Whitepaper

Explorando o caminho para a convergência entre TI e segurança física

Genetec™

Conteúdo

Sumário executivo

A convergência entre tecnologia da informação (TI) e segurança física começou há anos. Tudo começou com uma mudança do protocolo analógico para o protocolo de Internet (IP), seguida pela adoção de aplicações de segurança física hospedadas na nuvem. À medida que a tecnologia mudou, também mudou a relação entre TI e segurança física.

Atualmente, Diretores de Recursos Humanos, Diretores de Segurança da Informação (CISOs) e Diretores de Segurança (CSOs) estão buscando maneiras de integrar essas habilidades e equipes. Eles estão cientes que os riscos físicos e de segurança da informação precisam ser entendidos e tratados como riscos comerciais inter-relacionados. Eles também sabem que dados valem ouro. Mas responsabilidades isoladas e culturas departamentais únicas tornam esta tarefa difícil.

A segurança física e de TI têm pontos fortes diferentes que são importantes para um negócio seguro e bem administrado. A segurança física ajuda a proteger instalações, pessoas e ativos de uma organização. A TI mantém a rede corporativa cibersegura e resiliente. Embora ambos os papéis sejam críticos, estes grupos não compreendem necessariamente como se complementarem.

As ameaças à cybersecurity tornaram-se implacáveis e os requisitos de compliance de privacidade estão em constante evolução. Com habilidades e recursos limitados, não é de admirar que as organizações nem sempre consigam acompanhar.

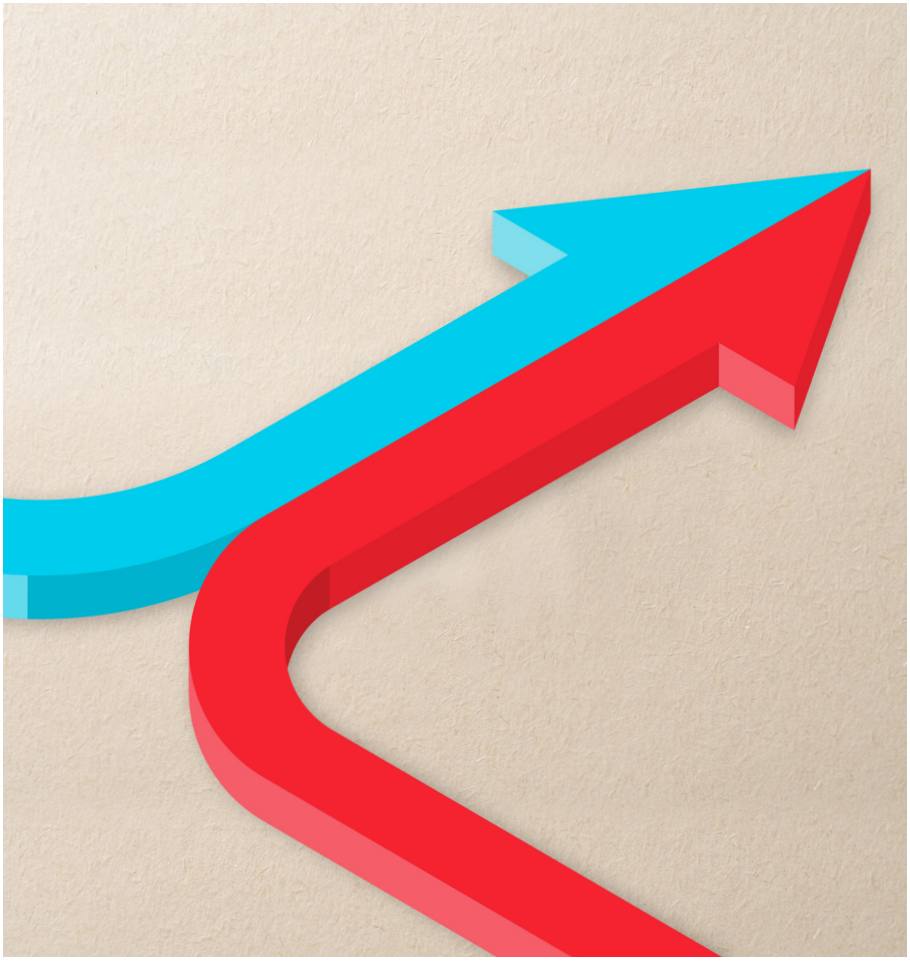
Encontrar maneiras de gerenciar dados provenientes de diversas fontes diferentes e otimizar esse processo também pode ser uma tarefa difícil. Sensores e atividades de segurança física criam um hub de dados, enquanto as equipes de TI administram vários projetos baseados em dados. Mas como eles podem trabalhar juntos para otimizar as operações comerciais e trazer dados de segurança física para a análise?

As organizações que enfrentam esses problemas estão considerando estratégias para unificar essas equipes. Algumas equipes de TI estão trazendo segurança física para seus grupos. Alguns líderes de segurança física estão expandindo seus departamentos com habilidades de TI. Outras empresas estão ampliando a função das Operações de Segurança (SecOps) para abordar os riscos de segurança e aproveitar os dados provenientes de ambos os grupos.

1

O dilema da convergência tecnológica centrado no ser humano.

Durante anos, as equipes de segurança física e TI trabalharam de forma independente. Eles se mantiveram focados em suas tarefas e objetivos, dando suporte a funções empresariais essenciais de suas próprias maneiras. Mas com o tempo, isso mudou muito.



Em meados da década de 2000, os profissionais de segurança física começaram a migrar de soluções analógicas para soluções IP. Com isso, as equipes de TI passaram a se envolver mais na tomada de decisões em torno dos sistemas de segurança física. Seu conhecimento sobre redes, dispositivos da Internet Industrial das Coisas (IIoT) e cybersecurity forneceu insights valiosos. Complementou o conjunto de habilidades das equipes de segurança que sabem como proteger a empresa, seus colaboradores e ativos.

A colaboração entre as equipes de TI e de segurança física tornou-se crucial para garantir o sucesso da implementação e integração de novas soluções. Nos últimos anos, a TI começou a adotar soluções na nuvem como prática padrão, portanto, colaborar ainda mais tornou-se essencial para garantir a seleção, governança e resiliência cibernética adequadas a soluções de segurança física em rede.

Esta convergência de dispositivos de segurança e IIoT, facilitada pela adoção de IP e agora de soluções na nuvem, tem sido uma plataforma de lançamento para a jornada de transformação digital. Isto levou à constatação de que os dados de segurança física capturados ainda permanecem em grande parte inexplorados. Conectar sensores e sistemas de todas as áreas de negócios, seja segurança física, operações ou infraestrutura predial, tornou-se o catalisador para grandes ganhos de eficiência e novos insights de negócios.

Hoje, os dados de segurança física são uma mina de ouro dentro de uma organização. Acumular mais dados para iniciativas de transformação digital está na responsabilidade da TI. E a segurança física está posicionada para agregar mais valor operacional a uma empresa.

Enquanto isso, CTOs, CISOs e CSOs estão observando o desenrolar de toda essa convergência e analisando os desafios e considerações. Suas preocupações são com a integração da equipe, delineamento de papéis, governança e a complexidade do processo de tomada de decisão.

Este whitepaper oferece três estratégias diferentes de colaboração entre TI e segurança física. Também explica como a unificação desempenha um papel crítico nesta convergência, independentemente da estratégia escolhida.

2

Problemas comuns relacionados à convergência de TI e segurança física

Os líderes empresariais estão ansiosos para encontrar um terreno comum entre esses departamentos. Mas nem sempre é uma tarefa fácil. Muitas vezes existem desafios fundamentais que dificultam o elemento humano desta convergência. Aqui estão alguns problemas comuns que muitas organizações enfrentam ao tentar melhorar a colaboração entre as equipes de TI e de segurança física.

1. Os diferentes pontos fortes de cada equipe

Tanto a TI quanto a segurança física desempenham um papel crítico no gerenciamento de riscos corporativos. Mas os tipos de riscos que supervisionam são muito diferentes.

A segurança física tem uma compreensão detalhada do cenário de ameaças físicas. Eles sabem como avaliar riscos em diferentes tipos de instalações e empresas de grande porte. Eles podem identificar vulnerabilidades, pontos cegos e comportamentos suspeitos. Eles são especialistas em proteção de ativos, qualificados em investigações forenses e sabem como controlar rapidamente incidentes com risco de vida.

A TI se destaca em todas as áreas de conectividade de rede, IoT e cybersecurity. Eles sabem tudo sobre design de sistemas de segurança de TI e arquitetura de cybersecurity. As vulnerabilidades que detectam e mitigam estão ligadas a software e hardware. Eles ficam atualizados sobre as ameaças cibernéticas em evolução e reavaliam continuamente estratégias para manter a rede corporativa e todas as aplicações conectadas a ela seguras.

Como essas equipes estão focadas em seus próprios objetivos, elas podem nem sempre reconhecer a sobreposição em seu trabalho. Uma implantação de segurança física bem arquitetada e ciberneticamente resiliente pode fazer diferença. Isso significa que os profissionais de segurança física podem operar sem problemas para manter o negócio seguro e vice-versa.

Então, quem deve supervisionar o processo de compra de novas soluções de segurança física? As equipes de segurança física têm conhecimento profundo para implementar um sistema de segurança robusto que funcione bem na rede? Conseguem garantir desempenho e confiabilidade em um ecossistema grande e muitas vezes disperso de dispositivos? Ou a TI precisa intervir para ajudar a orientar os requisitos e especificações de implementação?

2. Prioridades diferentes em conflito.

Cada segundo conta quando uma ameaça física potencial é detectada. É por isso que as equipes de segurança física exigem que todas as informações estejam disponíveis para o maior número de pessoas possível. Ter uma visão compartilhada e abrangente do que está acontecendo garante que eles possam tomar decisões informadas para mitigar rapidamente qualquer situação.

A TI, por outro lado, normalmente deseja limitar o número de dispositivos na rede para minimizar a exposição a ameaças cibernéticas. Como a segurança física também é considerada um centro de custos, a TI nem sempre considerou os projetos de segurança física como alta prioridade.

Essas prioridades diferentes podem criar atritos entre as duas equipes. Os desafios surgem quando a segurança física não compreende totalmente o impacto potencial das ameaças cibernéticas que podem resultar das suas implementações. Eles também ocorrem quando a TI não avalia totalmente o impacto potencial que os pontos cegos podem ter nas atividades de segurança física.

Em alguns casos, a desconexão entre as equipes pode levar a segurança física a encontrar suas próprias soluções. Especialmente em organizações menores, elas podem estar mais ansiosas para adotar serviços na nuvem sem avaliar totalmente a viabilidade, confiabilidade ou credenciais de cybersecurity do fornecedor. Quanto mais tempo essas equipes permanecerem focadas em objetivos diferentes, maior o potencial para riscos organizacionais.

3. Exposição crescente a riscos cibernéticos

As empresas hoje possuem centenas ou milhares de dispositivos físicos de segurança em suas redes. Eles também estão investindo nos dispositivos IoT mais recentes, digitalizando processos antigos e encontrando maneiras de capitalizar os dados que coletam. Mas onde crescem as oportunidades de negócio, também crescem os riscos. Adicionar mais dispositivos e soluções à rede aumenta a exposição a vulnerabilidades de cybersecurity.

Os ataques cibernéticos também estão se tornando mais frequentes e sofisticados. Desde hacks de sistema e ataques DDoS até o aumento da prevalência de ataques de ransomware, é uma batalha constante manter as novas ameaças sob controle. E os riscos de terceiros ainda dominam todos os ataques cibernéticos.

Segundo o Relatório Estado da Cybersecurity da Accenture, 61% das violações cibernéticas bem-sucedidas vêm de ataques indiretos a organizações através de sua supply chain. No mundo digitalmente conectado de hoje, não existem mais perímetros de rede claramente definidos.

As empresas também estão tentando cumprir leis rigorosas de cybersecurity e privacidade em todas as regiões e indústrias. Tudo isto colocou uma enorme pressão sobre os recursos. Os departamentos estão lutando para encontrar a equipe necessária para manter as melhores práticas de cybersecurity. No entanto, ainda precisam aderir a novas políticas, como o Regulamento Geral de Proteção de Dados (GDPR), Lei de Proteção à Privacidade do Consumidor (CPPA) ou Lei de Portabilidade e Responsabilidade do Seguro de Saúde (HIPAA), entre outras.

E mesmo quando o fazem, obter compliance geralmente envolve trabalho e tarefas demoradas. Desde a concepção e implementação de políticas corporativas, procedimentos de auditoria e sistemas, até o reinvestimento em novas tecnologias, o custo de compliance com a proteção de dados e privacidade está aumentando hoje.

4. Mineração de dados essenciais

As empresas investem em soluções de segurança física para proteger edifícios, ativos e pessoas. Com o tempo, houve um despertar para o potencial de todos os dados coletados por esses sistemas.

Durante a crise sanitária, por exemplo, os líderes empresariais recorreram aos seus dados de segurança física para melhorar a gestão dos níveis de ocupação e do fluxo de pessoas nas suas instalações. Isto levou a novas discussões sobre como usar esses dados para dar suporte às operações comerciais.

Hoje, esses líderes olham para os dados de segurança física de forma diferente. De acordo com pesquisas recentes, 63% das organizações concordam que a segurança física e os dados relacionados são essenciais.

E vai além do que apenas extrair os dados que já possuem. Eles querem construir e implementar sistemas que possam servir a dois objetivos principais: segurança mais robusta e coleta de dados que dê suporte às operações comerciais. Para que isso aconteça, eles precisam das pessoas certas com as habilidades certas para prepará-los para uma otimização eficaz de dados.

Mas há uma desconexão em jogo. Embora os dados venham de investimentos em segurança física, as equipes de TI são normalmente o grupo mais envolvido em projetos de dados e iniciativas de transformação digital.

3

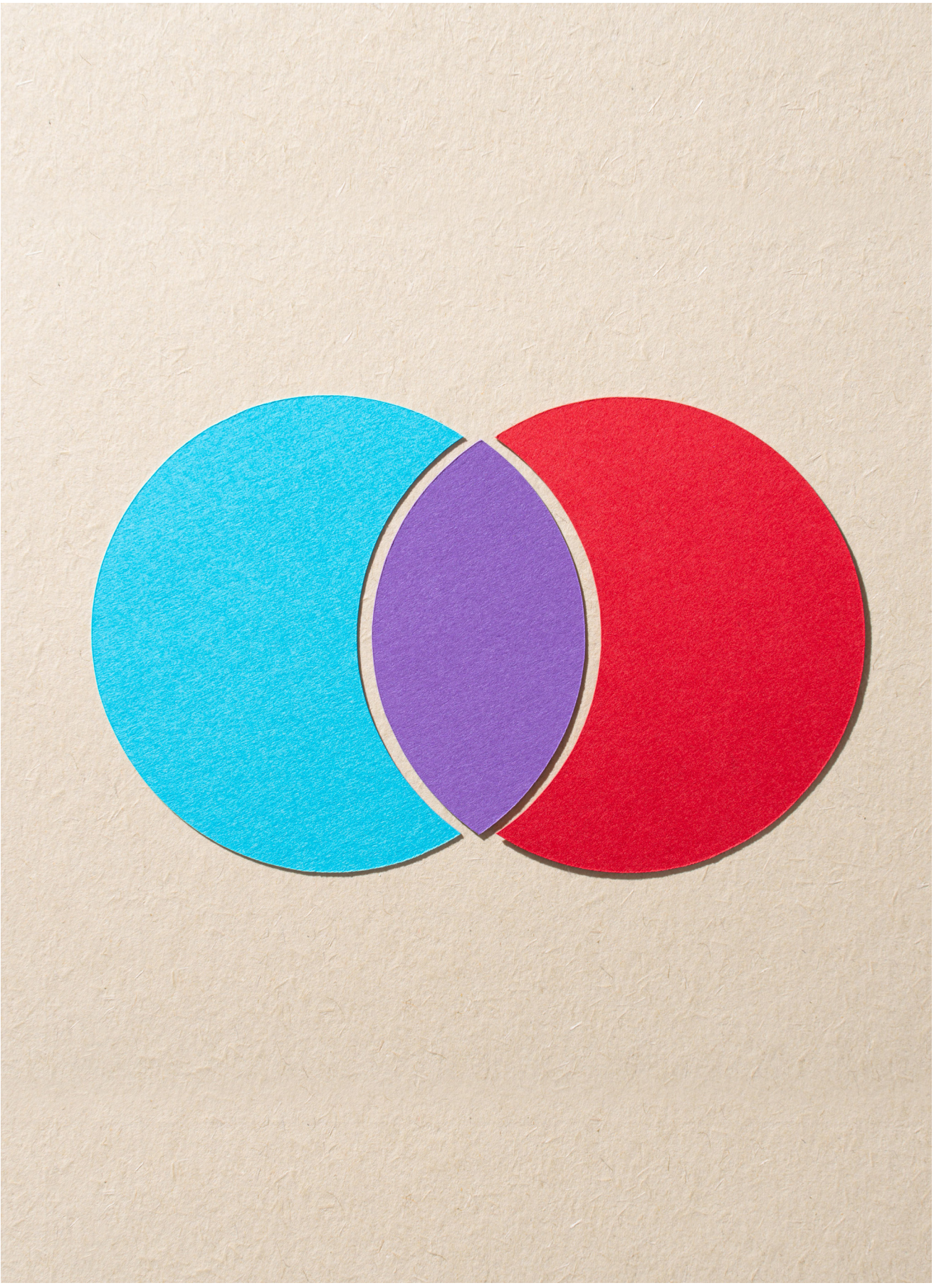
Três estratégias para melhor colaboração entre as equipes de TI e segurança

À medida que as tecnologias convergem, também convergem as funções de TI e de segurança física em uma organização.

A combinação de dois conjuntos de habilidades importantes dentro de um grupo pode ajudar a unificar o gerenciamento e a mitigação de riscos em toda a organização. Também ajuda a otimizar recursos, reduzir custos operacionais e melhorar o compliance.

Então, qual é a melhor maneira de unir essas equipes? Não há uma resposta única que sirva para todos. Abaixo estão três maneiras pelas quais as organizações estão enfrentando esse desafio hoje.

De acordo com uma Pesquisa da ASIS, 76% dos CISOs e CSOs acreditam que a combinação das funções de segurança cibernética e física fortalecerá o desempenho da gestão da segurança. 83% acreditam que um único líder de segurança aumentará a eficácia e o status da função de segurança.



Abordagem 1

A segurança física se expande com conjuntos de habilidades de TI

Nesse cenário, a segurança física ampliaria sua equipe com mais habilidades de TI. Isto incluiria a contratação de recursos dedicados dentro do seu departamento que supervisionariam tarefas específicas relacionadas com TI. Incorporar os recursos internos de TI existentes no departamento físico é outra opção. De qualquer forma, isso garante que a segurança física fique de posse daquilo que fazem de melhor. Ter recursos de TI qualificados na equipe também fortalece a forma como eles supervisionam e abordam quaisquer problemas de tecnologia e rede.

PRÓS

- Os profissionais de segurança física são especialistas no ambiente físico e sabem como proteger pessoas, ativos e edifícios
- A segurança física permanece no controle da otimização da funcionalidade do sistema para melhor identificar os riscos e responder a vários incidentes, garantindo ao mesmo tempo que os sistemas sejam implantados de maneira cibersegura
- A segurança física pode entender como colaborar da melhor forma com integradores, consultores e parceiros da comunidade mais ampla para aprimorar a segurança organizacional
- A segurança física pode avaliar e implementar mais facilmente novas soluções que cumpram os padrões e requisitos de TI em evolução (para soluções na nuvem, resiliência cibernética etc.)

CONTRAS

- A segurança física pode não ter uma compreensão clara de quais habilidades de TI são mais necessárias em seu departamento ou o que procurar no processo de contratação
- A segurança física pode ter limitações orçamentárias. Encontrar financiamento adicional para novas funções especializadas pode atrasar ou limitar o crescimento das habilidades das equipes de TI
- A segurança física permanece separada das equipes corporativas de TI. Isto poderia impedir a liderança de ter uma visão completa da gestão de riscos nestes principais grupos empresariais

Abordagem 2

SecOps assume tarefas de segurança física

Neste cenário, um grupo novo ou já estabelecido de Operações de Segurança (SecOps) dentro do departamento de TI assume tarefas específicas de TI e de segurança física. Os grupos SecOps têm experiência em cybersecurity relacionada a TI, otimização de rede e mitigação de riscos. As responsabilidades agora evoluiriam para supervisionar esses domínios também na segurança física. Eles também se concentrariam no gerenciamento de dados em toda a empresa, inclusive de fontes de segurança física. Seu objetivo principal seria usar essas informações para extrair valor comercial.

PRÓS

- SecOps atuam como um grupo centralizado em gerenciamento de dados e riscos. Isso amplia a visibilidade sobre vulnerabilidades em toda a empresa e novas oportunidades de negócios
- Geralmente, os SecOps têm expertise em cybersecurity, redes, nuvem, IoT e análise de dados
- Expandir esses conjuntos de habilidades para a segurança física ajuda a maximizar recursos e economizar custos
- SecOps são especialistas em dar sentido aos dados e identificar melhorias operacionais. Essas habilidades podem ser usadas para aprimorar procedimentos e políticas relacionadas à avaliação de riscos, resposta a incidentes e compliance da indústria para tornar as operações de segurança física ainda mais eficientes

CONTRAS

- Os SecOps podem enfrentar resistência ou relutância por parte da segurança física ou TI que deseja manter o controle sobre seus dados e operações. Isto poderia diluir o seu foco durante a transição e criar riscos organizacionais
- Os SecOps estão focados em defesa, detecção e resposta proativas. Para isso, investem pesadamente em ferramentas de automação para cumprir suas atribuições. Essa maneira de trabalhar impulsionada pela tecnologia pode provocar medo de obsolescência em diversos profissionais de segurança física e de TI
- SecOps podem incluir uma vasta equipe de diferentes especialistas. Isto pode exigir uma liderança segmentada dentro do departamento, o que prejudica o propósito pretendido de ter dados mais centralizados e governança de risco

Abordagem 3

A TI começa a supervisionar as diretrizes de segurança física.

Nesse cenário, a TI se tornaria muito mais ativa na tomada de decisões sobre segurança física. Também poderiam assumir a segurança física como parte de suas atribuições. Isso significaria que o CISO se tornaria o líder predominante tanto dos especialistas em TI quanto em segurança física dentro da empresa. Isto confere uma visão mais central das operações e estratégias de mitigação de riscos, com foco em redes resilientes e ecossistemas de segurança.

PRÓS

- A área de TI conhece melhor a cybersecurity. Eles entendem como projetar redes e construir arquiteturas de sistemas que sejam eficientes, otimizadas e resilientes
- A TI entende as complexidades dos riscos da supply chain. Eles podem garantir que todos os fornecedores e soluções escolhidos atendam às melhores práticas e padrões de cybersecurity
- A área de TI tem mais conhecimento sobre nuvem e dados. Eles podem garantir que a empresa capitalize todos os recursos inovadores da tecnologia de ponta, sistemas operacionais, aplicações e hardware

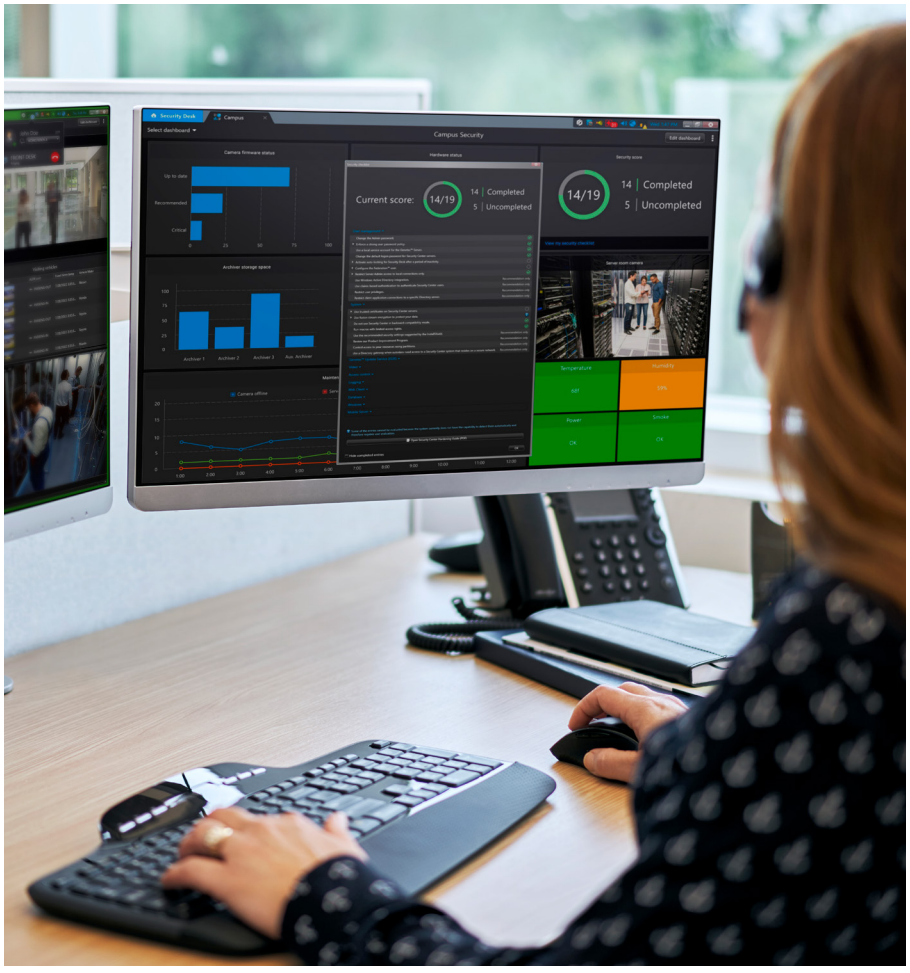
CONTRAS

- A área de TI não tem um conhecimento profundo de como proteger melhor pessoas, instalações e ativos. A segurança física é uma prática especializada e aprimorada que requer anos de treinamento e experiência prática
- A área de TI pode não se adaptar bem a um modelo de vendas liderado por integradores ou querer depender de especialistas em segurança física intermediários para comprar e implantar soluções
- A área de TI pode não saber como melhor instalar e configurar um sistema de segurança física para otimizar a eficiência do operador. Eles estão menos cientes dos protocolos de resposta apropriados ou de como colaborar da melhor forma com parceiros da comunidade
- A área de TI geralmente prioriza esforços que minimizam as vulnerabilidades de cybersecurity. Por causa disso, eles podem relutar em adicionar novos dispositivos, sensores ou tecnologias que possam aumentar a eficiência da segurança física ou o fortalecimento do perímetro

Escolhendo a estratégia que melhor se adapta a uma organização

Não existe uma abordagem certa ou errada para convergir as equipes de TI e de segurança física. Esses departamentos têm pontos fortes de longa data no cumprimento de objetivos essenciais de negócios. A dedicação compartilhada em manter a organização segura é, sem exceção, impressionante. E, em muitos casos, essas equipes já encontraram maneiras de se adaptar e trabalhar mais estreitamente em conjunto para implementar com sucesso novos projetos e aprimorar processos.

Com isto em mente, é importante considerar todas as nuances dentro da organização antes de se comprometer com qualquer estratégia. Às vezes, construir com base em colaborações existentes pode ser o melhor passo a seguir. Em outros casos, escolher uma estratégia combinada que se ajuste à cultura e às dinâmicas únicas da empresa pode ser a abordagem vitoriosa. De qualquer forma, encontrar novas maneiras de integrar essas equipes e conjuntos de habilidades resultará em uma mitigação de riscos mais eficaz e otimização de dados em todo o negócio.



4

Por que a unificação desempenha um papel crítico na convergência

Independentemente da estratégia escolhida, é essencial uma maior colaboração entre segurança física e TI. E investir numa solução de segurança unificada pode ajudar. Isso garante que as organizações obtenham uma visão abrangente dos sistemas, riscos e oportunidades. Também os prepara para lidar com ameaças físicas e de cybersecurity em evolução, ao mesmo tempo em que aproveita ao máximo os dados que coleta para criar insights valiosos.

1. Suporta as três estratégias de convergência

Ter uma plataforma de segurança aberta e unificada pode ajudar a facilitar a transição ao reunir equipes de TI e segurança física. Isso porque uma solução unificada é construída desde o início para incluir sistemas como videomonitoramento, controle de acesso, reconhecimento automático de placas de veículos e outros.

Com a unificação, as equipes não precisam mais trabalhar em sistemas isolados ou compilar dados de locais diferentes para tomar decisões. Em vez disso, todos os vídeos e dados são alimentados para uma plataforma intuitiva, que todos podem acessar.

Ferramentas de visualização detalhada de dados ajudam todos os especialistas dedicados (segurança física, TI e SecOps) a entender rapidamente os dados e identificar quaisquer riscos ou oportunidades. Todos não apenas terão o que precisam para supervisionar suas tarefas, mas também poderão trabalhar de forma mais colaborativa.

Uma plataforma aberta oferece ainda mais às organizações a flexibilidade para integrar tudo, desde analíticos avançados até sistemas de negócios críticos. Isso significa que eles podem continuar expandindo e coletando mais informações em toda a empresa ao longo do tempo.

2. Simplifica as operações comerciais

Profissionais de segurança física podem acessar milhares de câmeras e portas, sensores de intrusão, reconhecimento automático de placas de veículos, intercomunicadores e muito mais em locais e regiões geográficas.

Uma plataforma unificada de segurança física simplifica o gerenciamento de dados para TI e SecOps, consolidando vários dados do sistema de segurança em uma única plataforma. Ele fornece uma integração perfeita e um formato de dados padronizado, para que haja caminhos consistentes para extrair e exportar informações para bancos de dados externos ou data lakes. Isto agiliza o processo de compartilhamento de dados, melhora a colaboração e permite a utilização eficiente de informações de segurança dentro do ecossistema de dados mais amplo.

Também capacita as equipes de segurança porque elas só precisam aprender, configurar e gerenciar um único sistema, em vez de vários sistemas individuais. Também pode reduzir a fadiga causada por alarmes, classificando o ruído, para que o operador possa concentrar sua atenção em ameaças reais e em procedimentos de resposta guiados. Tudo isso melhora a consciência situacional, permite uma melhor tomada de decisões e garante o compliance.

3. Melhora as funcionalidades de privacidade e cybersecurity

Trabalhar a partir de uma plataforma de segurança unificada permite que as equipes de TI e segurança implementem uma estratégia única e global de proteção de dados e privacidade. Tudo, desde a forma como criptografam dados e permitem autenticações multifatoriais até como compartilham evidências e definem privilégios de usuário, pode ser aplicado para todos os sistemas de segurança física.

Uma plataforma unificada cria uma visão abrangente dos riscos em tempo real e ferramentas eficazes para fortalecer sistemas e dispositivos. Isso inclui monitoramento de disponibilidade do sistema, widgets especializados em score de segurança, painéis de integridade customizados e serviços de gerenciamento de atualização. Automatizar políticas de retenção, agendar relatórios de auditoria e usar mascaramento para privacidade simplifica ainda mais o compliance.

4. Simplifica o acesso aos recursos de nuvem e nuvem híbrida

Escolher uma plataforma de segurança flexível e unificada oferece às organizações várias opções de implantação: in loco, nuvem e nuvem híbrida. Isso apoia políticas de cloud-first e hybrid-first para possibilitar uma maior segurança física e convergência de TI.

Os serviços na nuvem ajudam a reduzir as cargas de trabalho das equipes de TI e segurança. As equipes não precisam mais gerenciar infraestrutura, lidar com atualizações ou monitorar a integridade do sistema. Em vez disso, tudo, desde firmware de dispositivo e patches de software até outros dados críticos de segurança, é automaticamente enviado ao sistema.

Os serviços na nuvem também podem facilitar novas aplicações empresariais. Por exemplo, as empresas podem facilmente estender o acesso ao sistema de segurança física a outros departamentos para melhorar as operações. Também podem experimentar novos serviços na nuvem, como compartilhamento seguro de arquivos digitais ou simplificação do fluxo de visitantes entre sites. Como essas soluções na nuvem exigem investimento inicial e tempo de implantação mínimos, tudo isso pode ser feito com pouco risco para a organização.

E não importa quantos sistemas uma organização possa ter em execução em servidores locais ou conectados à nuvem, a unificação garante que todos eles se conectem a um head-end central e que a experiência do usuário permaneça sem interrupções.

5. Otimiza coleta de dados e inteligência de negócios

Quando todos os dados de segurança física são reunidos em uma plataforma, as equipes podem obter insights significativos para os negócios. É importante ter uma plataforma unificada que ofereça visualização de dados avançada. Ela pode exibir dados em mapas, gráficos ou histogramas, em vez de bancos de dados e planilhas. Isso pode ajudar as equipes a iniciarem o trabalho real mais rapidamente, acessar insights valiosos e descobrirem alguns problemas inesperados.

As equipes podem identificar padrões em incidentes de segurança e compreender melhor o desempenho das estratégias de segurança atuais. A partir daí, poderão encontrar oportunidades para melhorar a resposta a incidentes ou fazer melhorias para redução de custos nos protocolos de operação padrão (SOPs).

Com uma visão orientada por dados, as equipes podem encontrar novas maneiras de otimizar espaços, simplificar o estacionamento, expandir os esforços de sustentabilidade ou cumprir as normas da indústria. Eles também poderiam estender as informações do sistema a outros departamentos focados em melhorar a experiência do cliente ou os serviços comerciais.

5

Perguntas no caminho para uma maior colaboração entre TI e segurança física

Identificar a melhor maneira de reunir essas equipes leva tempo. É um processo que requer muitas discussões internas e considerações exclusivas de cada organização.

Aqui estão algumas questões a considerar à medida que os líderes iniciam sua jornada rumo a uma maior segurança física e convergência de TI:

1. Quais são nossos objetivos de negócios para avançar na mitigação e avaliação de riscos corporativos?
2. Quais questões específicas estão impedindo nossa organização de integrar as habilidades de segurança de TI e física em um único grupo? Quais medidas podemos tomar para aliviar a desconexão?
3. Nossa equipe de segurança física exige habilidades e suporte adicionais de TI em seu departamento? Temos orçamento para iniciar o processo de contratação? Quais habilidades específicas relacionadas à TI darão melhor suporte à segurança física hoje e daqui a 5 anos?
4. Nossa equipe de TI dispõe de largura de banda para lidar com as complexidades do planejamento, implantação e mitigação da segurança física?
5. Que tipo de resistência podemos esperar se unirmos essas equipes? Como podemos amenizar algumas das interrupções e fazer com que todos estejam na mesma página?
6. Temos os recursos, competências e orçamento para compor ou ampliar uma equipe SecOps internamente?
7. Nosso arsenal de tecnologia atual suporta uma política global de cybersecurity e privacidade em nossos sistemas de segurança física?
8. Existem ativos ou serviços de segurança que podem ser migrados para a nuvem ou transferidos para um serviço gerenciado para aliviar a carga sobre nossa equipe de TI?
9. Quais problemas estamos tentando resolver em nossa organização? Quais dados são mais relevantes para resolver esses problemas?
10. Estamos aproveitando ao máximo todos os dados de segurança física que coletamos? Como cada departamento gerencia e analisa os dados?
11. A nossa tecnologia de segurança física suporta a convergência centrada no ser humano? Os profissionais de TI, segurança física e SecOps podem obter o que precisam com a tecnologia de que dispomos para cumprir com eficácia suas atribuições?

6

Investindo em uma visão abrangente da sua organização

A convergência de TI e segurança física está acontecendo. E os líderes empresariais entendem que o sucesso depende da união das suas equipes.

Do ponto de vista humano, esta união incentiva a aprendizagem multifuncional e a troca de conhecimento entre as equipes. A resolução conjunta de problemas e a visão de vários especialistas internos levam a maiores inovações e resultados. Metas e mentalidades compartilhadas também ajudarão a refinar as melhores práticas em segurança, TI e operações de negócios.

É fundamental descobrir como usar melhor os pontos fortes existentes na organização e unir a segurança física e os conjuntos de habilidades de TI. O mesmo ocorre com a identificação de que forma novos talentos centrados em dados, tais como SecOps, podem agregar valor adicional à empresa.

Independentemente do caminho a seguir, essa colaboração proporciona aos líderes um melhor controle sobre tecnologias emergentes, oportunidades de dados e ameaças cibernéticas.

Hoje, as organizações procuram maneiras de otimizar a segurança e a eficiência operacional. E enquanto a convergência tecnológica está preparando o cenário para isso acontecer, os líderes de segurança física e TI entendem que o sucesso depende também de unir suas equipes. Alguns estão considerando diferentes maneiras de unir a segurança física e o conjunto de habilidades de TI. Outros procuram alargar o âmbito do SecOps para incluir tarefas de segurança física.

Independentemente da estratégia, uma maior colaboração entre estes grupos é benéfica. As organizações terão uma visão mais unificada dos sistemas, riscos e oportunidades em toda a empresa. Estarão mais bem preparados para lidar com ameaças em evolução e manter a resiliência cibernética. Eles também estarão posicionados para capitalizar os dados de segurança física para impulsionar a transformação digital.

A escolha de uma plataforma de segurança aberta e unificada pode ajudar a facilitar a transição para esta nova estrutura organizacional. A unificação aumenta a visibilidade em todas as áreas críticas: segurança física, cybersecurity e otimização de dados. E a abertura dá às organizações a flexibilidade para se adaptarem e expandirem, independentemente da abordagem que escolham ou de como as coisas evoluem no futuro.

Fundada em 1997, a Genetec é líder global em plataformas de segurança unificadas, com uma ampla oferta para uma variedade de especialidades de segurança.

Suporte à decisão operacional: Gere mais eficiência para tratamento de incidentes e tomada de decisão através de fluxos de trabalho avançados que orientam os operadores desde o alerta da situação até os procedimentos baseados em políticas para exportação de compilação detalhada de casos.

Gerenciamento de caso investigativo: Simplifique o gerenciamento de casos e acelere as investigações com uma plataforma que permite centralizar evidências digitais e colaborar de forma segura com investigadores, agências externas e o público.

Serviços na nuvem: Estenda os recursos do seu sistema de segurança in-loco e reduza os custos de TI com serviços na nuvem altamente escalável, sob demanda que capacitam sua cidade a lidar facilmente com os requisitos de segurança em rápida mudança e operar com maior eficiência.

Reconhecimento automático de placas de veículos: Automatize a detecção de veículos de interesse, aumente a eficiência da fiscalização em estacionamentos e acelere as investigações de segurança pública por meio da capacidade de compartilhar dados de placas de veículos com agências selecionadas e organizações parceiras, sem violar propriedade e privacidade.

Videomonitoramento: Obtenha uma maior consciência situacional e aumente a segurança em sua cidade com a capacidade de compartilhar câmeras entre agências e organizações, fornecendo uma imagem operacional em comum e melhorando o tempo de resposta a incidentes.

Controle de acesso: Aumente a segurança da sua organização de forma eficaz, responda às ameaças e tome decisões mais claras e em tempo hábil usando uma plataforma unificada e pronta para IP, seja para implantação de um novo sistema de controle de acesso ou para atualizar uma instalação existente.

Genetec Inc.
genetec.com/br/fale-conosco
info@genetec.com
@genetec

Por favor, recicle

ATUALIZADO: 20 DE MAIO DE 2024