalação. Fazemos as atualizações para você ou as tornamos acessíveis em nossa extranet segura para implementação, para que sua organização possa implantá-las facilmente em seus próprios termos.

Você não consegue corrigir efetivamente sistemas antigos. As redes de missão crítica baseadas em IP de hoje exigem atualizações periódicas para que se mantenham atualizadas. A Motorola Solutions oferece atualizações de sistema para permitir a atualização da tecnologia de software e hardware em toda a sua infraestrutura, garantindo a disponibilidade do sistema.

MONITORAMENTO DE SEGURANÇA

O monitoramento remoto de segurança oferece a maneira mais econômica e segura de monitorar suas redes. Nossos recursos de monitoramento remoto permitem proteção 24/7/365, são fornecidos por especialistas técnicos e são apoiados pela automação.

Usamos um processo sistemático para detectar, analisar, investigar, resolver e reportar incidentes para proteger seu sistema.

DETECÇÃO DE AMEAÇAS POTENCIAIS - Seus sistemas da Motorola Solutions são pré-configurados com sensores de detecção de intrusão, autenticação e integração de servidor de registro e integração de antivírus para detectar worms, vírus e outras formas de software malicioso. A inteligência de ameaças de notícias de mídia global e social também é constantemente alimentada no sistema. Existem ferramentas para capturar e examinar os logs do sistema em toda a infraestrutura de rede, dispositivos, sistemas operacionais, software e aplicativos. Se um malware ou evento de intrusão for detectado em seu sistema, um alerta será gerado e a ação apropriada será tomada.

ANÁLISE DE DADOS AUTOMATICAMENTE - Usando algoritmos de aprendizado de máquina, todos os eventos em seu sistema são filtrados automaticamente para incidentes reais, omitindo ameaças falsas. Este sistema é programado e treinado para identificar tentativas de intrusão, infecção por malware, varredura baseada em rede e atividade de autenticação.

INVESTIGAÇÃO DE INCIDENTES - Os detalhes do incidente são gerados automaticamente e enviados para analistas de segurança que pesquisam e analisam minuciosamente o incidente, aproveitando a base de conhecimento para triagem qualificada e solução de problemas.

RESOLUÇÃO DE UM INCIDENTE - Se um incidente for confirmado em seu sistema, nossos tecnólogos trabalharão rapidamente para identificar e implementar uma correção. Eles monitorarão o evento até que seja totalmente resolvido e o incidente seja encerrado para sua satisfação. Para encerrar o caso, eles fornecerão assistência no local para garantir que a situação seja corrigida e seu sistema retorne ao modo operacional total.

RELATÓRIOS - Queremos mantê-lo informado sobre quaisquer alterações na integridade do seu sistema. Nossos relatórios pós-incidente são gerados rapidamente, usados para implementar medidas preventivas, compartilhados com sua equipe e aproveitados em futuras operações de segurança para melhor proteger sua rede.

PORTAL MYVIEW

Entendemos que é fundamental que você tenha total visibilidade do desempenho de todo o seu ecossistema de tecnologia. Nosso portal de gerenciamento baseado na web fornece insights acionáveis sobre o status e a integridade do seu sistema, permitindo que você fique de olho na integridade do seu ecossistema de missão crítica. Conhecido como Portal MyView, ele fornece informações rápidas e fáceis sobre seus incidentes de segurança e status de entrega de serviços a partir de uma única plataforma baseada na web.

SEU MOTOROLA SOLUTIONS EDGE: PESSOAS, PROCESSOS E FERRAMENTAS

A segurança cibernética eficaz vai além da tecnologia. Nossos talentos líderes do setor, processos de segurança e ferramentas de ponta fazem parte de uma abordagem integrada que simplifica a complexidade e torna mais fácil para sua organização gerenciar riscos.

PESSOAS

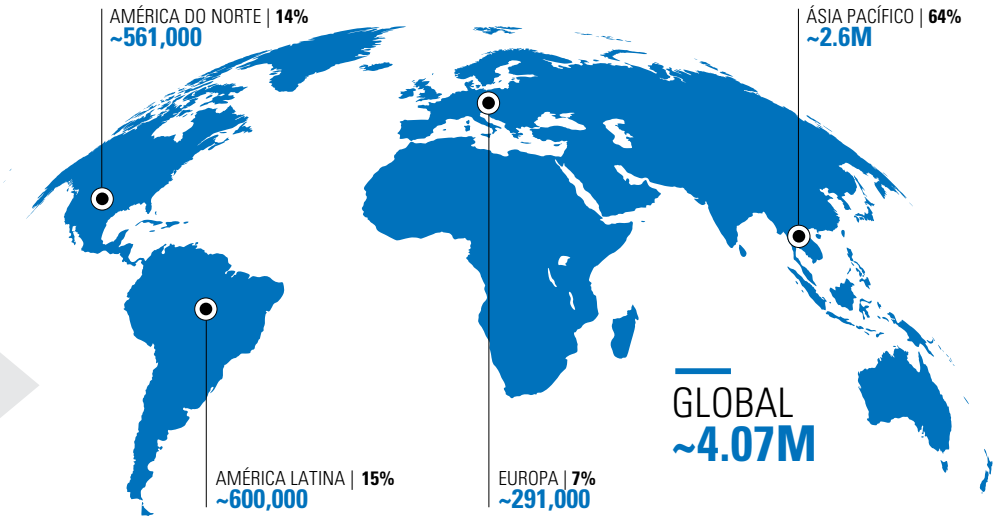
A falta de experiência em segurança cibernética é um desafio constante que muitas organizações enfrentam atualmente. Isso pode retardar a adoção e a implementação das ferramentas e processos críticos necessários para uma proteção eficaz da segurança cibernética.
Nosso pessoal é a força motriz de nossa cultura de segurança, totalmente integrada em tudo o que fazemos.

Nossos especialistas em segurança cibernética orientam toda a gama de nossas soluções de segurança cibernética, buscando constantemente uma segurança cibernética mais preditiva e proativa. Eles possuem as principais certificações de segurança cibernética do setor, como CJIS (Divisão de Serviços de Informações da Justiça Criminal), FIPS (Padrões Federais de Processamento de Informações) e FISMA (Lei Federal de Gerenciamento de Segurança da Informação) e permanecem afiados com treinamento abrangente e contínuo. Criamos o Programa Motorola Solutions Cyber Champions, que infunde princípios e conhecimento de segurança cibernética em nível básico em todas as áreas da empresa. Investimos continuamente em educação e treinamento cibernético porque, quando nossos especialistas em segurança cibernética estão preparados para o sucesso, você também está. Usamos a Estrutura da Força de Trabalho de Segurança Cibernética do NIST para orientar nossos esforços de educação cibernética e treinamento.

Além disso, a equipe de inteligência de ameaças da Motorola Solutions cria uma visão holística do cenário de ameaças cibernéticas e como isso afeta as prioridades de negócios e a infraestrutura de nossos clientes. A equipe analisa e comunica a capacidade, oportunidade e intenção de uma ameaça cibernética direcionada aos produtos e clientes da Motorola Solutions. Esse nível de consciência situacional fornece às partes interessadas e aos tomadores de decisão as informações necessárias para priorizar recursos e permitir melhores decisões de segurança. Nossos especialistas estão aqui para ajudá-lo a navegar em um ambiente de tecnologia complexo para que seu pessoal possa se concentrar na missão, não na tecnologia.

A CRISE DO PESSOAL DE SEGURANÇA CIBERNÉTICA

La escasez global de personal de ciberseguridad se estima en 4 millones de profesionales con más de 500,000 de estos puestos ubicados en América del Norte. Asia Pacífico, con sus economías en crecimiento y nuevas regulaciones de privacidad, está experimentando la escasez más grande, calculada en 2.6 millones de puestos.[3]



PROCESSOS

Nossos processos de segurança cibernética são orientados por três objetivos principais: confidencialidade, integridade e disponibilidade. Dados e informações devem ser restritos a pessoas autorizadas a acessá-los e não devem ser divulgados a terceiros; os dados devem ser mantidos intactos, completos e precisos, com os sistemas de TI operacionais; e todas as informações devem estar disponíveis para usuários autorizados sempre que necessário. Embora muitas organizações simplesmente se concentrem na prevenção, no atual clima de ameaças, todas as empresas devem estar totalmente preparadas para um cenário de ataque cibernético de "pior caso".

Com a Estrutura de Segurança Cibernética do NIST em sua essência, nossa abordagem à segurança cibernética se concentra em opções de mitigação, monitoramento contínuo, diagnóstico e remediação para proteger sistemas e redes. Além disso, estamos alinhados com os princípios das práticas de gerenciamento ITIL reconhecidas pelo setor, design de serviço, transição de serviço e operações de serviço para entrega de serviço. Nossa equipe experiente se baseia em amplo conhecimento global para desenvolver um modelo de entrega de serviço, arquitetura e políticas que atendam às suas necessidades.

FERRAMENTAS

Criminosos e intervenientes estatais estão sempre evoluindo a tecnologia que usam em ataques cibernéticos. Para estar um passo à frente, nos tornamos cada vez mais preditivos e proativos com investimentos em ferramentas sofisticadas, como automação e análise. Quando aplicadas corretamente, a automação e a análise podem reduzir os custos operacionais, acelerar a resposta do serviço e aumentar a tomada de decisões preditivas, eliminando muitos dos processos manuais demorados envolvidos no gerenciamento de ameaças. Além disso, o uso de análises avançadas para examinar ameaças e padrões de falha em todo o sistema pode evitar incidentes de segurança com mais eficácia, abordando suas causas raiz antes que afetem o sistema.

Com base em um rico data lake, essas ferramentas otimizam continuamente o desempenho do sistema.
Também investimos continuamente em outras tecnologias avançadas, como gerenciamento de incidentes e eventos de segurança (SIEM); detecção de intrusão de rede e varredura de vulnerabilidade. Empregamos as ferramentas mais avançadas de segurança cibernética para que você possa sempre acompanhar as tendências tecnológicas complexas, sem investir tempo e recursos adicionais.

RESILIÊNCIA CIBERNÉTICA FEITA CORRETAMENTE

Os ataques cibernéticos podem acontecer a qualquer pessoa em qualquer momento. Você está pronto? Nossos serviços de segurança cibernética oferecem a experiência, tecnologia de ponta e capacidade de resposta para ajudá-lo a chegar lá. A parceria com a Motorola Solutions para segurança cibernética permite que sua equipe se concentre em sua missão, e não na manutenção de sistemas. Nós gerenciamos a complexidade para você, o que significa que você está sempre no ritmo da inovação a um custo previsível. Nossa equipe de especialistas se tornará sua equipe, protegendo holisticamente seus ativos de comunicação mais importantes, antecipando problemas antes que eles se tornem problemas e melhorando continuamente os planos para evitar ataques futuros.

A Motorola Solutions é líder em comunicações de missão crítica por um motivo. Trazemos a mesma confiança e compromisso em que você confia há mais de 90 anos para todos os serviços de segurança cibernética que oferecemos. Com pessoas, processos e ferramentas líderes do setor, estamos redefinindo o que significa garantir a resiliência para operações de missão crítica.

ESCALA GLOBAL E EXPERIÊNCIA

4M
USUÁRIOS NO NOSSO SERVIÇO GERENCIADO

20M
EVENTOS MONITORADOS PROATIVAMENTE TODOS OS DIAS

13K
SISTEMAS INSTALADOS

100K
CLIENTES EM 100 PAÍSES

90+
ANOS DE EXPERIÊNCIA

NOTAS
1 Revista de Defesa Cibernética
2 Pesquisa de Benchmark de Gerenciamento de Sistemas LMR da Motorola Solutions de 2018
3 Estudo da Força de Trabalho de Segurança Cibernética ISC2 2019, 2019

Veja como a Motorola Solutions pode ajudar a manter sua organização segura.
Visite www.motorolasolutions.com para saber mais.

MOTOROLA SOLUTIONS

Motorola Solutions, Inc. 500 West Monroe Street, Chicago, IL 60661 U.S.A. 800-367-2346 **motorolasolutions.com**