Rockwell Automation

RESULTADOS DA PESQUISA DE 2022

Preparação para cibersegurança em infraestrutura crítica: evitando "O grande desligamento"

Sumário

Introdução	3
Resumo executivo	4
Identificar riscos e lacunas	5
Proteger ativos críticos	7
Detectar ameaças previamente	10
Responder a incidentes rapidamente	13
Recuperar com um Plano	14
Preparar para o Futuro	15
Apêndice: Todos os resultados da pesquisa	16

INTRODUÇÃO

Os setores de infraestrutura crítica estão enfrentando uma tempestade perfeita em cibersegurança. As organizações de tecnologia operacional (TO) são desafiadas com vulnerabilidades crescentes, lacunas de cibersegurança novas e existentes, uma superfície de ataque em expansão e ameaças globais crescentes.

Atores sofisticados e com bons recursos, como gangues de ransomware e hackers de estado-nação, têm em vista as organizações de infraestrutura crítica. Em 2021, 83% das organizações de infraestrutura crítica pesquisadas disseram ter sofrido violações de cibersegurança[1]. À medida que os ataques continuam a aumentar e as fraquezas da infraestrutura crítica permanecem sem serem reduzidas, O grande desligamento – um desastre em grande escala com implicações amplas e prejudiciais – se aproxima da realidade. As organizações de infraestrutura crítica não podem mais esperar à margem, despreparadas.

Para entender o estado da cibersegurança da infraestrutura crítica e obter informações sobre a preparação e as melhores práticas das organizações, a Rockwell Automation contratou a ISMG para fazer uma pesquisa com os líderes de TI e cibersegurança em vários setores da infraestrutura crítica. Este relatório apresenta nossas descobertas, juntamente com as lições aprendidas e recomendações.

Organizamos este relatório em cinco temas principais alinhados com a Estrutura de cibersegurança NIST (Identificar, Proteger, Detectar, Responder e Recuperar). Essa estrutura também é usada pela Rockwell Automation como um roteiro fundamental para avaliar e fortalecer a cibersegurança da infraestrutura crítica.

[1] Skybox Security (via Yahoo! Finance): 83% of Critical Infrastructure organizations suffered breaches, 2.021 cybersecurity research reveals, 11 de novembro de 2021

RESUMO EXECUTIVO

Atacantes que desejam causar estragos ou obter rápido retorno sobre o investimento descobriram que as organizações de infraestrutura crítica são um alvo atraente. As gangues de ransomware, por exemplo, geralmente visam empresas de serviços públicos, energia, petróleo e gás. Eles são os mais propensos entre todos os setores a pagar resgate[2] porque não podem arriscar nenhum tempo de parada não programada.

As complexidades do ambiente de TI e TO também dificultam a recuperação dessas organizações, e os danos das paralisações podem ser imensos, incluindo tempo de parada não programada, perdas financeiras e ameaças à segurança e ao bem-estar público.

A pesquisa ISMG mostra que as organizações de infraestrutura crítica estão se movendo na direção certa. Eles estão tomando medidas para melhorar a preparação e a resiliência da cibersegurança. No entanto, a pesquisa também mostra que o progresso é lento em comparação com a urgência. Muitos estão lutando para superar obstáculos como escassez de orçamento e talentos, falta de priorização de gerenciamento e falta de percepção sobre a melhor forma de fortalecer as defesas hoje.

A maioria está ausente ou está indo muito devagar em etapas fundamentais, como avaliações de inventário, segmentação de rede e monitoramento de ameaças. Consequentemente, as vulnerabilidades generalizadas persistem por toda a infraestrutura crítica.

As principais descobertas para liderança em negócios e segurança incluem:

1. **As organizações de infraestrutura crítica permanecem amplamente abertas a ataques cibernéticos.** A pesquisa encontrou lacunas significativas em áreas de alta prioridade, como monitoramento de inventário de ativos, gestão de acesso remoto, gestão de patches, segurança de endpoint, segmentação de rede, resposta a incidentes e planejamento de recuperação, avaliações de segurança da cadeia de fornecimento e conscientização de segurança dos funcionários. Por exemplo, menos de 20% das organizações pesquisadas conduzem auditorias de inventário de ativos com a frequência adequada. Apenas um terço tem práticas eficazes de gerenciamento de patches de TO. Além disso, a detecção contínua de ameaças é um ponto cego em todos os setores, com 60% das organizações sem detecção de ameaças em tempo real. O setor de manufatura e maquinário se destaca em particular, pois apenas 37% dos entrevistados citaram ter alguma medida em vigor em todas as questões. É surpreendente que os outros 63% não estejam fazendo nada – é apenas uma questão de tempo até vermos consequências desastrosas.
2. **Fechar brechas deve se tornar uma prioridade urgente.** Os ataques divulgados recentemente expõem os altos custos do tempo de parada dos ataques cibernéticos e não apenas o potencial de prejudicar operações, mas também de interrupções da vida diária. Os ataques às redes de ICS (sistemas de controle industrial) de TO (tecnologia operacional) em indústrias que apresentam risco de impactos na segurança pública, como água, alimentos, petróleo e gás, saúde e transporte, estão crescendo em volume e intensidade, e as organizações de infraestrutura crítica não estão se movendo rápido o suficiente para reduzir o risco. Por exemplo, apenas 56% dos entrevistados podem analisar, conter e reduzir as ameaças recebidas hoje.
3. **O orçamento inadequado aumenta o risco e atrasa o progresso.** Os líderes de segurança citaram que a falta de financiamento está dificultando sua capacidade de aplicar ferramentas e processos conhecidos de redução de riscos, como avaliações de inventário e gestão de patches. Dado o cenário de ameaças e o dano potencial de um ataque cibernético, as organizações devem reconhecer que o custo de não fazer nada (ou fazer algo muito lentamente) pode afetar drasticamente o tempo de disponibilidade, comprometer os sistemas e, por fim, impactar os clientes finais, a economia e até a segurança nacional.
4. **As organizações não estão olhando muito à frente.** O governo dos EUA está aumentando seu foco na cibersegurança, especialmente porque os riscos geopolíticos estão crescendo. O governo federal planeja financiar US$ 1 bilhão em subsídios de cibersegurança para organizações de infraestrutura crítica, mas menos de 30% dos entrevistados têm um plano de cibersegurança em vigor para ajudar a identificar lacunas críticas de cibersegurança e ajudar na criação de uma solicitação de subsídio, o que poderia ajudar a fechar essas lacunas.
5. **As organizações de infraestrutura crítica devem agir rapidamente.** Com base nessas descobertas, os profissionais de cibersegurança da Rockwell Automation recomendam estas etapas principais:
    - Realizar avaliações precisas de risco e vulnerabilidade para localizar as áreas de maior fraqueza.
    - Desenvolver um plano de cibersegurança com base nos resultados da avaliação.
    - Segmentar e fortalecer redes com IDMZ (Zona Industrial Desmilitarizada) e firewalls.
    - Implementar o monitoramento de ameaças.
    - Preparar e ensaiar planos de resposta a incidentes.

DEMOGRAFIA DA PESQUISA

A pesquisa foi realizada em janeiro de 2022 e recebeu 122 respostas. A ISMG solicitou respostas de líderes seniores de segurança industrial, cujas funções variavam de CISO e chefe de segurança a engenheiro de fábrica e gerente de negócios. CISOs e diretores ou chefes de segurança compunham as duas maiores coortes, quase 25% e 19%, respectivamente.

Os setores representados pelos entrevistados da pesquisa variaram em quase 20 TO verticalizadas, 57% representando organizações de infraestrutura crítica, incluindo verticais de petróleo e gás, energia, química, água/esgoto. As fabricantes tiveram o maior número de respostas dentre as verticalizadas com 18%.

[2] Sophos, "The State of Ransomware 2.021," abril 2021

SEÇÃO 1

Identificando e avaliando riscos

A segurança da infraestrutura crítica tornou-se mais complexa nos últimos anos. Os atacantes estão investindo recursos enormes para entender como os novos sistemas e redes de infraestrutura crítica interconectados operam e para encontrar os pontos fracos que podem explorar. Os operadores de infraestrutura crítica, no entanto, estão atrasados em obter essa visibilidade para si mesmos, para que possam identificar seus riscos e priorizar estratégias de defesa.

Para evitar O grande desligamento, as organizações de infraestrutura crítica precisam tomar medidas imediatas e urgentes para entender os riscos e fechar lacunas.

Avaliações de inventário

A auditoria de inventário de ativos é um primeiro passo fundamental na avaliação de riscos. É também uma área em que as organizações têm problemas para obter os insights certos e a frequência certa de relatórios. Como um entrevistado compartilhou, "o inventário é realmente difícil de manter atualizado. Uma máquina virtual pode ser montada e desmontada antes mesmo que a equipe de governança saiba que ela existiu."

Entre os participantes da pesquisa, a frequência mais comum para a avaliação do inventário de base instalada foi inferior a trimestral, com quase 30% das respostas apontando para essa frequência. Esse ritmo também foi o mais comum entre três setores muito críticos: manufatura e maquinário; saúde, setor de saúde pública e serviços de emergência; e produtos farmacêuticos e químicos.

No geral, 45% das organizações monitoram seu inventário trimestralmente e menos de 1 em cada 5 conduz as auditorias diariamente, que é a prática mínima recomendada pela Rockwell Automation.

Por que isso é importante?

Cada dispositivo não contabilizado cria um ponto de entrada vulnerável em sua rede. Há alguns anos, avaliações trimestrais ou mesmo mensais poderiam ser adequadas. Agora, com a velocidade dos ataques de hoje, as verificações diárias são essenciais na maioria dos casos e alguns entrevistados observaram que estão migrando para avaliações em tempo real, o que é possível com o design de rede correto e as ferramentas de monitoramento instaladas.

Também encontramos um desalinhamento na conscientização organizacional sobre as avaliações de inventário da base instalada. Os líderes de nível C (por exemplo, CIOs, CEOs, COOs) que participaram da pesquisa eram mais propensos a pensar que as avaliações eram realizadas a cada hora, diariamente ou semanalmente. No entanto, os técnicos com melhor visão do dia a dia das operações de segurança (por exemplo, chefes de segurança, diretores de TI e arquitetos ou engenheiros) pintaram um quadro menos positivo, descrevendo consistentemente a frequência como mensal, trimestral ou menos frequente.

RECOMENDAÇÕES

Inventários de ativos automatizados melhoram a prevenção ou interrupção de ataques resultantes da falta de visibilidade. Uma variedade de ferramentas e serviços automatizados estão disponíveis para simplificar o processo de avaliação de inventário, tanto para TI quanto para TO, em qualquer frequência que você decida que esteja dentro do seu limite de tolerância a riscos. Para organizações de infraestrutura crítica com risco de impactos descomunais na população, o inventário em tempo real é uma estratégia prudente, oferecendo visibilidade completa de seus ativos de rede.

Sistemas Críticos de Negócios

Nossa pesquisa constatou que apenas 56% das organizações tinham sistemas críticos de negócios identificados e priorizados, indicando que esta é uma área de urgência (Figura 1). Além disso, com base na experiência da Rockwell Automation, algumas organizações subestimam a eficácia de suas proteções em torno de sistemas críticos para os negócios. Os comentários da pesquisa refletiram parte dessa ambiguidade, com um entrevistado observando que resolveu essa etapa com um software de segurança robusto.

Na realidade, a implantação de controles gerais de cibersegurança pode não proteger adequadamente os sistemas altamente críticos nos níveis necessários. Os sistemas operacionais e de negócios com o mais alto nível de criticidade geralmente devem ser fortalecidos com segmentação de rede adicional, controles de acesso e de identidade, como autenticação multifator e medidas relacionadas. Identificar e priorizar a criticidade primeiro garante que as estratégias de segurança adicionais corretas sejam aplicadas adequadamente para lidar com o risco, sistema por sistema.

Zero Trust é uma prática recomendada de segurança crescente em todos os setores. Ela também está no radar do governo federal dos Estados Unidos para que as organizações de infraestrutura crítica implementem, e ele tem um papel a desempenhar nesta etapa de identificação de sistemas críticos para os negócios.

Zero Trust não é um modelo de segurança "tudo ou nada" – pode ser abordado de vários ângulos e aplicado de forma incremental, mesmo em pequenas etapas. Identificar e priorizar o que é mais crucial para a organização é uma etapa fundamental nessa jornada incremental, gerando os insights para colocar os controles Zero Trust onde eles são mais necessários.

Os sistemas críticos de negócios estão identificados e priorizados?

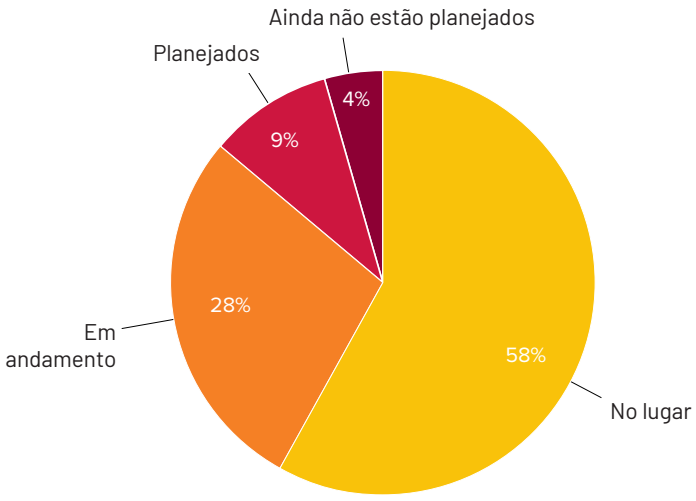


Figura 1

RECOMENDAÇÕES

Tomando emprestado a estratégia Zero Trust, examine todos os elementos DAAS da organização – dados, ativos, aplicativos e serviços – e priorize cada um com base na criticidade. Essas são as 'Superfícies protegidas' da organização, cada uma obtendo os controles de cibersegurança corretos aplicados em ordem de prioridade.

Na infraestrutura crítica, aplicativos e dados ICS e da linha de produção são exemplos de sistemas prováveis de serem críticos nos negócios. Pergunte às suas equipes de negócios, operações, TI e segurança o que acontece se esses sistemas forem bloqueados por um ataque de ransomware. Quais sistemas permitem operações de produção, segurança ou integridade de dados, comunicações, continuidade da cadeia de fornecimento ou simplesmente a capacidade de fornecer serviços aos clientes para ajudar no exercício de priorização.

SEÇÃO 2

Proteção e Implementação de Salvaguardas

A transformação digital, a digitalização de processos e a tecnologia IoT, juntamente com a convergência de TO e TI resultante, melhoraram a eficiência e a confiabilidade da infraestrutura crítica, permitindo que os provedores atendam melhor ao público e forneçam serviços de maneira mais econômica.

Embora esses desenvolvimentos sejam positivos, eles expuseram as organizações de infraestrutura crítica a novas ameaças e vulnerabilidades decorrentes da maior exposição à Internet por meio de sensores e dispositivos, trabalhadores remotos, APIs de terceiros e controladores lógicos programáveis não seguros, gateways, atuadores e muitos outros componentes.

Os controles de segurança para sistemas de TO diferem das práticas de TI porque muitos componentes de TO geralmente carecem de proteções básicas. Muitas vezes, os sistemas em obsolescência que controlam a produção nem mesmo podem ser corrigidos e, se forem, não serão corrigidos na velocidade normal de TI – juntamente com outras manutenções do chão de fábrica.

Além disso, a segurança de TO está se movendo para ficar mais sob a responsabilidade do CISO, mas muitos CISOs não entendem totalmente as implicações do gerenciamento de TO e, por extensão, a segurança IoT. Por outro lado, os líderes de engenharia de fábrica devem preservar o tempo de disponibilidade de forma confiável e não podem se dar ao luxo de derrubar redes de TO por longos períodos para corrigir falhas de segurança, especialmente não durante a operação.

Talvez isso esteja por trás dos resultados da pesquisa, mostrando que apenas 28% dos entrevistados têm, hoje, um roteiro de segurança de TI/TO convergente, com outros 35% indicando que a etapa está em andamento. As organizações de infraestrutura crítica devem seguir o exemplo da indústria de fabricação e maquinário, onde 84% dos entrevistados indicaram que já alcançaram essa convergência ou a têm em seu roteiro. Claramente, os outros setores devem ganhar muito terreno para alcançá-los.

No entanto, a marcha para a convergência continuará. Para criar um roteiro convergente robusto, os líderes de TI e TO precisam mergulhar juntos em um verdadeiro processo de planejamento conjunto. A Rockwell Automation normalmente recomenda aos nossos clientes reservar uma semana inteira para que um orientador de processo experiente possa orientar as duas equipes na identificação de todos os elementos, barreiras e requisitos de segurança. Essa abordagem consegue a aceitação de todas as partes interessadas à medida que decisões importantes são tomadas.

Alguns clientes também criam um Centro de Excelência em Cibersegurança (COE), reunindo TI, TO e grupos das partes interessadas do negócio para trabalharem juntos continuamente para criar sistemas funcionais e solucionar problemas juntos quando surgem novos problemas.

Acesso remoto seguro

Os atacantes explorarão qualquer caminho que possa criar uma porta aberta dentro de uma organização. Com a mudança promovida pela pandemia para locais de trabalho completamente remotos ou híbridos e o aumento geral da mobilidade do trabalhador, o acesso remoto pouco seguro tornou-se um alvo fácil.

Os sistemas de acesso remoto geralmente usam segurança desatualizada, muitas vezes contando apenas com senhas e sem autenticação multifator (MFA). Nos setores de serviços públicos, extração de petróleo/gás e mineração, as credenciais de login são o tipo de dados mais comumente exposto em violações[3], e a abundância de credenciais roubadas e vazadas na dark web facilita a invasão de sistemas de acesso remoto por hackers mal-intencionados. Portanto, enquanto 69% dos entrevistados relatam ter acesso remoto seguro, o resultado é potencialmente enganoso em termos de proteção de acesso remoto adequada.

A pandemia do COVID-19 criou um desafio e um benefício a esse respeito. Um de nossos entrevistados observou que os modelos de trabalho híbrido dificultaram o acesso remoto consolidado, enquanto outro disse que o "modelo de trabalhar de qualquer lugar" que se tornou padrão durante a pandemia obrigou as organizações a prestarem mais atenção.

RECOMENDAÇÕES

Um programa confiável de gerenciamento de identidade e acesso (IAM) é fundamental para uma estratégia Zero Trust. O IAM fornece visibilidade a respeito de quem está solicitando acesso, a quais aplicativos e dados, de onde, usando qual dispositivo, a que horas – e controla outras normas comportamentais aprovadas. Isso permite monitorar e aplicar políticas e controles de acesso. Uma solução IAM que integra MFA pode reduzir significativamente a ameaça de senhas comprometidas.

Zona industrial desmilitarizada (IDMZ)

A criação de uma rede isolada (air gap) entre os sistemas ICS e TO e a TI usando uma IDMZ é uma base inicial do projeto de cibersegurança de rede que ajuda a garantir que os atacantes não possam se mover lateralmente para redes e controladores de TO se obtiverem acesso aos sistemas de TI – e vice-versa. De acordo com as respostas da pesquisa, cerca de 50% das organizações têm um IDMZ dentro de sua arquitetura de TO e outros 25% estão trabalhando nisso (Figura 2).

O setor de cuidados com a saúde, setor de saúde pública e serviços de emergência estão especialmente atrasados – 38% dos entrevistados ainda não têm uma IDMZ planejada, em comparação com 16,5% em todos os setores. Essas descobertas se alinham com o que a Rockwell Automation vê no mercado mais amplo.

As redes isoladas da IDMZ não são o ponto final para a cibersegurança, especialmente porque os sistemas de TO e os dispositivos IoT podem se conectar diretamente à Internet por meio de redes de TI. Medidas adicionais devem ser implementadas para uma defesa robusta.

Qual é o status da implementação de uma Zona Desmilitarizada Industrial (IDMZ) dentro da arquitetura de segurança de TO?

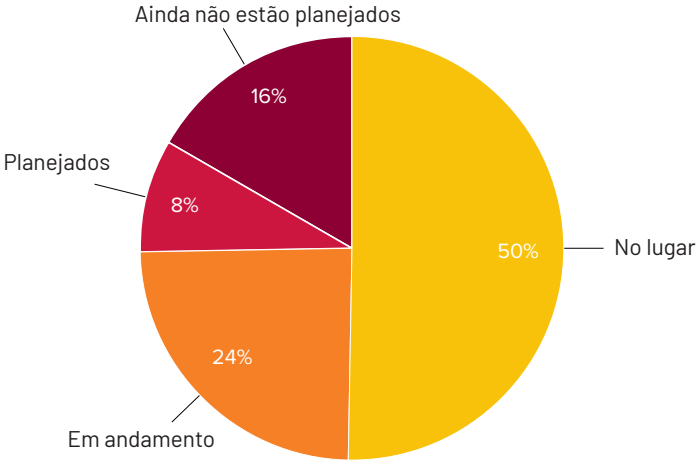


Figura 2

RECOMENDAÇÕES

Para uma arquitetura segura, implemente o IDMZ como uma prática recomendada básica. Separar redes e ativos de TI e TO uns dos outros garante que os atacantes não possam se mover entre os dois sistemas. No entanto, lembre-se de que a arquitetura moderna de segurança da infraestrutura crítica deve incluir defesas adicionais, especialmente em torno das superfícies de proteção críticas para os negócios e em todos os ativos habilitados para a Internet.

[3] Verizon, "Relatório de investigações de violação de dados de 2021" maio de 2021

Gestão de patches

O patch de correção de TO é um ponto de atenção significativo. A pesquisa validou o que é visto rotineiramente no campo: a gestão de patches não é considerada uma prática importante, não é financiada ou simplesmente muito complicada de realizar. Entre nossos participantes, apenas 37% implementaram uma gestão de patches de TO eficaz e 13% ainda nem planejaram uma abordagem de em relação aos patches (Figura 3).

Na fabricação e maquinário verticais, 42% das organizações pesquisadas não possuem uma gestão de patches eficaz implantada ou mesmo em andamento. As principais indústrias que estão à frente das demais no progresso desse tópico são as de manufatura nos EUA e Reino Unido/Irlanda, e as financeiras no Oriente Médio e Ásia-Pacífico (APAC).

Essas descobertas são alarmantes em todos os aspectos, considerando a taxa de vulnerabilidades descobertas e o risco de malware oculto à espreita.

Muitos sistemas de TO não podem ser corrigidos normalmente devido à funcionalidade limitada e pequena e/ou estruturas obsoletas que não permitem a incorporação de componentes de segurança. A correção também pode levar um dia inteiro [cada] quando você tem dezenas ou centenas de servidores de rede – incrivelmente caro em termos de tempo de parada, portanto, os operadores da fábrica historicamente têm resistido às abordagens de TI para correção.

Qual é o status da gestão eficaz de patches de TO?

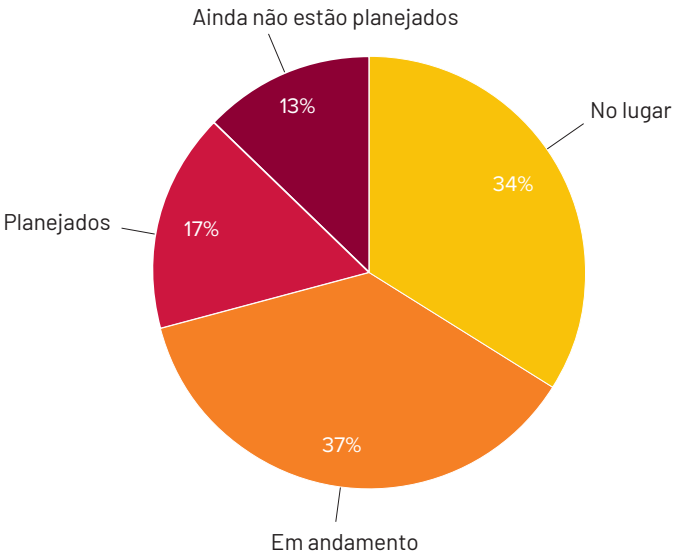


Figura 3

Lacunas de segurança adicionais

- **Mídia removível.** Pouco mais da metade das organizações citou procedimentos de segurança eficazes para mídias removíveis. Quanto ao resto, qualquer pessoa pode efetivamente coletar dados a qualquer momento ou adentrar e potencialmente inserir malware nas redes. Basta olhar para os casos de pessoas com acesso interno como Snowden e Manning para entender as possíveis implicações. Um entrevistado, cuja organização está trabalhando em uma correção, ofereceu este excelente insight: "Configure sua próxima geração de ferramentas de detecção e resposta de endpoint (EDR) para não permitir cartões de memória".
- **Segmentação de rede** Em uma história semelhante, apenas 49% das organizações implementaram segmentação ou microssegmentação para proteger sistemas críticos de negócios. Este é um componente essencial das Melhores práticas exigido por muitas políticas governamentais e um componente central do Zero Trust. Dada a eficácia da abordagem Zero Trust, é provável que sejam exigidas mais ordens dos provedores de infraestrutura crítica para segmentar as redes de maneira eficaz.
- **Conscientização dos funcionários.** 69% das organizações implementaram programas de conscientização, treinamento e teste de segurança dos funcionários. O setor financeiro e bancário da Ásia-Pacífico e do Oriente Médio lidera neste quesito, enquanto o setor de viagens e transporte dos EUA não citou nenhum treinamento. Quase ⅓ das organizações em geral não implementou o treinamento de segurança, que é uma das melhores práticas da estrutura do NIST e é altamente recomendada. O treinamento de conscientização é uma medida de proteção comprovada para prevenir e interromper ataques que começam com phishing (86% das violações confirmadas). Independentemente de seu programa estar nas mãos do RH ou da TI, certifique-se de que ele cobre as ameaças de cibersegurança e as melhores práticas específicas para a TO. Também recomendamos testes de penetração para ajudar a identificar as áreas em que os funcionários precisam de mais treinamento.

RECOMENDAÇÕES

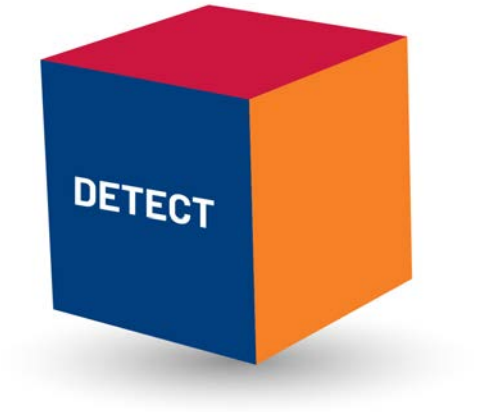
Os atacantes estão constantemente procurando por vulnerabilidades. Nenhuma organização, especialmente aquelas de Infraestrutura Crítica, pode seguir em frente no estilo "Fazendo como sempre fizemos". À medida que aumenta o risco de tempo de parada não programada devido a ataques cibernéticos, o equilíbrio risco-recompensa entre não fazer nada e, finalmente, abordar as complexidades da instalação de patches de TO deve se inclinar naturalmente para a prevenção, dado o alto potencial de perdas e danos.

A gestão eficiente e eficaz de patches de TO começa com experiência industrial intensa e especialização em cibersegurança de TO. Esse conhecimento ajuda a evitar armadilhas comuns e aproveita as melhores práticas de várias implementações bem-sucedidas. Trabalhar com um parceiro que entende a dinâmica dos ambientes de produção, juntamente com as implicações severas do tempo de parada não programada devido a incidentes cibernéticos, pode simplificar esse processo complexo, mas necessário, e executar a instalação de patches de TO com interrupções minimizadas.

[4] Verizon, "2021 Data Breach Investigations Report," maio de 2021

SEÇÃO 3

Detecção de ameaças e identificação de eventos de cibersegurança



Um princípio central da segurança Zero Trust é a suposição de que uma violação já ocorreu; nenhuma conexão ou solicitação de acesso deve ser confiável até que seja verificada e autenticada, dinamicamente, todas as vezes. Esse princípio se baseia no monitoramento constante de atividades maliciosas em tempo real para detectar e reduzir ameaças.

Infelizmente, as respostas da pesquisa mostram que a detecção de ameaças é um ponto cego para organizações de infraestrutura crítica. Isso significa que ataques a sistemas de TO podem passar despercebidos e as organizações não estão lidando com os riscos de ataques frequentes, como ransomware, que podem debilitar as operações; atores de estado-nação que conduzem atividades de espionagem de longo prazo; e invasores que podem estar se movendo por sistemas e cadeias de fornecimento se preparando para um ataque em larga escala.

Detecção de ameaças e anomalias por meio de um SOC de TO

Um Centro de Operações de Segurança (SOC) de TO reúne as tecnologias, ferramentas, talentos e outros recursos para monitoramento e resposta a ameaças 24 horas por dia, 7 dias por semana. Um SOC de TO é indispensável para detectar ameaças e anomalias rapidamente e minimizar o impacto em sistemas críticos para os negócios. Nossa pesquisa constatou que 43% das organizações atualmente não possuem detecção de ameaças e anomalias em tempo real por meio de um SOC de TO (Figura 4), revelando uma ampla deficiência na preparação para cibersegurança.

A região Ásia-Pacífico, Austrália e Nova Zelândia está atrasada na implementação do SOC de TO, tendo "ainda não planejado" como a principal resposta. Entre os entrevistados nesta região, 31% não têm um SOC de TO planejado, em comparação com 16% em todo o mundo. Aprofundando ainda mais nos dados, não encontramos organizações na indústria de energia e nuclear da região com um SOC em vigor ou mesmo planejado. Para comparação, 74% das organizações no Oriente Médio e na África implementaram um SOC automatizado ou estão trabalhando nele, com dois setores verticais abrindo o caminho: financeiro e bancário; e energia e nuclear.

Além disso, 47% dos entrevistados não implementaram uma plataforma de gerenciamento de eventos e informações de segurança (SIEM) para analisar alertas de segurança de aplicativos e hardware de rede. Embora a maioria dos sistemas SIEM não gere alertas verdadeiramente em "tempo real", alguns chegam muito perto, tornando-os um item básico em seu conjunto de ferramentas SOC e um componente crítico da defesa eficaz da infraestrutura crítica.

Qual é o status da implementação da detecção de ameaças e anomalias em tempo real via SOC de TO (serviços próprios ou gerenciados) para malware, ransomware e vulnerabilidades?

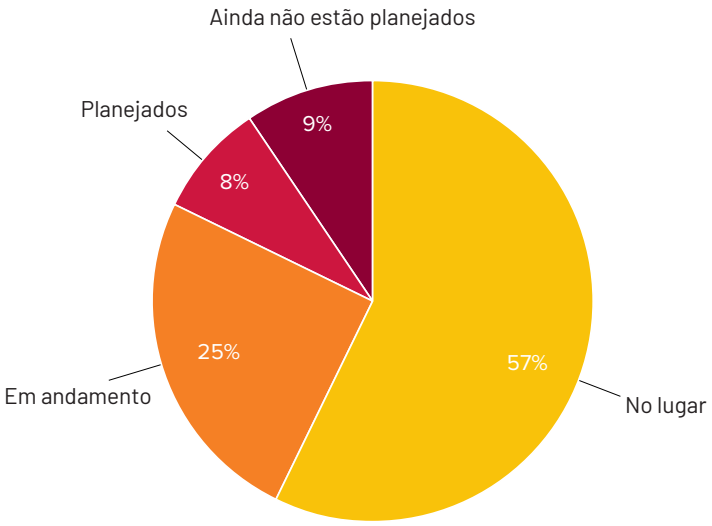


Figura 4

RECOMENDAÇÕES

Restrições de recursos, como a falta de talentos internos, podem criar obstáculos intransponíveis para a capacidade de muitas organizações de monitorar e detectar ameaças, mas essa é uma necessidade fundamental no atual ambiente de ameaças de TO em evolução. Aproveite as soluções de SOC de TO de terceiros que incluem serviços como monitoração contínua de ameaças e resposta a incidentes.

Ao trabalhar com um parceiro de SOC de TO confiável, você obtém a experiência real de uma equipe de segurança altamente treinada, mas também informações em tempo real obtidas de todos os clientes que usam o SOC. Um SOC de TO gerenciado também evita altos custos CapEx e garante que as mais recentes ferramentas, técnicas e insights de inteligência de ameaças sejam implantados em seu benefício – algo vantajoso considerando a escassez mundial de profissionais de segurança treinados, estimada em 2,72 milhões ((ISC)² 2021 Cybersecurity Workforce Study).

Protegendo Endpoints

De sensores de Internet das coisas industrial e dispositivos pessoais dos funcionários a controladores, a proliferação de endpoints expande enormemente a superfície de ataque de TO. Proteger as operações nesse ambiente é um problema crescente. Entre os líderes de segurança pesquisados, 46% não monitoram e controlam endpoints 24 horas por dia, 7 dias por semana em tempo real atualmente (Figura 5). Isso significa que grande parte dos dispositivos conectados aos sistemas de TO não estão configurados corretamente ou contêm falhas de segurança. As organizações podem ter sorte, mas na maioria dos casos é apenas uma questão de tempo até que os atacantes usem esses endpoints não seguros e não monitorados em ataques cibernéticos.

Qual é o status de ter todos os endpoints com acesso controlado e monitorado em tempo real 24 horas por dia, 7 dias por semana?

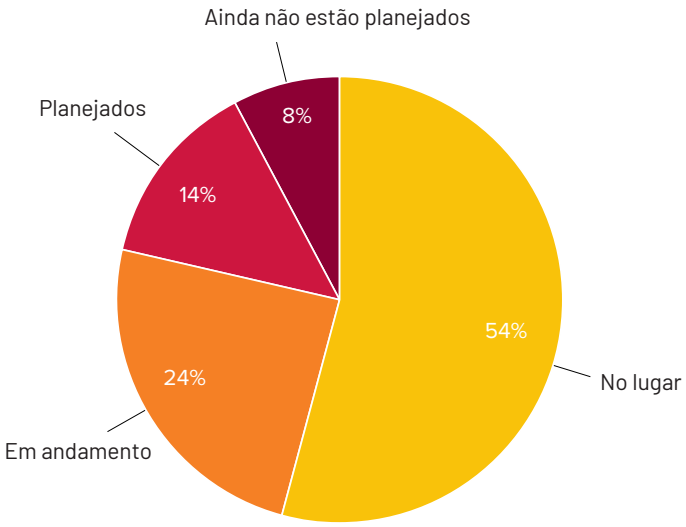


Figura 5

RECOMENDAÇÕES

Endpoints são uma área para reforçar rapidamente. Comece conduzindo a avaliação de inventário de ativos de rede discutida anteriormente para identificar todos os terminais conectados à sua rede. Uma vez identificados e avaliados seus riscos de segurança, você pode desenvolver um plano, com base em seus sistemas críticos de negócios e prioridades de segurança identificados, para as ferramentas, equipe e serviços necessários para fortalecer os perímetros em torno desses pontos de entrada.

SEÇÃO 4

Respondendo a Incidentes Cibernéticos

O planejamento e a preparação da resposta a incidentes são cruciais. As preparações corretas minimizarão o tempo de parada, as perdas financeiras, as interrupções de clientes e outros impactos negativos de incidentes de cibersegurança. Para provedores de infraestrutura crítica, a velocidade de resposta é especialmente urgente devido à extensão dos danos possíveis, incluindo serviços públicos e questões de segurança, em alguns casos para até milhões de pessoas.

As organizações de infraestrutura crítica estão avançando, pois 57% relataram recursos para analisar, conter e reduzir ameaças cibernéticas (Figura 6). No entanto, também detectamos que esta é uma área angustiante, talvez devido à mudança constante e rápida do cenário de ameaças. Um participante comentou: "Alguém descobriu isso?" Outro entrevistado pergunta: "Como as organizações de infraestrutura crítica planejam abordar a continuidade e a resiliência dos negócios enquanto ainda estão descobrindo como desenvolver uma estratégia básica de resposta a incidentes?"

Qual é o status da análise de ameaças cibernéticas, contenção de ameaças e recursos de redução de ameaças?

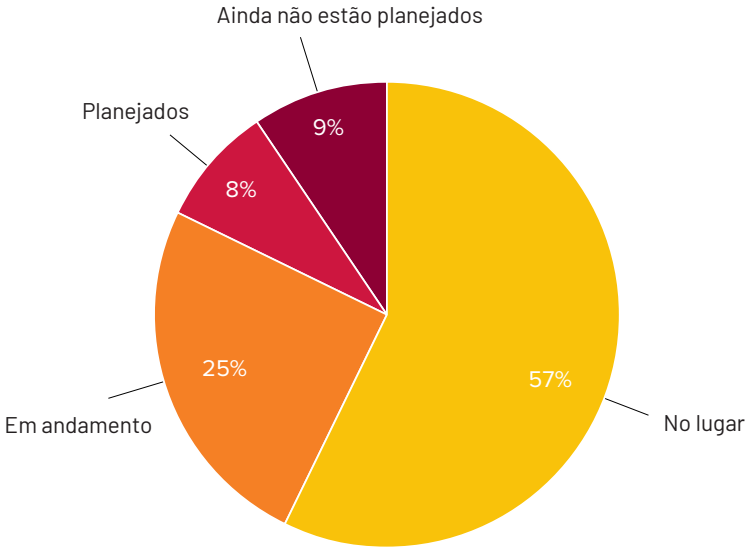


Figura 6

RECOMENDAÇÕES

Se os recursos e a experiência forem um problema no desenvolvimento de sua estratégia de resposta a incidentes, considere um provedor de serviços gerenciados – como um parceiro de SOC de TO – para agir rapidamente e evitar obstáculos nos esforços para contratar diretamente talentos experientes em cibersegurança, devido à escassez global de pessoal. Um parceiro de SOC de TO experiente com profundo histórico industrial, como a Rockwell Automation, pode garantir que você tenha um plano de resposta a incidentes eficaz pronto, mas também pode entrar em ação em seu nome para ajudar a bloquear e reduzir ataques, se necessário. Equipes de especialistas também realizam treinamento contínuo e testes de cenário para validar a capacidade de responder rapidamente. Além disso, um parceiro de SOC de TO de alta qualidade trará uma compreensão profunda dos requisitos de conformidade de TO e seus relatórios.

SEÇÃO 5

Recuperando-se Após um Incidente

46% dos participantes da pesquisa disseram que estão prontos hoje mesmo com processos de recuperação, sistemas, dados e procedimentos operacionais para restaurar as operações rapidamente após um ataque cibernético.

Em termos de recuperação de um ataque cibernético, o que conta como "rápido"? Em alguns casos, uma semana pode ser considerada adequado. Em outros, cada minuto importa.

Por exemplo, quando as empresas de energia sofreram interrupções durante a grande tempestade de neve de 2021 no Texas, uma semana de inatividade significou centenas de vidas perdidas. No caso do ataque de ransomware da Colonial Pipeline, mesmo 24 horas sem recuperação significavam milhões de dólares em custos e um impacto econômico incalculável decorrente da perda de suprimentos de gás na costa leste dos EUA.

Embora o retorno às operações normais seja o foco principal da fase de recuperação de incidentes, também é uma oportunidade para identificar áreas que precisam ser melhoradas. A implementação de mudanças significativas com base nos aprendizados dos incidentes cria uma cultura de melhoria contínua da cibersegurança, gerando sistemas cada vez mais resilientes e protegidos.

Aproveitando o Financiamento Federal

Em novembro de 2021, o Congresso dos EUA promulgou um projeto de lei de infraestrutura (H.R. 3684, Lei de Investimento e Trabalho em Infraestrutura) destinando cerca de US$ 2 bilhões para atualizações e aprimoramentos de cibersegurança na infraestrutura crítica. $ 1 bilhão do valor está previsto para subsídios de financiamento para organizações estaduais, locais, da sociedade e certas organizações sem fins lucrativos. As diretrizes de submissão de subsídios estão pendentes, no entanto, a Rockwell Automation espera que os subsídios se alinhem aos recursos da Estrutura de cibersegurança NIST devido ao uso da estrutura pela Agência de Cibersegurança e Infraestrutura (CISA).

Cerca de um terço dos entrevistados (29%) possui um plano de cibersegurança em vigor adaptável para envio de subsídios. Outros 25% têm um plano em desenvolvimento. Isso deixa aproximadamente 40% das organizações sem esse nível de preparação.

Um plano de cibersegurança não apenas permite que as organizações almejadas solicitem subsídios rapidamente quando disponíveis, mas também ajuda a colocar em ação o tipo certo de programa sistemático de cibersegurança que irá expor lacunas, reduzirá os riscos e ajudará a priorizar os esforços para proteger a organização e seus clientes de impactos nocivos.

A Rockwell Automation incentiva todos os líderes de infraestrutura crítica a se familiarizarem com esta legislação, preparar um plano de avaliação inicial e buscar financiamento se os subsídios forem aplicáveis à sua organização. Não espere até que os requisitos de subsídio sejam divulgados – tome medidas agora para começar a preparar e desenvolver seu plano. A Rockwell Automation criou um modelo de planejamento de cibersegurança e uma lista de verificação usando a estrutura NIST: **Faça o download do modelo de planejamento**

RECOMENDAÇÕES

O planejamento de recuperação e restauração deve ser uma prática operacional tão comum quanto a manutenção de ativos, fundamental para um tempo de disponibilidade operacional confiável. Os custos financeiros e humanos do tempo de parada não programada continuam aumentando e você não pode contar com a transferência do ônus do risco para sua seguradora. À medida que a responsabilidade cresce e a possibilidade de seguro se torna mais limitada, o ônus reverterá para o segurado para cobrir a maior parte das perdas e custos de recuperação.

PRÓXIMAS ETAPAS

Preparando-se para o futuro

Todo provedor de infraestrutura crítica deve agir agora para evitar O grande desligamento. Vidas, bem-estar, segurança e meios de subsistência dependem disso.

A cibersegurança de TO não é fácil. Por outro lado, a maioria das violações tem defesas conhecidas. As organizações de infraestrutura crítica fizeram grandes avanços em eficiência e confiabilidade por meio da transformação digital e automação; agora eles devem enfrentar a cibersegurança com a mesma tenacidade. Os resultados da pesquisa mostram que o setor está despertando para a necessidade de uma cibersegurança moderna e focada, embora lentamente – com grandes lacunas remanescentes, prioridades mal definidas e falta de clareza em relação aos riscos e melhores práticas.

No entanto, os líderes da infraestrutura crítica estão começando a prestar atenção. Muitos entrevistados relataram planejar ou ter proteções importantes em andamento. O setor está passando de uma baixa conscientização sobre esse assunto para uma reatividade após ataques significativos aparecerem nas notícias e a consequente resposta do governo, para perguntar como a cibersegurança pode ser acelerada em suas organizações.

Rockwell Automation: Protegendo aquilo do que o mundo depende

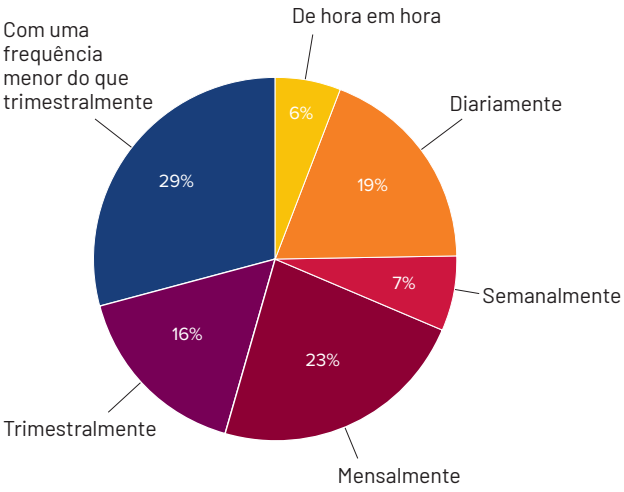
A Rockwell Automation oferece uma variedade de soluções e serviços de segurança industrial para ajudá-lo a gerenciar ameaças e aumentar a resiliência de seu ecossistema de TO e TI. Nossos especialistas podem ajudá-lo a criar uma infraestrutura de rede robusta e segura, além de ajudá-lo a se defender contra as ameaças e responder rapidamente aos incidentes. Além da profunda experiência e conhecimento das melhores práticas mais recentes, trazemos a sabedoria em operações de produção de mais de 100 anos em automação industrial. Nossa presença em todo o mundo permite que os clientes apliquem proteções de cibersegurança em escala global em vários locais com logística tão bem ajustada quanto você esperaria do líder do setor em automação industrial.

RECOMENDAÇÕES

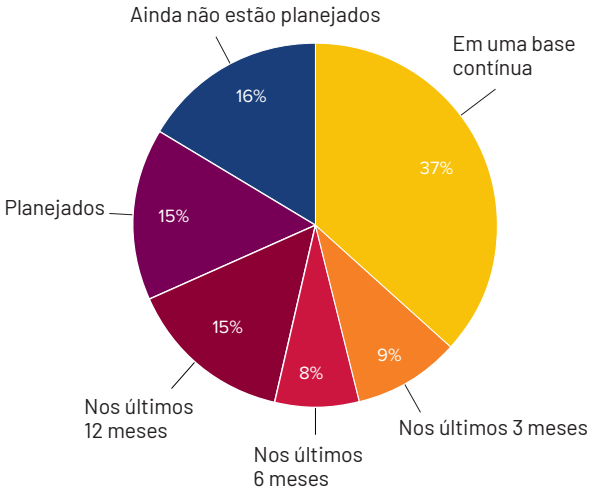
- Faça a **avaliação de preparação para cibersegurança da Rockwell Automation** e receba um relatório personalizado, comparado com os entrevistados originais da pesquisa. Veja como sua organização se compara por setor industrial, tamanho da empresa e região.
- Baixe nosso **Modelo de plano de cibersegurança de TO** para obter informações avançadas sobre ferramentas, serviços e equipe para defender suas operações com eficiência. Organizações de infraestrutura crítica dos EUA: use o Modelo de plano para ajudar a se preparar para o subsídio de financiamento que pode ajudar a fechar as lacunas de cibersegurança.
- **Fale com um profissional da Rockwell Automation** e saiba como podemos ajudá-lo com o programa certo de cibersegurança de TO para melhor proteger suas operações industriais.

APÊNDICE

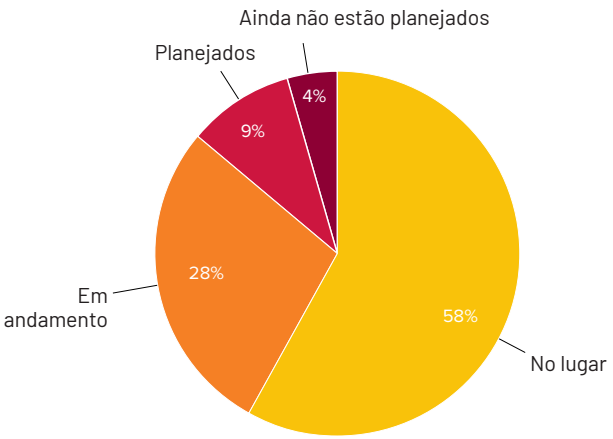
Com que frequência o inventário de base instalada é avaliado?



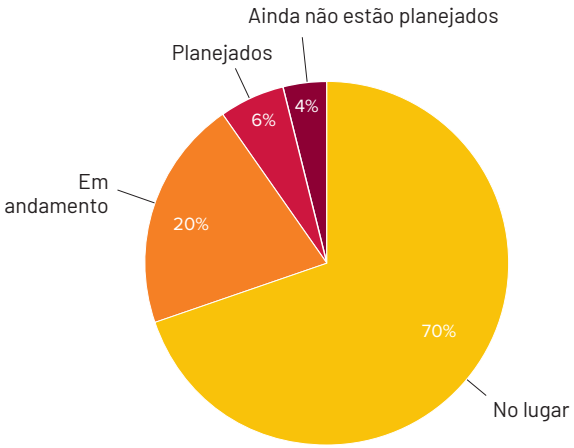
Com que frequência é realizada uma avaliação de risco da cadeia de fornecimento?



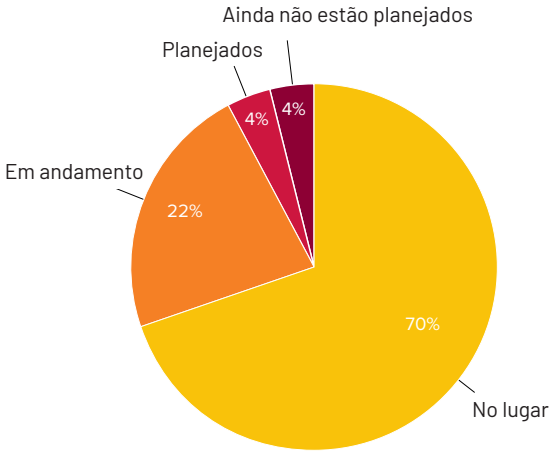
Os sistemas críticos de negócios foram identificados e priorizados?



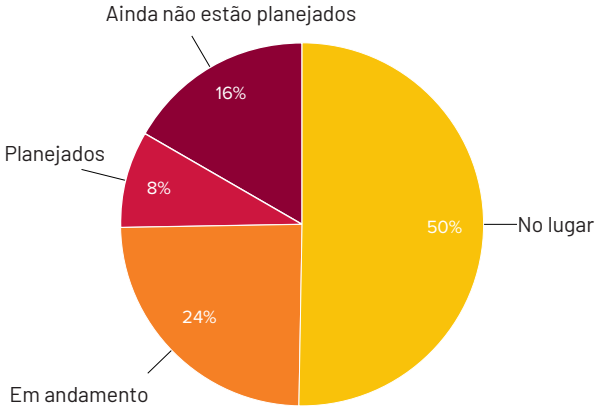
Qual é o status dos controles de acesso remoto para login externo seguro?



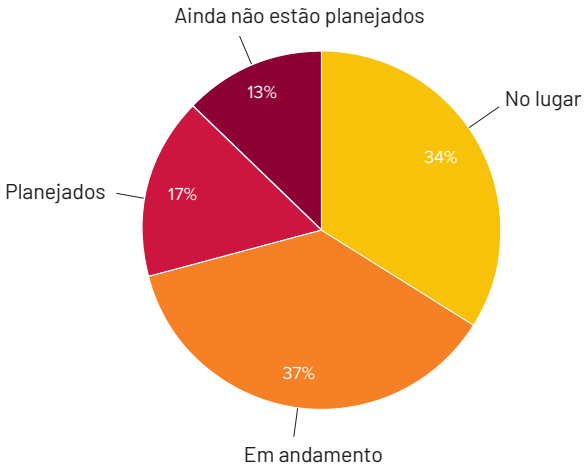
Qual é o status dos controles de acesso físicos que identificam e impedem o acesso não autorizado ao sistema?



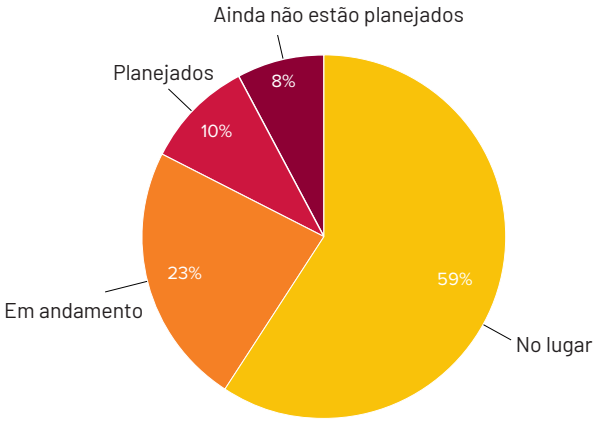
Qual é o status da implementação de uma Zona Desmilitarizada Industrial (IDMZ) dentro da arquitetura de segurança de TO?



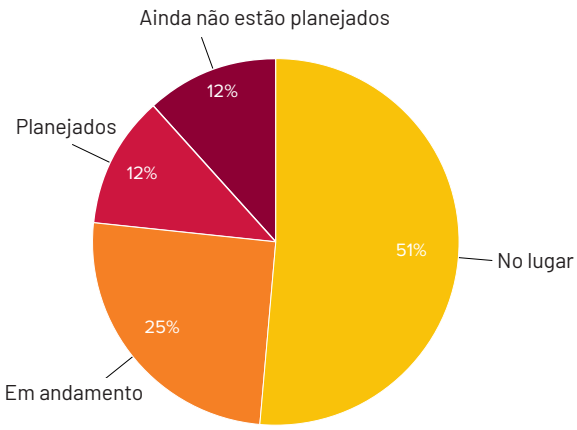
Qual é o status da gestão eficaz de patches de TO?



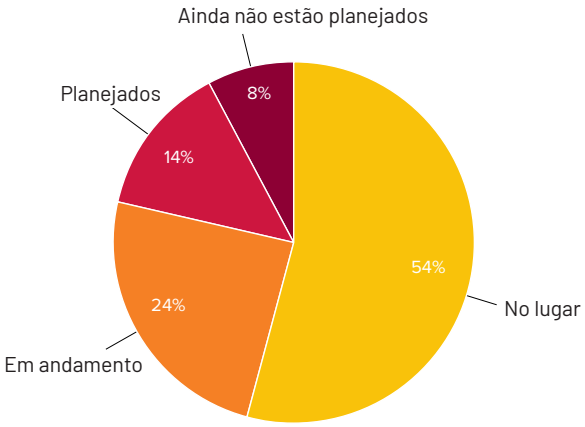
Os processos de backup de dados dos sistemas operacionais são executados regularmente?



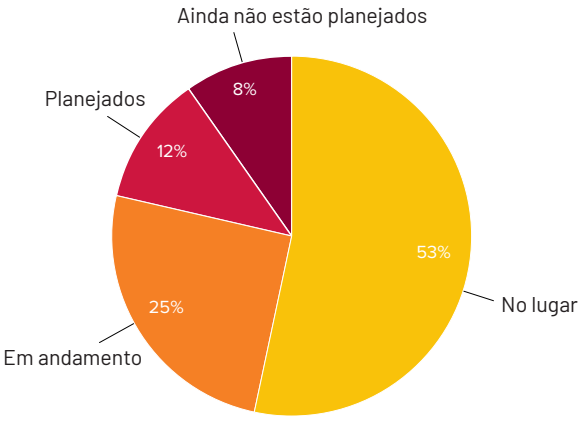
Tecnologia de proteção: Qual é o status dos procedimentos eficazes de segurança de mídia removível?



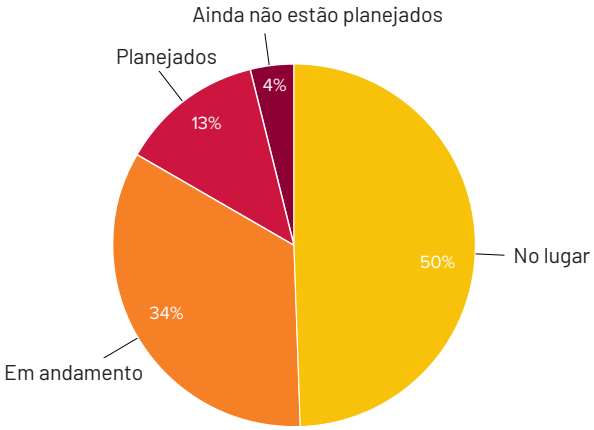
Qual é o status de ter todos os endpoints com acesso controlado e monitorado em tempo real 24 horas por dia, 7 dias por semana?



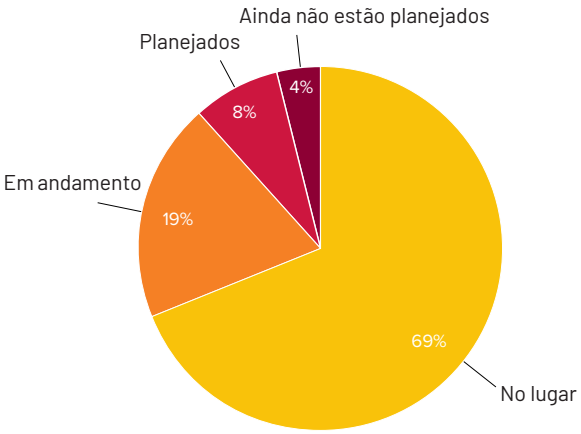
Qual é o status de um sistema de Gestão de Informações de Eventos de Segurança (SIEM), fornecendo análise em tempo real de alertas de segurança gerados por aplicativos e hardware de rede?



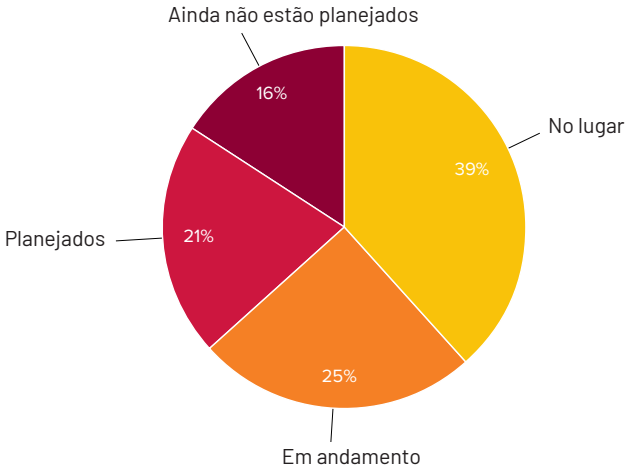
Qual é o status da implementação da arquitetura de segmentação/ microssegmentação de rede, colocando perímetros de segurança em torno de sistemas críticos para os negócios?



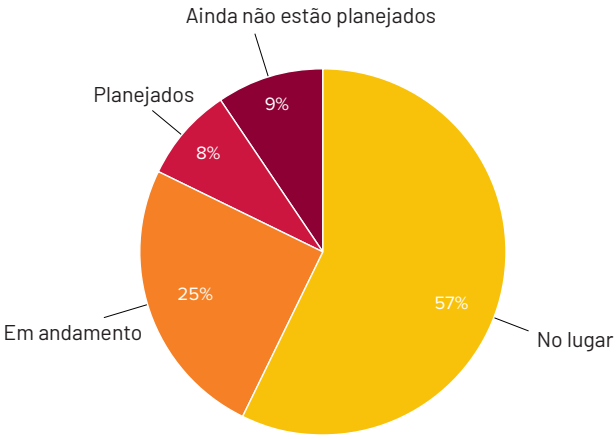
Você tem treinamento e teste de conscientização de segurança para os funcionários?



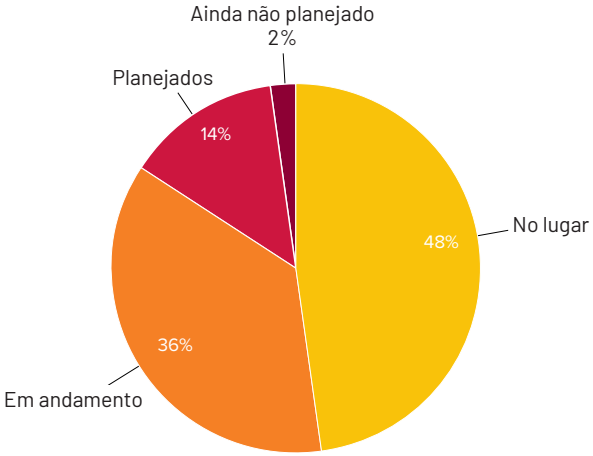
Qual é o status da implementação da detecção de ameaças e anomalias em tempo real via SOC de TO (serviços próprios ou gerenciados) para malware, ransomware e vulnerabilidades?



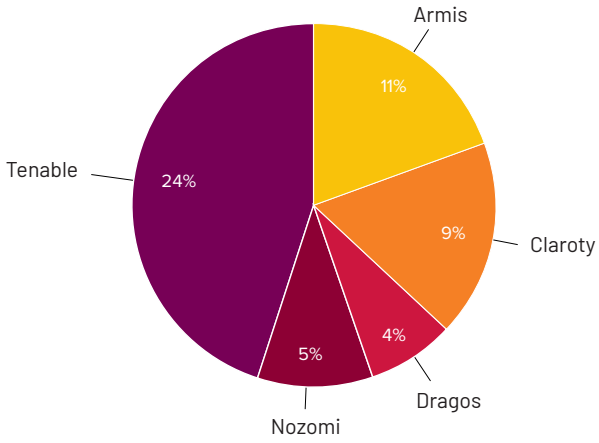
Qual é o status da análise de ameaças cibernéticas, contenção de ameaças e recursos de redução de ameaças?



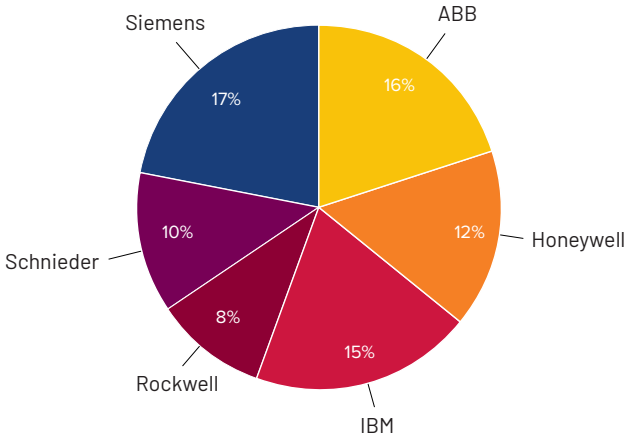
Status dos sistemas, dados e procedimentos operacionais para restaurar as operações rapidamente em caso de ataque cibernético?



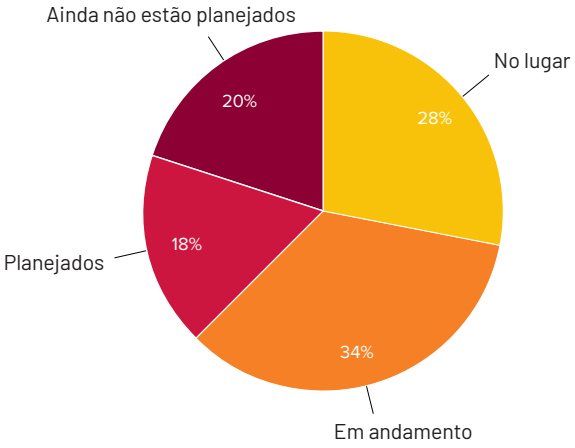
Plataformas ou serviços de detecção de ameaças de TO em uso?



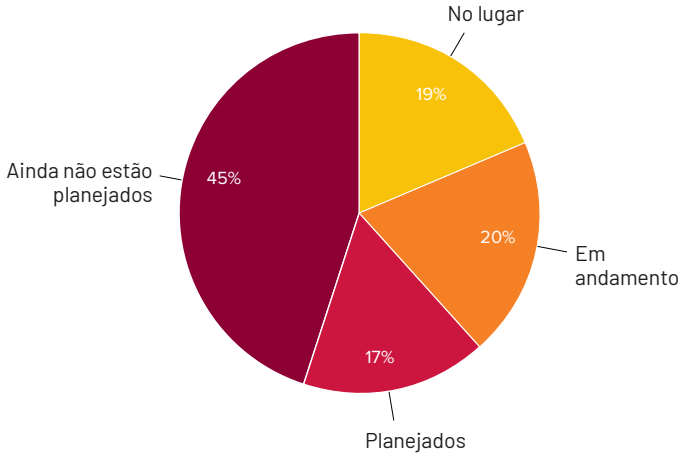
Provedores de serviços de Automação Industrial em uso?



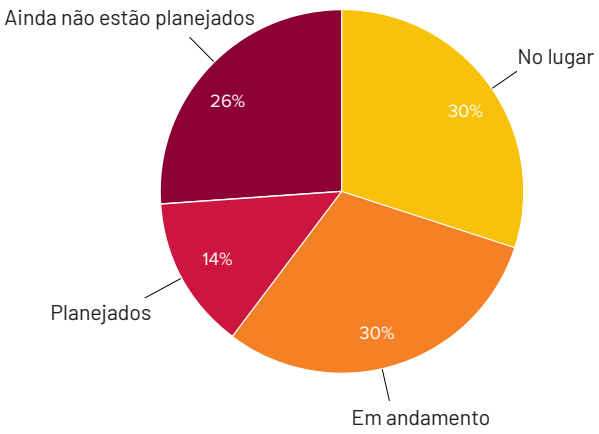
Qual é o status da implementação de um roteiro convergente de cibersegurança de TI/TO?



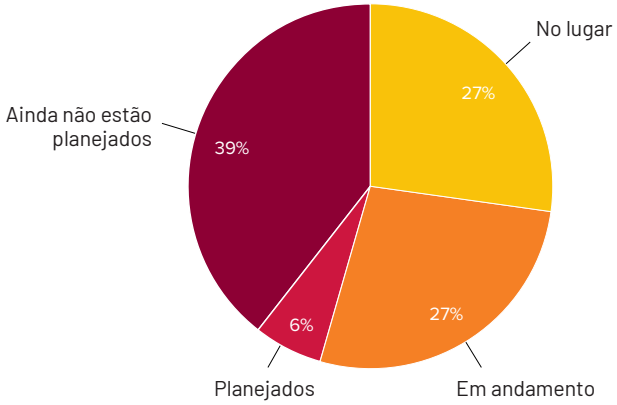
Qual é o status do uso de produtos certificados pelo Protocolo Industrial Comum (CIP) para proteger e criptografar as comunicações Ethernet?



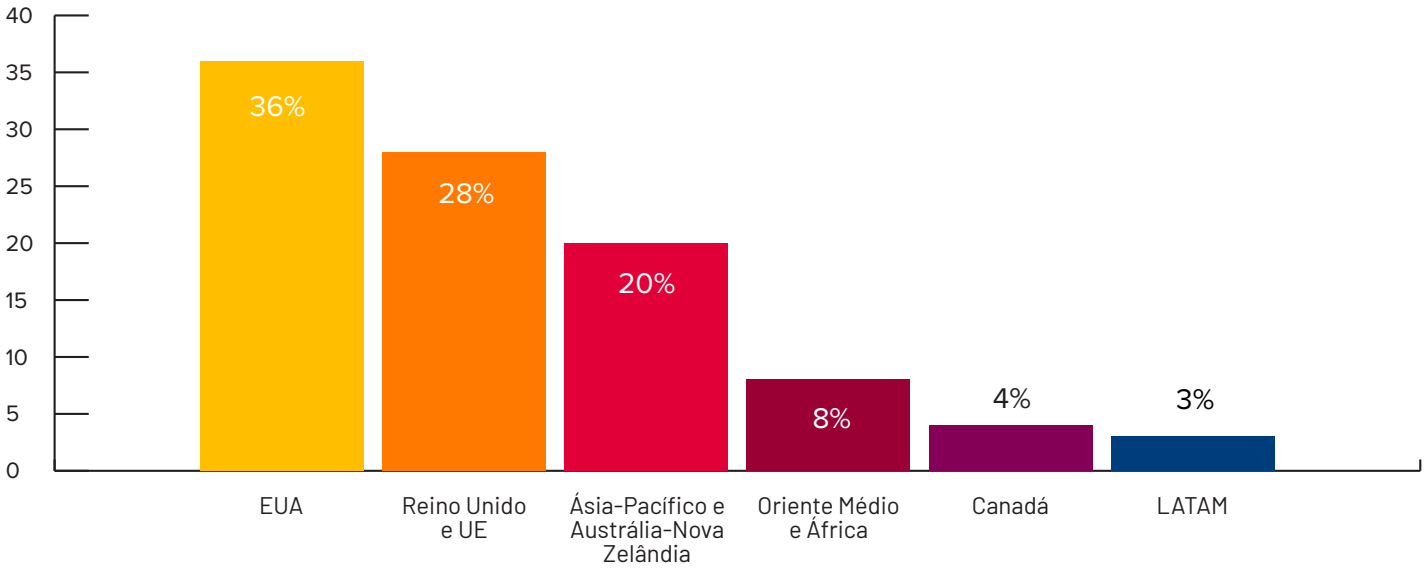
Sua organização trabalha com um ou mais parceiros de cibersegurança estabelecidos, fornecendo serviços de SOC de TO escalonáveis e atualizados dinamicamente?



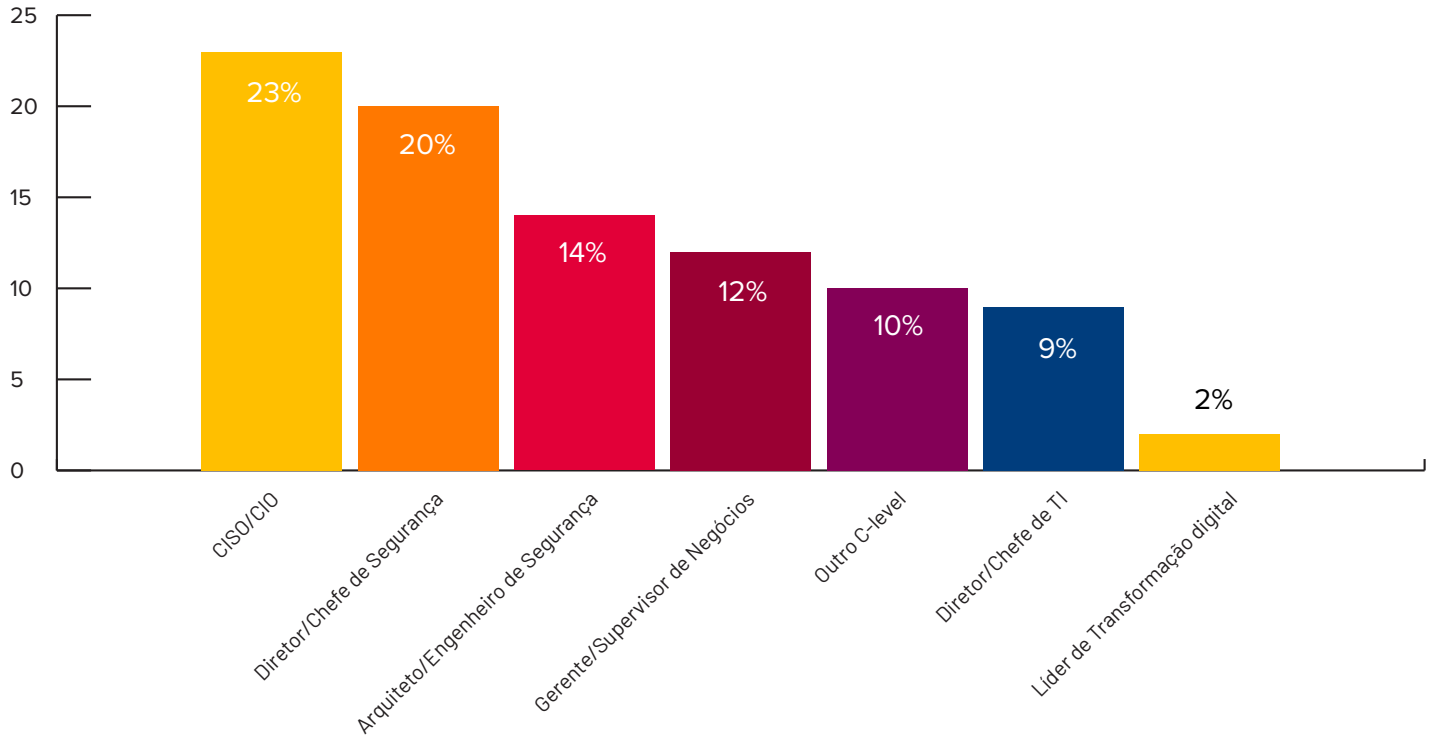
Sua organização possui um plano de cibersegurança adequado para submeter em busca de subsídios de financiamento da Lei de Infraestrutura dos EUA?



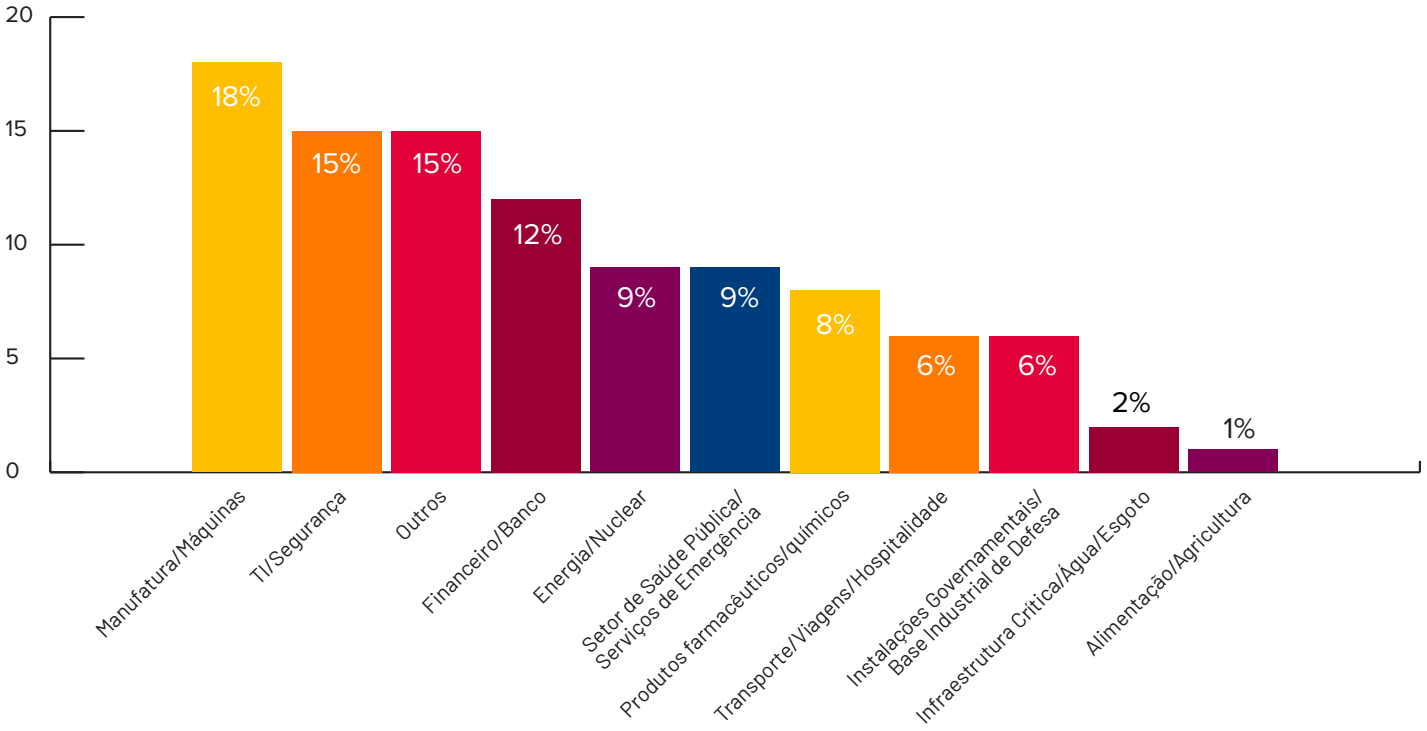
Participantes da pesquisa por região



Participantes da pesquisa por função



Participantes da pesquisa por setor da indústria



Conecte-se conosco.

rockwellautomation.com — expanding **human possibility**®

AMÉRICAS: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 EUA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
EUROPA/ORIENTE MÉDIO/ÁFRICA: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Bélgica, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
ÁSIA-PACÍFICO: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846
BRASIL: Rockwell Automation do Brasil Ltda., Rua Verbo Divino, 1488 – 1° andar, Chac. Sto Antonio, 04719-904, São Paulo, SP, Tel: (55 11) 5189-9500, www.rockwellautomation.com.br
PORTUGAL: Rockwell Automação, Lda., Av. Prof. Dr. Cavaco Silva, Edificio Ciência II, n.º 11 - 2ºC, Taguspark, Porto Salvo 2740-120, Tel.: (351) 214 225 500, www.rockwellautomation.com.pt

Publicação GMSN-SP016A-PT-P – junho de 2022