CG//One

JORNADA DE CIBERSEGURANÇA PARA A INDÚSTRIA E ENERGIA:

soluções de ponta para criar um ecossistema protegido em infraestruturas operacionais

E-BOOK

Índice

Introdução

A indústria mergulha cada vez mais na transformação digital com seus sistemas e dispositivos conectados à internet, abrindo um mundo de novas oportunidades e, junto a elas, novos desafios tecnológicos. Dentro desse contexto, a cibersegurança se torna um item essencial para minimizar os diversos riscos cibernéticos e, consequentemente, as perdas financeiras decorrentes de qualquer incidente de segurança.

Além disso, os sistemas industriais estão cada vez mais interconectados para a comunicação entre diferentes dispositivos e sistemas de controle, potencializando o risco de que um ataque a um sistema comprometa outros sistemas interconectados. Isso cria uma superfície expandida de ataque para os cibercriminosos explorarem, visando a parada das operações, roubo de propriedade intelectual ou, até mesmo, o hacktivismo (modalidade de crime motivados por ideologias ou questões políticas).

Também é importante mencionar que as ameaças cibernéticas estão evoluindo para níveis de sofisticação nunca vistos, essa infinita combinação exige uma abordagem robusta e proativa para garantir a segurança no mundo digital.

Com foco em líderes da indústria que buscam fortalecer suas defesas, este e-book oferece um guia prático para a construção de um ecossistema de cibersegurança sólido. Através de algumas soluções de ponta, você estará munido de ferramentas e estratégias para atender às crescentes demandas do setor.

O cenário

A Indústria está passando por sua Quarta Revolução Industrial, também conhecida pelo termo “Indústria 4.0”. Originado na Alemanha por volta de 2010, esse conceito impulsionou a informatização da manufatura, e suas ramificações só chegaram ao Brasil em 2013. Esse período marca o despertar das indústrias para a digitalização de suas operações, adotando um vasto conjunto de tecnologias avançadas, como inteligência artificial, robótica, internet das coisas e computação em nuvem. Essas inovações não apenas transformam os processos de produção, mas também modificam os modelos de negócios em todo o mundo.

A Tecnologia Operacional (OT, do inglês Operational Technology) refere-se aos sistemas e dispositivos empregados na automação e controle de processos físicos e operacionais em ambientes industriais. Enquanto a Tecnologia da Informação (TI) lida com computadores, redes e dados, a OT está voltada para equipamentos físicos, como sensores, atuadores, controladores lógicos programáveis (PLCs), sistemas de supervisão e aquisição de dados (SCADA) e outros dispositivos específicos da indústria.

Hoje, proteger os sistemas de Tecnologia Operacional, especialmente utilizados no setor industrial, é de vital importância. A OT administra as infraestruturas críticas que sustentam aspectos essenciais de nossas vidas, desde a gestão da rede elétrica até o funcionamento de sistemas de água e esgoto, redes de transporte, produção de bens essenciais e coordenação de cadeias globais de produção e abastecimento.

À medida que os ambientes industriais se integram cada vez mais às aplicações e redes corporativas de TI, os ativos cruciais de OT se tornam mais vulneráveis. A separação entre TI/OT dificulta a aplicação de estratégias ágeis de segurança cibernética, aumentando o risco de ameaças em tempo real e potencialmente resultando em consequências devastadoras que afetam infraestruturas, recursos e serviços.

O Relatório de 2023 da Fortinet sobre Tecnologia Operacional e Segurança Cibernética revela que três em cada quatro organizações que utilizam OT enfrentaram pelo menos uma invasão no último ano, enquanto quase um terço dos entrevistados relatou ter sido vítima de um ataque de ransomware. Isso destaca o crescente interesse do cibercrime neste setor, que ainda precisa aprimorar sua maturidade cibernética.

Uma análise dos dados de 2023 desse mesmo relatório revela que atualmente existem quatro tendências globais proeminentes:

- Houve um declínio geral nas invasões devido a menos violações internas, embora o ransomware e o phishing ainda sejam as principais ameaças. No entanto, essa diminuição pode ser atribuída ao fato dos cibercriminosos estarem adotando abordagens mais direcionadas;

- Quase todas as organizações passaram a atribuir a responsabilidade pela cibersegurança de OT a um diretor de segurança da informação (CISO), em vez de um executivo ou equipe de operações;

- Organizações e profissionais de OT têm à disposição uma ampla gama de soluções de cibersegurança para combater invasões. No entanto, indicações sugerem que produtos pontuais e a expansão de soluções descentralizadas podem dificultar a aplicação consistente de políticas em todo o cenário convergente de TI/OT;

- O número de entrevistados que consideram a maturidade de cibersegurança de suas organizações no nível 4 caiu de 21% para 13%, enquanto aqueles que acreditam estar no nível 3 aumentaram de 35% para 44%, em um ano. Essa oscilação indica uma autoavaliação mais realista por parte dos profissionais de OT em relação aos recursos de cibersegurança de suas organizações.

Os desafios

A seguir, exploraremos os principais desafios relacionados a cibersegurança que o setor industrial enfrenta atualmente, delineando estratégias e soluções para navegar neste ambiente complexo e em constante mudança.

Convergência de rede TI-OT

A convergência de rede de Tecnologia da Informação (TI) e Tecnologia Operacional (OT) é uma tendência crescente na indústria, impulsionada pela busca por maior eficiência e conectividade. Ela permite que empresas coletem, manipulem e analisem dados do sistema OT para gerar insights que podem otimizar operações, aumentar eficiências, fomentar a inovação e introduzir novos serviços.

Além disso, a convergência de TI/OT também permite usar dados do sistema de TI para atualizar e otimizar os sistemas de OT, a fim de que possam realizar suas operações físicas com mais eficiência.

No entanto, essa convergência também traz grandes desafios. Geralmente, a TI empresarial é gerenciada pelo diretor de TI (CIO), enquanto os sistemas OT são tipicamente gerenciados pelo COO. Historicamente, as implementações de TI e OT atendiam a problemas diferentes e, portanto, evoluíram para arquiteturas e protocolos significativamente diferentes. Agora, existem obstáculos estruturais e culturais para essa convergência. Na maioria das empresas, não há governança conjunta abrangendo TI e OT. Isso resulta em um número alto de processos duplicados e sobrepostos, agravado pela falta de perfis e habilidades interdisciplinares.

Outro ponto importante é que os dispositivos de OT mais antigos foram fabricados com pouca consideração para segurança, tornando-os alvo para criminosos realizarem um ataque contra toda a rede. Uma postura única de cibersegurança pode não ser suficiente para cobrir todos os dispositivos.

Internet das Coisas Estendida (XIoT)

O XIoT é um termo guarda-chuva para sistemas ciberfísicos conectados, abrangendo não apenas a tecnologia operacional, sistemas de controle industrial (ICS) e a internet das coisas industrial (IIoT), mas também outros dispositivos IoT dentro da empresa como, por exemplo, controles de elevadores e AVAC (Aquecimento, Ventilação e Ar Condicionado).

Essa revolução tecnológica dos dispositivos IoT, que deve chegar a 29 bilhões de dispositivos conectados até 2029, facilita a automação de processos, minimizando a necessidade de intervenção humana e a probabilidade de erros. Além disso, as soluções XIoT fornecem insights em tempo real de todos os cantos da organização, seja automatizando inventário, cadeia de suprimentos ou entrega de serviços. Isso capacita as organizações a monitorar, controlar e otimizar operações, além de melhorar a eficiência ao longo dos fluxos de trabalho.

No entanto, embora traga benefícios significativos, ao adotar ecossistemas XIoT, as organizações podem enfrentar riscos de vulnerabilidades decorrentes de medidas de segurança inadequadas nos dispositivos, o que pode abrir portas para que os atacantes ganhem acesso não autorizado. A natureza interconectada desses dispositivos também expande a superfície de ataque de uma organização, permitindo que atores maliciosos explorem um dispositivo comprometido como um ponto de apoio para infiltrar toda a rede. Dados da Zscaler apontam que em 2023 houve um crescimento de 400% no número de malwares focados em IoT.

Controle de acessos e roubo de propriedade intelectual

Embora haja uma crescente preocupação em proteger os centros industriais de ataques externos, há poucas ações eficazes para protegê-los contra ataques que podem ter sua origem interna.

A maioria dos fabricantes depende do acesso remoto para permitir que pessoal interno e de terceiros mantenha o CPS (cyber-physical systems) em seus ambientes de OT.

Um dos principais vetores de ataques direcionados a sistemas de tecnologia operacional é através de indivíduos que têm acesso às redes dessas tecnologias. Tradicionalmente, engenheiros de OT têm acesso administrativo compartilhado, e muitos deles acessam os ambientes remotamente. Essa dependência do acesso remoto à OT faz com que os cibercriminosos tentem explorar isso como um vetor de ataque.

Sem uma gestão adequada, pessoas mal-intencionadas podem facilmente acessar informações confidenciais e propriedades intelectuais, abrindo espaço para o roubo de dados sensíveis, como projetos em andamento e métodos exclusivos de produção. Isso pode acarretar na sabotagem das operações industriais, resultando em danos físicos, interrupções na produção e grandes impactos financeiros.

Alta dependência de serviços em nuvem

As redes de Tecnologia Operacional (TO) estão migrando para a computação em nuvem visando aprimorar sua eficiência e otimizar a utilização de recursos. No passado, os sistemas OT permaneciam localizados nas instalações, protegidos atrás das redes corporativas. Agora, dispositivos OT inseguros podem introduzir fraquezas na infraestrutura de nuvem da organização.

Mover hardware e software legados, que muitas vezes têm décadas de utilização, para a nuvem significa potencialmente introduzir uma série de vulnerabilidades em uma infraestrutura crítica, oferecendo aos criminosos a oportunidade de aproveitar técnicas históricas para obter acesso e realizar ataques.

Além de ampliar a superfície de ataque com os sistemas legados, os próprios recursos de nuvem, se estiverem mal configurados, podem deixar os ambientes críticos de OT em risco. Atacantes maliciosos que visam uma configuração incorreta ao se moverem lateralmente dentro da infraestrutura podem causar grandes danos e perdas financeiras às empresas.

Falta de investimento na área de segurança

As empresas devem alinhar o investimento em segurança cibernética com a estratégia de negócios e considerar a cibersegurança como um dos seus objetivos principais. Os CISOs enfrentam a tarefa de aumentar o ROI dos investimentos em segurança da informação e defender os investimentos para a alta administração ou conselho de administração.

No entanto, muitas empresas não alocam recursos suficientes para proteger seus sistemas industriais contra ameaças cibernéticas, o que as deixam vulneráveis à ataques. Segundo dados recentes da Kaspersky, 15% das empresas globalmente tiveram incidentes cibernéticos devido a investimentos insuficientes em segurança cibernética nos últimos dois anos.

Para indústrias de infraestruturas críticas o cenário ainda é pior: 25% das empresas de petróleo, gás e energia sofreram o maior número de incidentes cibernéticos devido à alocação inadequada de orçamento.

Proteja seu ambiente operacional com um ecossistema integrado de cibersegurança

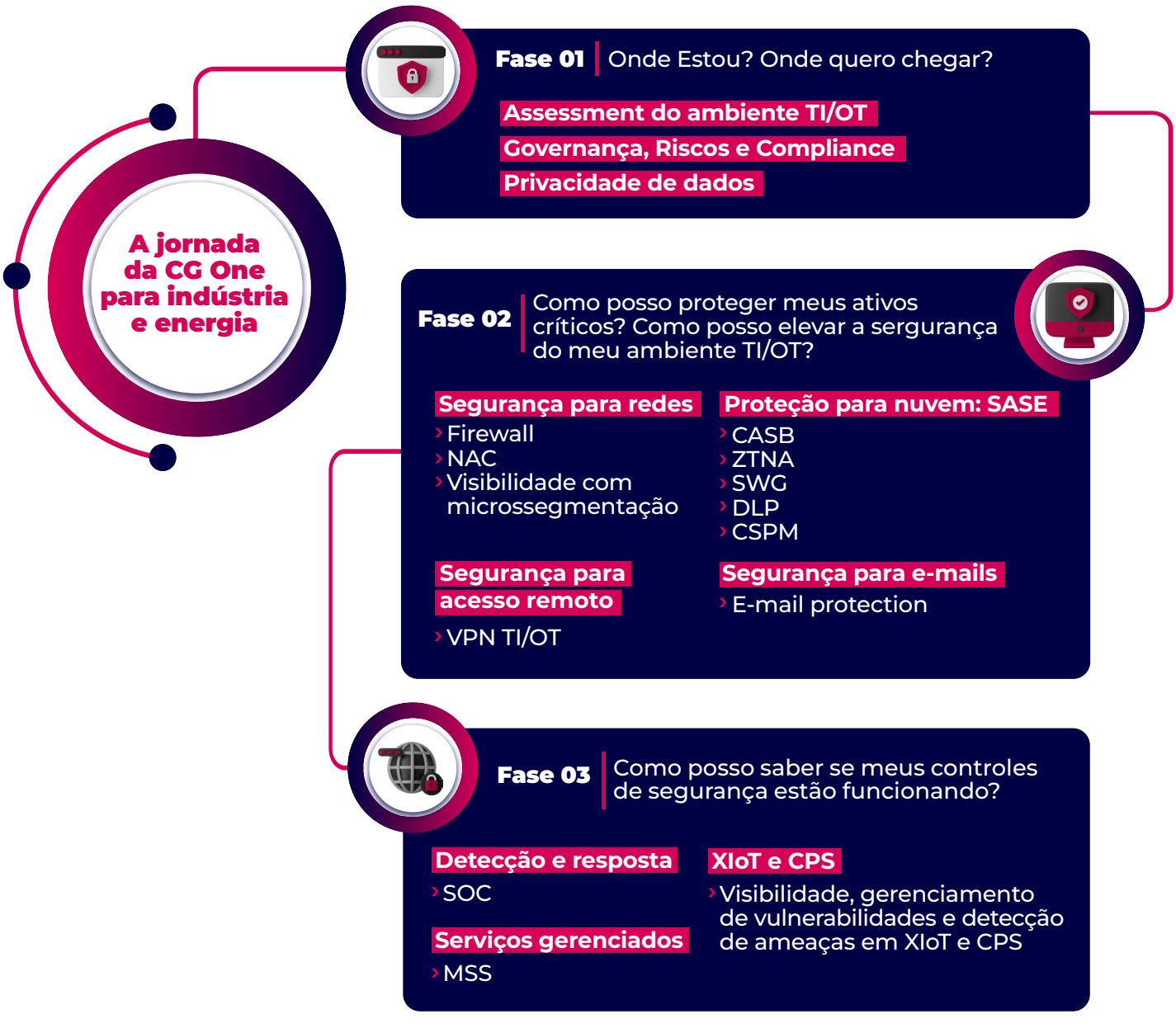
À medida que as organizações embarcam nas estratégias de negócios digitais, suas redes evoluem para abranger ambientes de IoT, multicloud e virtuais, acompanhados por fluxos de trabalho complexos. Muitas empresas utilizam produtos, ferramentas e aplicativos de diversos fornecedores, resultando em metodologias isoladas de gerenciamento de segurança.

A ausência de integrações tecnológicas nesses ambientes complexos dificulta cada vez mais a visibilidade das atividades na superfície de ataque expandida e a identificação de ameaças cibernéticas. Sistemas de segurança isolados não conseguem compartilhar a inteligência necessária para responder de forma rápida e automática a ameaças sofisticadas e ágeis.

Adotar um ecossistema integrado de soluções de segurança, interligadas para escalabilidade e adaptação conforme as demandas de negócios evoluem, te permite enfrentar integralmente os desafios ao longo da expansiva superfície de ataque.

A jornada da CG One para indústria e energia

Há mais de quatro décadas no mercado de tecnologia, proporcionamos proteção a ambientes industriais em setores cruciais como alimentício, automobilístico, manufatura, agrícola, energia, entre outros. A seguir, elencamos soluções de ponta do nosso portfólio para a sua jornada de maturidade em cibersegurança industrial.



FASE 01

Essa é a fase para estruturar e entender políticas, procedimentos e processos para monitorar os requisitos regulatórios, legais e de risco de segurança cibernética da organização. O objetivo é estabelecer bases para um programa sólido de cibersegurança.

Assessment do ambiente TI/OT

O assessment do ambiente de Tecnologia da Informação (TI) e Tecnologia Operacional (OT) é uma etapa crucial para entendermos a fundo a sua infraestrutura e necessidades específicas. Essa análise minuciosa nos permite oferecer soluções sob medida para otimizar seus sistemas e processos. Utilizamos o framework do NIST (National Institute of Standards and Technology) para avaliar sua segurança, conformidade com regulamentações e identificar áreas de aprimoramento. Com base nessa compreensão profunda, podemos apresentar propostas personalizadas do nosso portfólio, garantindo que as soluções recomendadas atendam perfeitamente às suas demandas e prioridades.

GRC (Governança, Riscos e Compliance)

Com a solução de GRC fornecida por nós, você amplia a capacidade das suas funções de gestão de riscos e segurança, através de uma plataforma unificada. Essa plataforma permite priorizar e gerenciar os riscos, capacitando-o a operar com confiança, mesmo diante de ameaças cibernéticas em curso. Isso não apenas fortalece a sua organização, mas também promove a resiliência em toda a cadeia de suprimentos.

01

Identifique e mitigue riscos

Obtenha inteligência regulatória e gerencie riscos de primeira ou terceira parte com base na metodologia escolhida.

02

Otimize o cumprimento e a gestão de auditoria

Centralize o desenvolvimento de políticas com inteligência empresarial integrada e recursos de colaboração aprimorados.

03

Alcance e mantenha a conformidade com certificações de segurança

Automatize a coleta de evidências e gerencie tarefas de GRC em toda a empresa com facilidade.

Privacidade de dados

Com a Privacidade de Dados, você pode adaptar-se facilmente às obrigações de conformidade previstas na LGPD, desde a obtenção e gerenciamento do consentimento até o atendimento automatizado às solicitações de exercício de direitos dos titulares e à conclusão de avaliações de impacto à proteção de dados.

01

Automatize fluxos de trabalho críticos

A plataforma de gestão de privacidade oferece a automação necessária para realizar as tarefas de gestão de privacidade.

02

Simplifique a conformidade

Com atualizações em tempo real e informações específicas por região incorporadas na plataforma, você simplifica o processo.

FASE 02

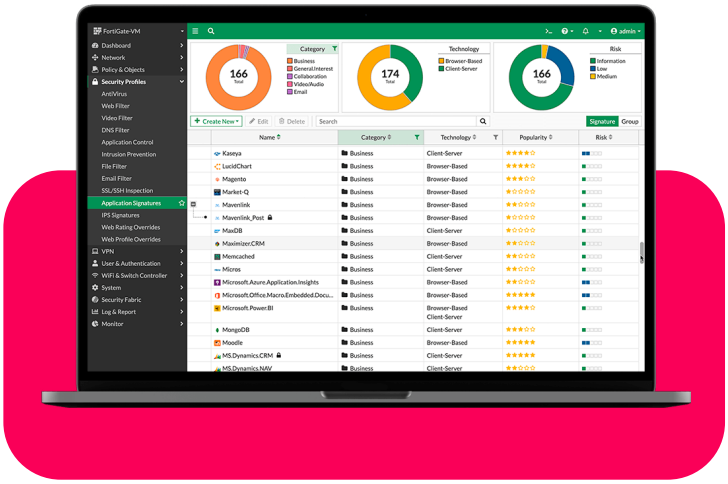
O objetivo da fase 2 é desenvolver e implementar medidas apropriadas para garantir a entrega de serviços críticos.

Segurança para redes

Next-Generation Firewall (NGFW)

O NGFW fornecido por nós possui um gerenciamento unificado projetado para redes híbridas, oferecendo uma convergência perfeita que pode ser dimensionada para atender a qualquer local: seja um escritório remoto, filial, campus, centro de dados ou ambiente de nuvem. Sua arquitetura ASIC (Application Specific Integrated Circuit) personalizada permite uma proteção líder do setor contra ameaças, incluindo recursos avançados de descriptografia em grande escala.

Além disso, o NGFW proporciona uma rede segura e completa, integrando funcionalidades como SD-WAN, switching, wireless e 5G. Essa abordagem abrangente simplifica a gestão de TI/TO, consolidando as soluções de segurança e rede em um console de gerenciamento centralizado e fácil de usar.



Premier Network Access Control (NAC)

O NAC do nosso portfólio representa uma abordagem abrangente de acesso de confiança zero, atuando como um guardião para todos os ativos digitais conectados à rede empresarial. Desde dispositivos de TI, IoT, OT/ICS até IoMT, ele supervisiona e protege cada componente.

Além de defender contra ameaças de IoT, estende o controle para dispositivos de rede de terceiros e orquestra respostas automáticas a uma variedade de eventos de rede. O NAC destaca-se como uma solução abrangente e eficaz para a segurança e gestão de todos os ativos digitais na rede empresarial.

Visibilidade com microssegmentação

Nossa solução de visibilidade com microssegmentação oferece a maneira mais simples, rápida e intuitiva de aplicar os princípios Zero Trust. Ela foi projetada para impedir a movimentação lateral através da visualização da atividade em seus ambientes de TI/OT, implementação de políticas precisas de microssegmentação e detecção rápida de possíveis violações.

A solução adquire informações detalhadas sobre a infraestrutura através de uma variedade de métodos, incluindo sensores baseados em agentes, coletores de dados de rede, registros de fluxo de nuvem privada e integrações que não requerem agentes. Essas informações são enriquecidas com contexto relevante através de um processo flexível e altamente automatizado de rotulagem, que inclui integração com fontes de dados existentes, como sistemas de orquestração e bancos de dados de gerenciamento de configuração.

Segurança para a nuvem

SASE (Secure Access Service Edge)

Com SASE do nosso portfólio, você unifica os serviços de rede e segurança em uma arquitetura na nuvem não só para proteger usuários, aplicações e dados e fornecer acesso rápido e seguro, mas também para monitorar continuamente suas atividades.

Além disso, com a solução SASE totalmente convergente, você pode usar uma SSE (Security Service Edge) completa, incluindo FWaaS (Firewall), NG SWG (Gateway Web Seguro), CASB (Cloud Access Security Broker), DLP (Data Loss Prevention) e ZTNA (Zero Trust Network Access), junto com o poder da Borderless WAN, para aplicar controles de segurança baseados em políticas para fornecer acesso seguro independentemente de onde os usuários, dados, aplicativos ou dispositivos estejam localizados.

A tecnologia oferece uma rede rápida e confiável para a força de trabalho híbrida com serviços de segurança zero trust completos e incorporados.

Segurança para e-mails

Proteção contra ataques via e-mail e aplicativos de colaboração

Proteger-se contra ameaças cibernéticas por e-mail e aplicativos de colaboração é essencial no cenário atual para assegurar a confidencialidade, integridade e disponibilidade dos dados da empresa. Com a solução de proteção de e-mails do nosso portfólio, as organizações podem implementar uma segurança de e-mail abrangente que aborda todas as áreas da comunicação empresarial.

Prevenção contra phishing

A tecnologia de prevenção de phishing que fornecemos utiliza inteligência artificial e aprendizado de máquina para identificar padrões e comportamentos suspeitos, bloqueando eficazmente tentativas de golpes desse tipo. Além disso, a solução é continuamente atualizada e aprimorada para combater as táticas cada vez mais sofisticadas dos cibercriminosos.

Proteção completa contra malware

O nosso serviço de proteção contra malware (HEC) oferece uma linha de defesa robusta contra uma ampla gama de ameaças, incluindo vírus, ransomware, trojans e outras formas de malware. Utilizando uma combinação de tecnologias de detecção de assinaturas, análise heurística e inteligência em tempo real, o HEC é capaz de identificar e neutralizar ameaças antes que elas possam causar danos à sua rede e sistemas.

Segurança para acesso remoto

VPN para IT/OT

Oferecemos uma ampla gama de VPNs escaláveis e de alta velocidade, com criptografia robusta, projetadas para proteger sua empresa contra ataques em ambientes de TI e OT, garantindo a segurança de todos os dados transmitidos pela rede.

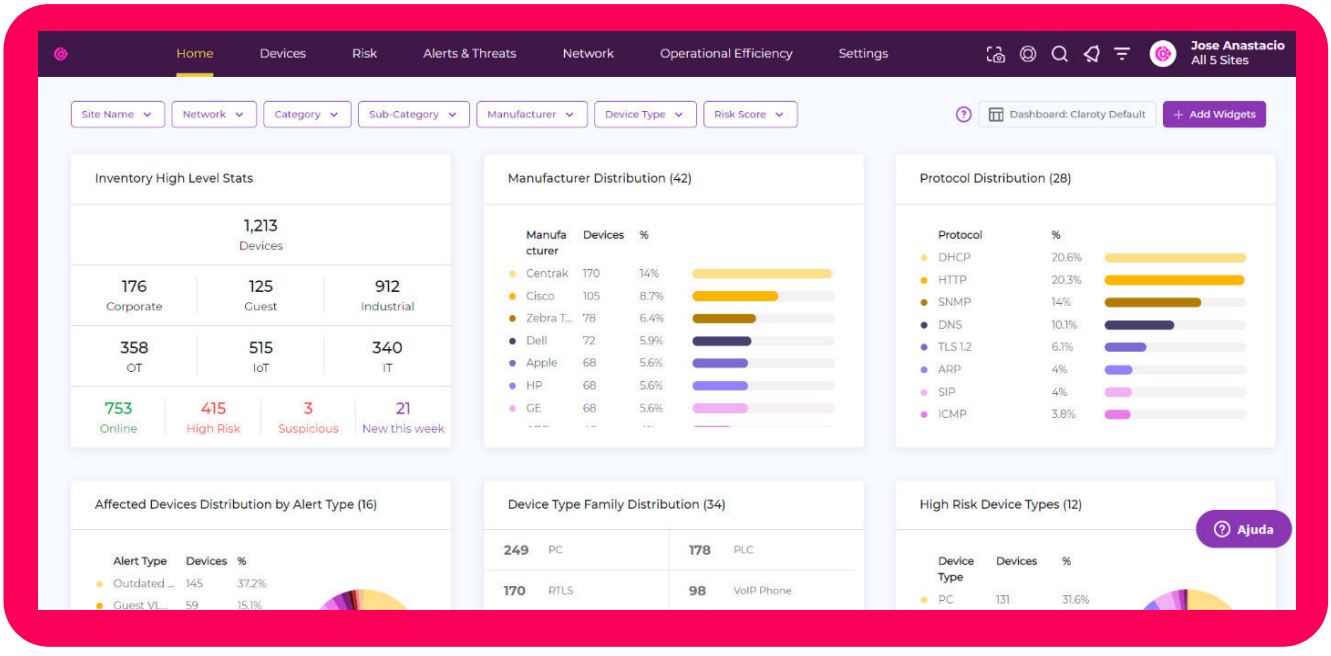
A solução que fornecemos proporciona túneis seguros que mantêm os invasores afastados dos seus dados e atividades online. Utilizando SSL e IPsec em conjunto com hardware ASIC (Circuito Integrado Específico de Aplicação), garantimos uma experiência rápida e confiável para todos os usuários.

FASE 03

O objetivo da fase 3 é desenvolver e implementar atividades apropriadas para identificar a ocorrência de um evento de cibersegurança e obter visibilidade da proteção dos ambientes.

Visibilidade, risco, gerenciamento de vulnerabilidades e detecção de ameaças em XIoT e CPS

Esse tipo de solução, voltada não somente para XIoT (Cross-Industry Internet of Things), mas também para todos sistemas e dispositivos CPS (Cyber-Physical Systems), oferece uma série de funções essenciais para garantir a segurança e a integridade dos ambientes interconectados. Essas funções combinadas fornecem uma abordagem abrangente para garantir a segurança e a proteção desses sistemas contra ameaças cibernéticas em constante evolução.



01 **Visibilidade abrangente**
Obtenha visibilidade completa sobre todos os dispositivos conectados, aplicativos e comunicações dentro de ambientes XIoT e CPS.

02 **Detecção de ameaças avançadas**
Identifique e receba alerta sobre atividades suspeitas ou potencialmente maliciosas em tempo real utilizando técnicas avançadas de detecção, como análise de comportamento e assinaturas de ameaças.

03 **Análise de tráfego e comportamento**
Monitore continuamente o tráfego de rede e o comportamento dos dispositivos, identificando anomalias que possam indicar atividades maliciosas ou falhas de segurança.

04 **Gestão de vulnerabilidades**
Identifique vulnerabilidades nos dispositivos e sistemas conectados, permitindo a implementação de patches e atualizações de segurança para mitigar riscos.

05 **Proteção de ativos críticos**
Proteja ativos críticos, como sistemas de controle industrial (ICS),dispositivos médicos e infraestrutura essencial contra ameaças cibernéticas.

06 **Isolamento e contenção de ameaças**
Em caso de detecção de ameaças, isole rapidamente os dispositivos comprometidos, minimizando o impacto de ataques e prevenindo a propagação para outros sistemas.

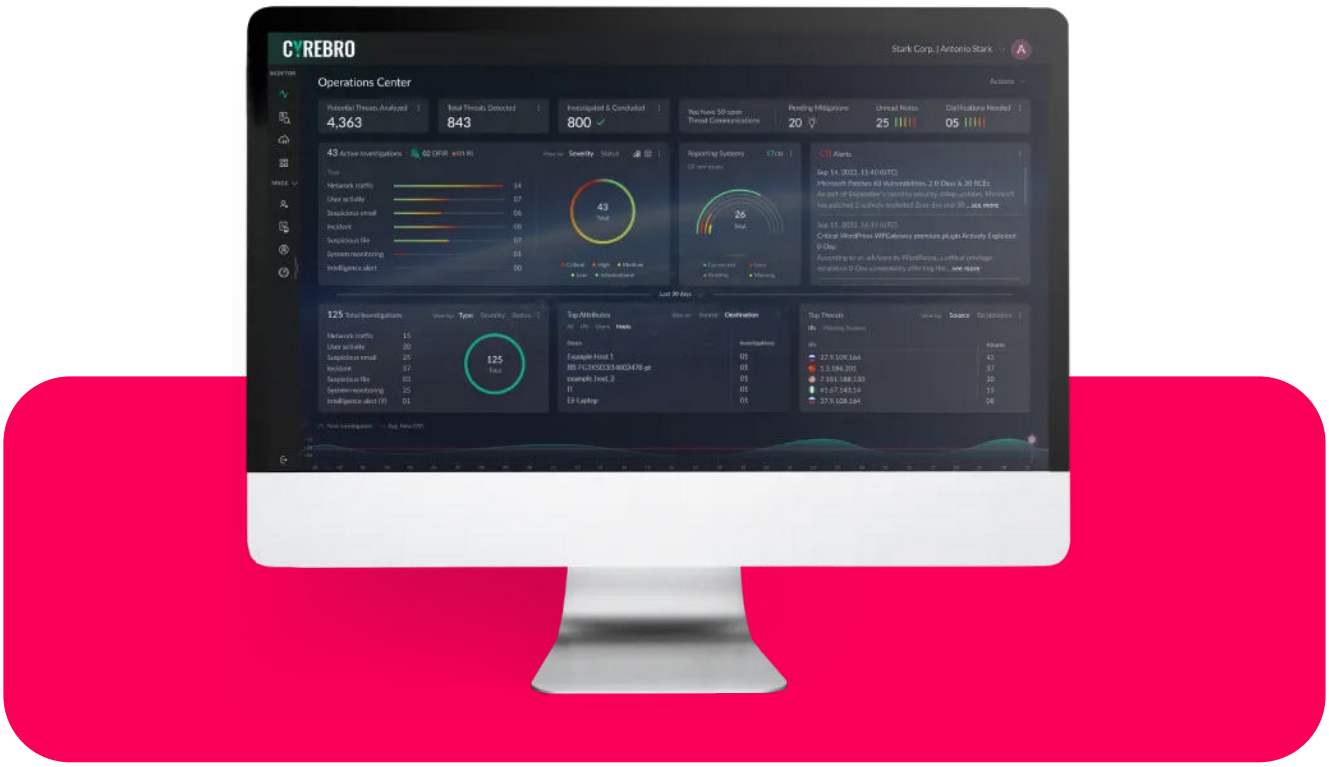
07 **Conformidade e auditoria**
Mantenha a empresa em conformidade com regulamentos de segurança cibernética e auditorias, obtendo relatórios detalhados sobre o estado da segurança e atividades de rede.

08 **Integração com infraestrutura existente**
Integra-se com a infraestrutura de segurança existente, permitindo uma implantação fácil e eficiente em ambientes XIoT e CPS.

Security Operations Center (SOC)

Nosso SOC, que conta com tecnologia Cyrebro, é o núcleo de segurança cibernética mais avançado e tecnológico do mercado. Ele oferece uma infraestrutura SOC gerenciada inédita e adaptável para o setor industrial, combinando IA para garantir uma nova geração de detecção e resposta a incidentes.

Além disso, possui monitoramento 24/7 com mais de 120 analistas, permite mitigar ameaças cibernéticas e fornece inteligência e caça proativa contra riscos ou possíveis ataques. Tudo isso através de uma plataforma interativa que proporciona visão em tempo real dos seus eventos mais críticos em todas as operações, camadas, redes e sistemas.



01

Respostas a incidentes

A resposta e a mitigação de ameaças categorizadas em nível 1 a 4, em tempo real.

02

Threat intelligence

A equipe de inteligência monitora ameaças em fóruns parceiros, OSINT, Deep e Dark Web, para agir rapidamente na criação de indicadores de comprometimento (IoCs), caso seja encontrado algo.

03

Threat hunting

Com aprendizado e inteligência de mais de 600 clientes ao redor do mundo, nossa equipe proativa realiza pesquisas para identificar o risco dos clientes com base nos IoCs. Ao detectar uma ameaça específica, o cliente é notificado para agir rapidamente.

04

Otimização

Combinação de Machine Learning com SIEM e SOAR, incorporando mais de 2.000 casos de uso customizados para correlacionar seus eventos de segurança. Desenvolvimento e aprendizado contínuos de otimização de regras, atualizações de IOC e novas tecnologias de detecção.

05

Investigação forense

Investigação contínua de suspeita de atividade maliciosa e ameaças cibernéticas, incluindo análise post-mortem.

Conte com o MSS (Managed Security Services) para a gestão da sua operação

Gestão e otimização: asseguramos a gestão eficiente da operação.

Alta disponibilidade: garantimos alta disponibilidade e desempenho contínuo do ambiente, que é crucial para a segurança e estabilidade operacional.

Adaptação às demandas: proporcionamos uma base sólida que permite às organizações adaptarem-se e escalarem de acordo com as demandas atuais e futuras.

Todas as soluções de cibersegurança em só lugar

Enquanto você se concentra em impulsionar o seu negócio, nossa equipe de especialistas está pronta para cuidar de todas as suas complexidades tecnológicas. Conte conosco para ser seu parceiro estratégico de segurança digital e riscos.

Network Security
Configuração, otimização e fortalecimento das infraestruturas de rede.

Security Information
Proteção de ativos críticos e prevenção de ataques cibernéticos.

Integrated Risk Management
Gerenciamento de riscos para melhorar a visibilidade e o processo de tomada de decisão.

Parceiros:

Akamai, algosec, Checkmarx, CHECK POINT, CLAROTY, CYBERARK, CYREBRO, FORTINET, GetGlobal, KEYSIGHT, netskope, OneTrust, proofpoint.

CG//One

Quem somos

Somos a CG One, a evolução da marca Compugraf. Com mais de 40 anos de expertise no mercado de tecnologia, somos especializados em segurança cibernética para todo o ecossistema digital das empresas.

Desenvolvemos e gerenciamos soluções de Segurança da Informação, Proteção de Redes e Gerenciamento Integrado de Riscos, e nosso portfólio é orientado de acordo com as práticas e os padrões de segurança do NIST® Cybersecurity Framework.

Contamos com um time qualificado e certificado que já proporcionou operações seguras para mais de 500 empresas de diversos portes e setores, em todo o Brasil.

Fale conosco