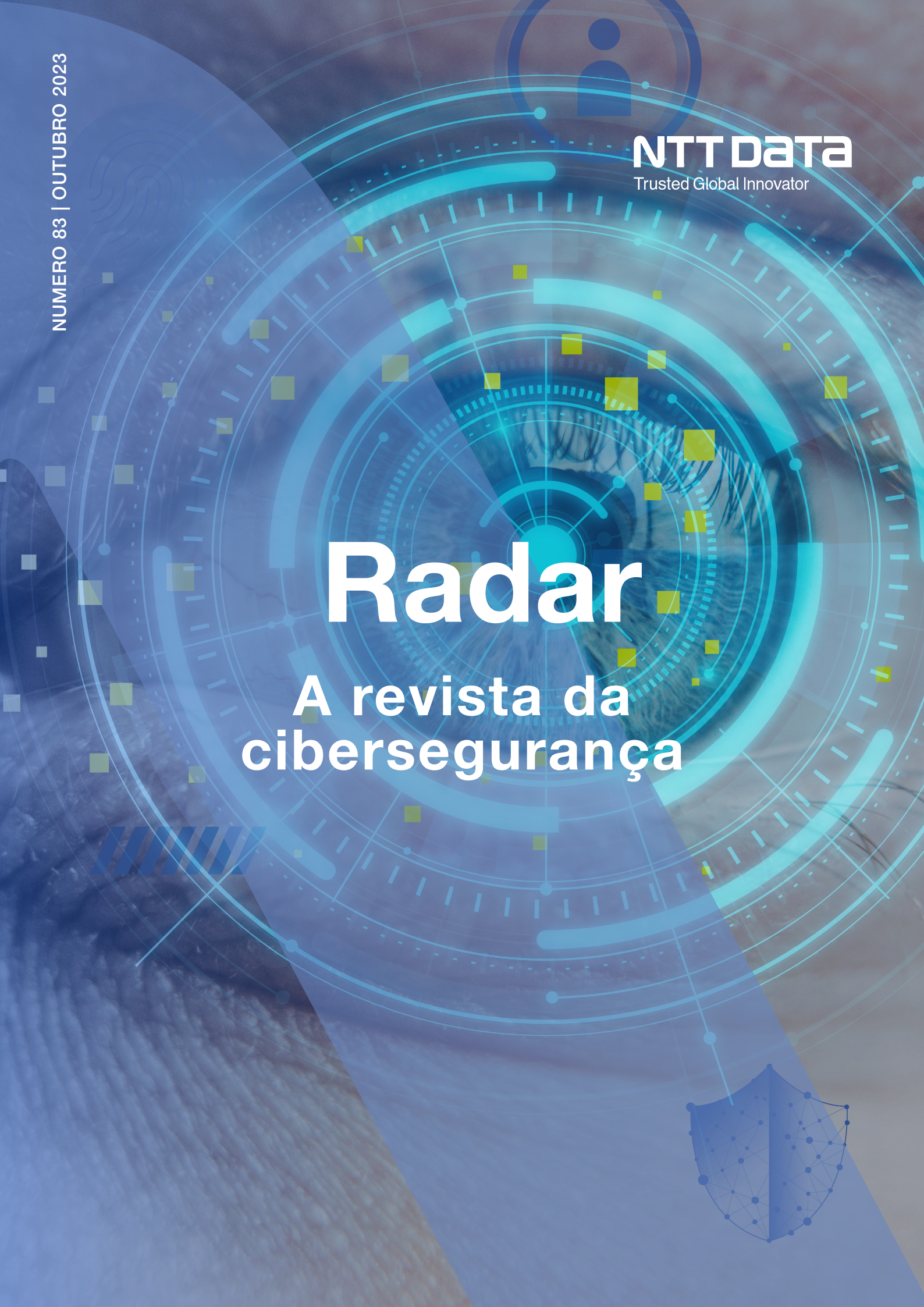
NUMERO 83 | OUTUBRO 2023

NTT DATA
Trusted Global Innovator

Radar

A revista da cibersegurança



COMO GERENCIAR OS RISCOS NOS NOVOS MODELOS DE INTELIGÊNCIA ARTIFICIAL?

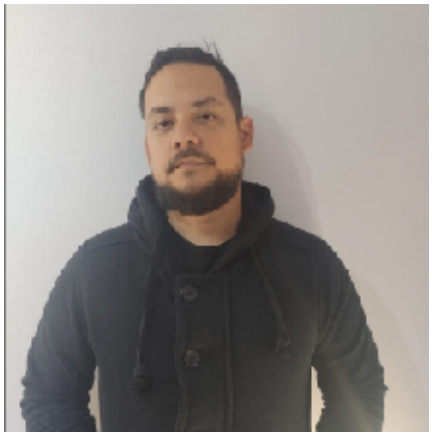
No ambiente interconectado de nossa era, a cibersegurança transcende seu papel técnico para se tornar o bastião que protege nossa infraestrutura digital. É a garantia de confiança em nossas operações diárias. A inteligência artificial (IA) é utilizada em muitas aplicações empresariais e de produção, incluindo automação, processamento de linguagem e análise de dados produtivos. Isso permite que empresas de todos os setores otimizem seus processos de fabricação, operações e melhorem a eficiência interna. Com o uso de diferentes regras de programação computacional, a IA permite que uma máquina se comporte como um ser humano e solucione problemas.

É importante mencionar que nenhum módulo de IA vem pronto desde o início para operar e funcionar como um verdadeiro suporte ao trabalho e à tomada de decisões da empresa. É necessário decidir sobre uma estratégia e um conjunto de dados para seu treinamento e posterior implementação. Atualmente, as grandes empresas que estão promovendo a IA têm os recursos para configurar a infraestrutura necessária para o treinamento (GPUs/TPUs, enormes bases de dados etc.). Os modelos podem ser retreinados com dados específicos de empresas menores (uma técnica chamada Transfer Learning). Nessa etapa de pré-processamento, o papel dos especialistas ligados ao sistema que está sendo treinado é fundamental, caso contrário, o modelo fará previsões que não estão alinhadas à realidade.

A incorporação da IA não está isenta de possíveis novas violações de segurança e proteção de dados que as empresas devem considerar e às quais devem dedicar recursos e tempo. As boas práticas recomendam a anonimização dos dados usados para treinamento, mas, às vezes, é possível reidentificar a fonte dos dados. Os modelos de machine learning e deep learning procuram padrões nos dados, portanto, é importante que os dados fornecidos sejam verificados/preparados por um especialista (por exemplo, um especialista em governança de dados), pois o modelo será tão bom quanto os dados utilizados em seu treinamento.

Neste ponto, surge um aspecto novo e de vital importância a ser considerado. Neste ponto, surge um aspecto novo e de vital importância a ser considerado. Um sistema de IA, embora possa se tornar um grande aliado na tomada de decisões para uma empresa, também apresenta um novo conjunto de vulnerabilidades, que podem ser exploradas maliciosamente para extrair informações confidenciais ou obter o controle do sistema.

Portanto, cumprir com uma estrutura mínima de medidas e controles de segurança pelo sistema de AI torna-se um requisito básico ao implementar o sistema e avançar para um ambiente de produção. A escolha certa dos controles de segurança e do desenvolvimento mínimo ajudará a fortalecer a segurança e a privacidade das informações e a aumentar a confiança no uso dos sistemas de IA. Essa estrutura ajudará a reconhecer, avaliar e mitigar os riscos de cibersegurança que um sistema de IA pode criar em uma organização, minimizando o número de violações de segurança em potencial que o sistema possa apresentar no momento.



Matias Saavedra Lopez
Project Leader de Cibersegurança na NTTDATA Chile

CIBERCRÔNICA

Nesta edição da RADAR, falaremos sobre ataques à cadeia de suprimentos no processo de desenvolvimento de software, uma técnica conhecida como ***Supply Chain Compromise***, de acordo com a MITRE. O uso de modernos frameworks de desenvolvimento da Web possibilitou a prevenção de técnicas comuns de ataque à Web, basta olhar para o OWASP TOP 10 2021 para perceber que as injeções de exploração passaram para o terceiro lugar.

No entanto, os cibercriminosos também modernizam seus ataques, e é por isso que, nos últimos anos, os ataques à cadeia de suprimentos têm crescido - vale lembrar o desastre causado pelo pelo Log4j em 2021.

Um ataque à cadeia de suprimentos implica em uma violação de um componente ou biblioteca de software e é amplamente utilizado para afetar as aplicações finais.

> “uma falha na biblioteca que interage com os mecanismos de banco de dados, possibilitando a execução de instruções SQL de consulta, modificação ou exclusão com parâmetros infectados.”

Desde então, os ataques à cadeia de suprimentos se tornaram uma modalidade eficaz para os cibercriminosos, que implementam diferentes táticas e técnicas para afetar os componentes de software ou seus desenvolvedores.

Por exemplo, podemos observar o recente ataque em junho à solução MOVEit (CVE-2023-34362), o software líder de mercado para transferência segura de arquivos. O interessante é que os invasores se aproveitaram de uma injeção SQL na produção e usaram essa violação para obter acesso a bancos de dados de empresas como BBC, British Airways, Aer Lingus, Boots, entre outras.

Os cibercriminosos aparentemente encontraram uma falha na biblioteca que interage com os mecanismos de banco de dados, possibilitando a execução de instruções SQL de consulta, modificação ou exclusão com parâmetros infectados.

Por outro lado, o usuário de conexão entre o MOVEit e o banco de dados é executado com privilégios de administrador, possibilitando que os invasores obtenham acesso remoto ao servidor das aplicações. Aparentemente, o grupo CL0P está envolvido no ataque, uma vez que eles utilizaram um backdoor conhecido como LEMURLOOT para vazar os dados. As empresas afetadas pelo ataque foram notificadas e a equipe do MOVEit acionou seu plano de resposta a incidentes, gerando os respectivos alertas de comprometimento e patches associados para mitigar a violação.

Outro ataque à cadeia de suprimentos que está afetando a comunidade Python é a recente campanha lançada em agosto, ao que parece norte-coreana, contra bibliotecas de código aberto. Os cibercriminosos estão supostamente incluindo códigos maliciosos em dependências conhecidas que são processadas pelo famoso gerenciador de pacotes PyPI (pip). A técnica utilizada consiste em criar bibliotecas com nomes e descrições muito semelhantes às originais, mas com pequenas variações, de modo que os desenvolvedores sem conhecimento importem essas bibliotecas maliciosas, como Vmconnector, Tableediter e pyVmomi, que são algumas das bibliotecas afetadas.

Os cibercriminosos clonam o projeto original e, em seguida, incluem partes de código malicioso e, finalmente, fazem o upload delas para o gerenciador de pacotes Python. Isso altera ligeiramente o nome da biblioteca usando caracteres especiais. De acordo com a análise da ReversingLabs produzida a partir de sua plataforma Titanium, ferramenta utilizada para monitorar bibliotecas OpenSource e analisar seu código-fonte (SAST), os cibercriminosos incluíram código malicioso em uma biblioteca Vmconnect falsa, na qual foram identificados snippets de código capazes de criar processos do sistema operacional, enumerar informações do sistema e ocultar dados usando base64 e conexões com sites remotos.

Ao analisar os domínios encontrados nas URLs do código-fonte, o Reversing Labs descobriu que poderiam estar relacionados ao grupo Lazarus (amplamente conhecido por ser financiado pelo governo norte-coreano), que assumiu a responsabilidade pelos recentes ataques de ransomware. Aparentemente, o vetor está mudando, já que a confiança dos desenvolvedores nos gerenciadores de pacotes e a falta de conhecimento estava favorecendo o grupo de cibercriminosos. O ReversingLabs também detectou essas mesmas técnicas de ataque à cadeia de suprimentos em gerenciadores de pacotes para linguagens específicas, como NodeJS (npm), Ruby (gem) e C# (nuget).

Também podemos lembrar o ataque à 3CX em março deste ano, de acordo com a Mandiant, a aplicação para desktop da 3CX foi infectada com código malicioso depois que cibercriminosos norte-coreanos comprometeram o ambiente de desenvolvimento da empresa por meio de sofisticados ataques à rede interna. O objetivo dos criminosos era modificar o software original para incluir snippets de código do tipo RAT e obter acesso não autorizado aos computadores dos usuários finais da 3CX. O impacto do ataque ainda é estudado meses depois, pois as técnicas utilizadas eram tão sofisticadas e criativas que não eram conhecidas.

O ataque aparentemente teve início com um desenvolvedor da 3CX instalando um software de trading com código malicioso, e rapidamente os cibercriminosos infectaram a máquina e a usaram como um vetor de entrada para a rede interna. Sabe-se também que as credenciais e informações confidenciais foram comprometidas ao examinar os repositórios de código da conta do desenvolvedor. Com esses acessos, os cibercriminosos fizeram movimentos laterais até chegarem aos ambientes de CI/CD da aplicação da 3CX. De acordo com a Mandiant, técnicas de injeção de DLL e persistência em nível de serviço foram executadas para incluir bibliotecas maliciosas no código-fonte da aplicação original. A Mandiant atribui o ataque ao grupo cibercriminoso norte-coreano Nexus.

Para terminar, esses ataques à cadeia de suprimentos estão sendo abordados pelos fornecedores de ferramentas de segurança de aplicações. A equipe da Snyk, uma ferramenta de verificação de vulnerabilidades de componentes de terceiros, mantém uma lista atualizada de bibliotecas mal-intencionadas que são carregadas nos gerenciadores de pacotes tradicionais. Em agosto, a equipe da Snyk relatou mais de 500 bibliotecas maliciosas, quase 20% delas em linguagem C e C++, o que pode indicar que até mesmo os dispositivos de Internet das Coisas (IoT) são alvo de cibercriminosos.

Enquanto as organizações não implementarem medidas de segurança adequadas, os ataques à cadeia de suprimentos continuarão sendo um vetor de ataque eficaz para os cibercriminosos. Os processos de desenvolvimento e aquisição de software, componentes e bibliotecas de terceiros devem ser os pilares para a segurança. O investimento em programas robustos de segurança de aplicativos é essencial para garantir que o ciclo de vida do software seja protegido e que, em caso de ciberataques em componentes e bibliotecas de terceiros, seja possível adotar uma reação em tempo hábil. Em curto prazo, a implementação do Software Bill of Materials (SBOM) é indispensável para determinar a superfície de ataque das organizações contra ameaças à cadeia de suprimentos de softwares.

USO DA METODOLOGIA FAIR NA ANÁLISE QUANTITATIVA DE RISCO

Por: NTT DATA Europa & Latam

A metodologia de risco quantitativo FAIR vem sendo discutida há muitos meses. Na edição anterior da RADAR, apresentamos a metodologia e seus benefícios. No entanto, ainda existem muitas dúvidas sobre seu uso, o que é preciso fazer para adotá-la em uma organização e que tipo de informação é necessária para implementar essa metodologia. Neste artigo, vamos examinar mais de perto como abordar a análise de um cenário e que tipo de perguntas devemos nos fazer.

Vamos ver alguns exemplos de cenários:

- indisponibilidade de serviços bancários transacionais pela Web no setor bancário
- indisponibilidade de um canal de compras pela Web no setor de varejo
- indisponibilidade de um site de inscrições de seguros de uma seguradora

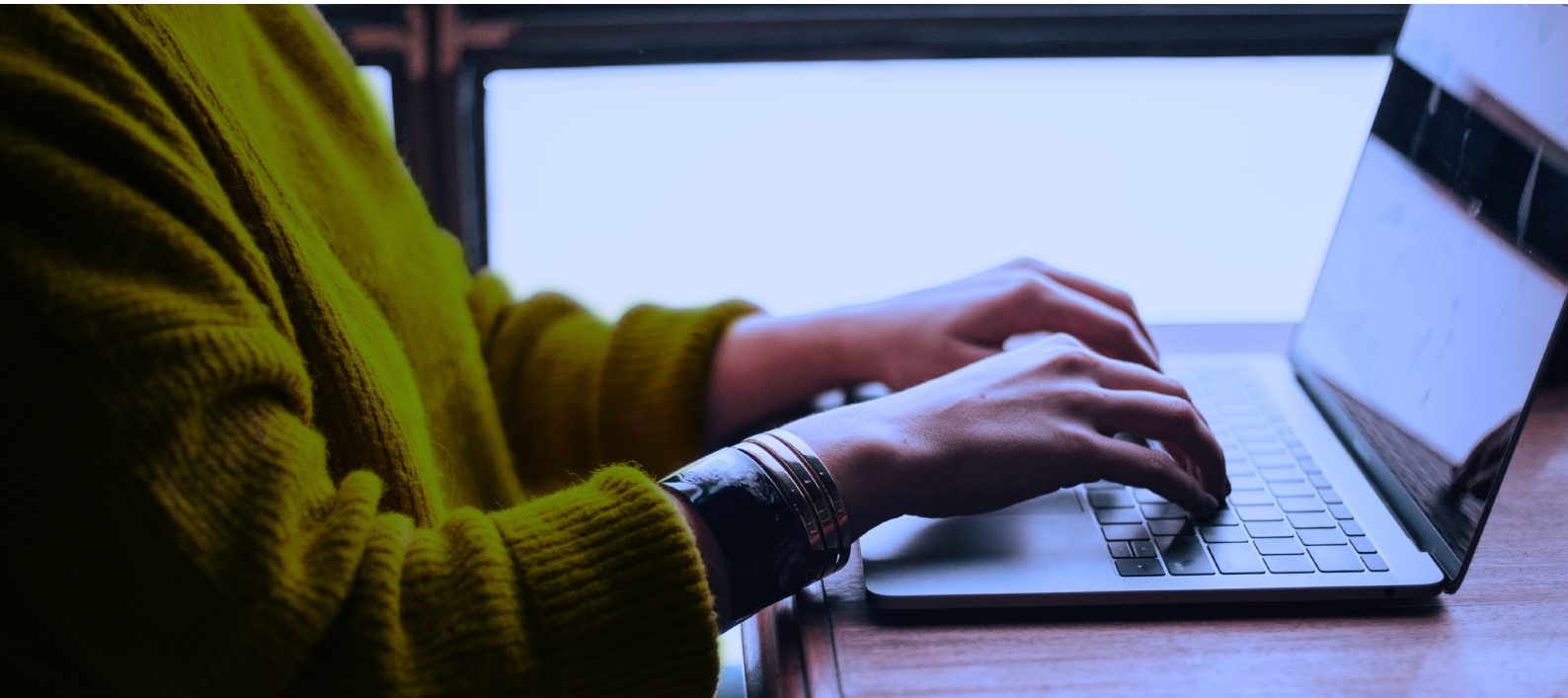
Nesses cenários, a FAIR ajuda a responder às seguintes questões:

- Quanto vou perder financeiramente no próximo ano, no cenário mais provável, devido à indisponibilidade do sistema?
- Quanto vou perder, no mínimo?
- E no máximo?

Dados reais apresentados à alta administração podem ajudar a alavancar os investimentos necessários para mitigar os riscos existentes. A primeira etapa consiste em contextualizar o cenário da organização, determinando o setor ao qual ela pertence, seus processos e seus ativos críticos. Isso servirá para definir o escopo do cenário à ser avaliado. O cenário deve considerar um ativo e um agente de ameaça, por exemplo, um website de serviços bancários que fica indisponível devido a um ramsonware. É importante enfatizar que cada cenário (ativo + agente de ameaça) que encontrarmos deve ser analisado separadamente pela FAIR, embora, à medida que os cenários forem analisados e as informações forem coletadas, serão aplicadas aos próximos cenários.

Uma vez definido o cenário, podemos iniciar a avaliação da magnitude da perda e da frequência dos eventos de perda. Começaremos com a magnitude da perda, que é dividida em duas categorias principais: **perda primária** (perda direta para a organização e/ou principais stakeholders) e **perda secundária** (perda para a organização e/ou principais stakeholders como resultado de uma reação negativa de terceiros).

Para avaliações da magnitude da perda primária, é necessário pensar em seis subcategorias: produtividade, resposta, reputação, substituição, vantagem competitiva e multas e decisões judiciais.



Para começar a avaliação, precisamos fazer as seguintes perguntas:

- **Perda de produtividade:** após o ataque e a interrupção da disponibilidade do website operacional, quantos colaboradores serão afetados no melhor cenário e quantos no pior cenário? Esses colaboradores ficarão sem trabalhar, qual é o salário deles e, portanto, qual é a perda financeira no melhor e no pior cenário? Como o modelo também solicita um valor "mais provável", podemos fazer a pergunta no cenário mais provável ou simplesmente calcular a média entre o valor mínimo e máximo.
- **Custos de recuperação:** a organização analisada deve ter um plano de recuperação. Quantas pessoas, no mínimo, executarão esse plano de recuperação? E no máximo? Quantas horas, no mínimo, espera-se que eles trabalhem? E no máximo? Qual será o custo dos seus serviços? Com essas informações, podemos calcular qual será o custo mínimo e máximo da recuperação e podemos usar a média para definir o cenário mais provável.
- **Perda devido a multas e decisões judiciais:** o ativo em análise terá um número de clientes que poderão ser afetados. Quantos serão os afetados, no mínimo? E no máximo? Em caso de denúncia, qual seria a multa que podemos pagar? Com essas informações, agora é possível calcular o valor que a organização pagaria em multas e decisões judiciais. O valor mais provável pode ser calculado com base no número de pessoas que provavelmente serão afetadas e no custo provável de uma multa, ou simplesmente calculando a média entre os valores mínimo e máximo.
- O **dano à reputação** causado no cenário também deve ser quantificado. Qual será a perda causada por danos à reputação, no mínimo? E no máximo? Qual seria o valor mais provável?
- É possível que ocorra uma **perda de vantagem competitiva** para outras organizações que prestam o mesmo serviço. Talvez as informações sobre essa perda possam ser obtidas de dados históricos sobre incidentes em que os clientes migraram para outras empresas. Qual foi a perda mínima registrada? E a máxima? E a mais provável?
- Por fim, as **perdas por substituição** devem ser consideradas, caso sejam aplicáveis. Ou seja, se os ativos envolvidos no cenário precisarem ser substituídos? Da mesma forma, serão considerados os valores de substituição mínimo, máximo e mais provável.

Lembre-se de que a magnitude da perda é dividida em duas partes (primária e secundária), portanto, agora temos de analisar as perdas causadas por terceiros. Para a perda secundária, analisamos as seguintes informações:

- **Perda secundária por resposta:** o impacto sobre os clientes fará com que parte da equipe de trabalho da organização se concentre na notificação desses clientes. Quantos clientes precisarão de atenção, no mínimo? E no máximo? E qual será o valor mais provável? Qual será o custo dessa notificação? Com isso, é possível calcular a perda de produtividade secundária mínima, máxima e mais provável.
- **Perda secundária por multas e decisões judiciais:** pode haver processos e reclamações de nossos clientes ou pelo fato de eles, por sua vez, serem processados por seus próprios clientes porque nosso incidente afetou um serviço que não conseguiram prestar em tempo hábil. Nesse caso, deve ser analisado qual seria o mínimo esperado para essas multas, sentenças ou sanções. Qual seria o valor mais provável e o que esperar no pior caso?
- **Perda secundária por produtividade:** para esse valor, precisamos pensar sobre a equipe adicional que será necessária contratar para lidar com as solicitações e reclamações recebidas. Por exemplo, a organização pode ser obrigada a reforçar o departamento jurídico ou a contratar consultores jurídicos externos. Nesse ponto, pensaremos em quantas pessoas adicionais precisaremos no mínimo, no máximo e, o mais provável, por quanto tempo e qual será a remuneração. Com esses valores, podemos calcular os valores mínimo, médio e máximo.
- **Perda secundária por danos à reputação:** Esse valor refere-se à perda de valor das ações e ao não cumprimento das projeções de aquisição de clientes. Devemos pensar em quanto perderemos com esses eventos, no mínimo, no máximo e no mais provável.

Depois que todas essas perguntas forem respondidas, a análise de perda financeira do cenário estará concluída. A última etapa é determinar a frequência dos eventos de perda e a vulnerabilidade do ativo no escopo do cenário.

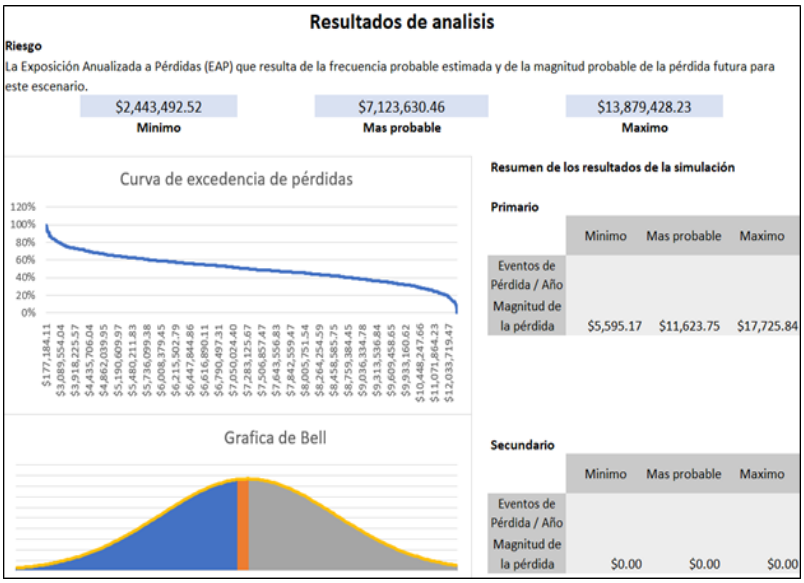
Para a frequência dos eventos de perda, pode ser realizada uma análise de incidentes anteriores e fazer uma previsão de quantos eventos ocorrerão no próximo ano, no mínimo, no máximo e em média. Por exemplo, em um cenário de indisponibilidade de um ativo, você pode analisar quantas vezes esse ativo ficou indisponível nos últimos cinco anos e considerar o mínimo, o máximo e a média como o mais provável.

E, por último, e talvez a questão mais complexa da análise: avaliar a resiliência do ativo. Esse ativo contará com diferentes medidas de segurança já implementadas na organização, o que reduzirá bastante a vulnerabilidade aos criminosos. Qual é a porcentagem, na melhor das hipóteses, em que os controles de segurança conseguem evitar o ataque? Qual é o pior cenário possível? E o mais provável?

Agora, com todas as informações coletadas, é possível inserir todas as informações na ferramenta de análise, o que nos permite ter uma estimativa da perda. O interessante da FAIR é que a ferramenta retornará 3 valores:

- Valor 1: valor mínimo de perda.
- Valor 2: valor de perda mais provável.
- Valor 3: valor máximo de perda.

Além disso, a ferramenta fornece uma visualização da quantidade de eventos possíveis por ano (com base nas informações de evento e vulnerabilidade fornecidas). Ou seja, poderemos dizer quantos eventos ocorrerão no mínimo, no máximo e no cenário mais provável.



Uma vez concluído esse ponto, inicia-se o processo estratégico. Quais são os projetos que podemos implementar para aumentar a resiliência? Quanto essa resiliência melhorará? E qual é o prejuízo previsto pelo modelo com essa nova medida de segurança? O importante será definir quais medidas, iniciativas, investimentos e implementações realizar para garantir que esses projetos tenham um impacto financeiro maior do que seu custo em perdas. A partir desse momento, as empresas poderão explorar todo o potencial da FAIR.

TENDÊNCIAS

Segurança e privacidade em Inteligência Artificial

De acordo com o Artificial Intelligence Index Report (2023), cerca de 31 países publicaram e/ou aprovaram alguma regulamentação relacionada à IA durante o período de 2016 a 2022. O objetivo dessa regulamentação é fornecer diretrizes de privacidade e segurança que devem ser consideradas em projetos que envolvam a concepção, o desenvolvimento e a implantação de um sistema de IA.

Então, o que precisa ser feito para garantir a segurança e a privacidade de um sistema de IA? Para que um sistema de IA seja seguro e garanta o direito à proteção de dados pessoais, é necessário verificar se está em conformidade com os controles legais, organizacionais e técnicos. Para isso, é essencial que, com base em uma estrutura focada nas regulamentações atuais, possa ser realizada uma avaliação para determinar o nível de maturidade do sistema de IA e, se necessário, adotar as medidas corretivas necessárias.

Mas quais são os domínios que devem ser analisados em uma estrutura de inteligência artificial?

a) Em primeiro lugar, é preciso garantir a correta **identificação e transparência do sistema de IA**. Devem ser analisados aspectos como: propósito, identificação de responsabilidades, transparência e identificação do contexto de uso e ter a garantia que essas informações estejam disponíveis.

b) Fundamentos do sistema de IA: assegurar que os fundamentos do sistema de IA estejam corretamente definidos. Devem ser analisados aspectos como: identificação da política de desenvolvimento, adequação dos modelos teóricos de base, assim como a estrutura metodológica e a identificação da arquitetura básica.

c) Gerenciamento de dados: Assegurar que os processos de coleta, armazenamento, processamento e proteção dos dados usados por um sistema de IA estejam corretamente definidos. Devem ser analisados aspectos como: atribuição da origem das fontes de dados, controle de vieses, preparação de dados e qualidade dos dados.

d) Gerenciamento de riscos: garantir que os riscos associados à implementação e à operação de um sistema de IA sejam identificados, avaliados, controlados e monitorados. Devem ser analisados aspectos como: mapeamento, avaliação e gerenciamento.

e) Compartilhamento de informações sobre incidentes e falhas de funcionamento: garanta uma comunicação eficaz entre as organizações e as partes interessadas em relação a incidentes de segurança, vulnerabilidades e falhas de funcionamento em um sistema de IA. Devem ser analisados aspectos como: a comunicação de incidentes graves, o acesso aos dados e ao código-fonte do sistema de IA.

(f) Verificação e validação: garantir que o sistema de IA opere de acordo com os requisitos estabelecidos e produza resultados precisos e confiáveis. Devem ser analisados aspectos como: consistência, desempenho, segurança e rastreabilidade.

Uma análise detalhada desses domínios e a adaptação dos sistemas de IA para atendê-los permitirão que as organizações aproveitem ao máximo essa tecnologia, sem colocar em risco seus negócios ou a confiança de seus clientes.

VULNERABILIDADES

Receba nosso boletim informativo completo e de vulnerabilidade inscrevendo-se aqui.

Oneview

CVE-2023-30908;-2650;-4304
Data: 07//09/2023

Descrição. Em 7 de setembro, foi publicada uma vulnerabilidade crítica (CVE-2023-30908) que afeta o produto HPE OneView, destinado à gestão de infraestrutura, desenvolvido pela Hewlett Packard Enterprise. Também foram publicadas duas vulnerabilidades (CVE-2023-2650 (alta) e CVE-2022-4304 (média)) sobre o mesmo produto.
Essas vulnerabilidades permitem que um hacker contorne a autenticação remotamente e acesse sem autorização o HPE OneView. Em função da forma como a ferramenta lida com as credenciais de usuário, uma solicitação explicitamente projetada para o HPE OneView pode ser manipulada.
Ao explorar essas vulnerabilidades, um hacker pode obter informações confidenciais, como chaves de criptografia e senhas, ou realizar um ataque de negação de serviço (DoS) contra o HPE OneView.

Link: https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbgn04530en_us
https://nvd.nist.gov/vuln/detail/CVE-2023-30908

Produtos afetados. Todas as versões anteriores à v8.5 ou v6.60.05 LTS.

Solução: A solução recomendada para corrigir essa vulnerabilidade é instalar os patches de segurança mais recentes para v8.5 ou v6.60.05 LTS.

Linux

CVE-2023-4206
Data: 06/09/2023

Descrição. Essa vulnerabilidade de transbordamento está associada à função route4_change no arquivo net/sched/cls_route.c. Por meio da manipulação de uma entrada desconhecida, ocorre uma vulnerabilidade da classe de estouro de buffer.
Os possíveis danos de um ataque bem-sucedido ainda não são conhecidos, embora possam levar à negação de serviço e ao escalonamento de privilégios. No momento, não há nenhum exploit conhecido para essa vulnerabilidade.

Link: https://www.debian.org/security/2023/dsa-5492
https://www.suse.com/security/cve/CVE-2023-4206.html
https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=b80b829e9e2c1b3f7aae34855e04d8f6ecaf13c8

Produtos afetados. Os recursos afetados por esta vulnerabilidade são:
- Red Hat Enterprise Linux 8 ou posterior
- SUSE Linux Enterprise Desktop/Server 15 ou anterior
- Debian 6.1.38-1 ou anterior e 4.19.249-2 (versão corrigida 6.1.52-1)

Solução: A solução recomendada para corrigir esta vulnerabilidade é instalar as versões mais recentes lançadas por cada fabricante.

PATCHES

Apple

Data: 07/09/2023

Descrição. A Apple lançou uma atualização de segurança para o iOS e o iPadOS que corrige duas explorações de dia zero (CVE-2023-41064 e CVE-2023-41061). A falha de segurança afeta a versão mais recente do Sistema Operacional iOS (16.6), descoberta por pesquisadores do Citizen Lab, que está relacionada à família do zero-click e consegue infectar o dispositivo com o malware Pegasus sem a necessidade de intervenção do usuário.
A exploração envolve anexos do PassKit com imagens maliciosas enviadas a partir da conta do iMessage de um hacker para a vítima utilizando o software Pegasus do NSO Group.
Essa vulnerabilidade está associada a um estouro de buffer no componente Image I/O, que permite que os aplicativos leiam e gravem a maioria dos formatos de arquivo de imagem.

Link:https://citizenlab.ca/2023/09/blastpass-nso-group-iphone-zero-click-zero-day-exploit-captured-in-the-wild/
https://support.apple.com/en-us/HT213905

Produtos afetados: A vulnerabilidade afeta todas as versões compatíveis (16.6 e anteriores).
Solução: As correções são aplicadas ao instalar o iOS 16.6.1 e o iPadOS 16.6.1.

Google Chrome

Data: 11/09/2023

Descrição. O Google lançou uma atualização de segurança para uma vulnerabilidade crítica de dia zero no Chrome (CVE-2023-4863). Essa vulnerabilidade é explorada por meio de um estouro de buffer no componente que manipula o WebP, um formato de arquivo gráfico rasterizado que substitui os formatos de arquivo JPEG, PNG e GIF.
A exploração dessa vulnerabilidade pode causar falhas de negação de serviço ou permitir a execução de códigos maliciosos nos sistemas.
A vulnerabilidade pode estar sendo explorada, pois o Google está ciente de que existe uma exploração para a vulnerabilidade, conforme relatado pela Apple Security Engineering and Architecture (SEAR) e pelo The Citizen Lab da Munk School da Universidade de Toronto.

Link: https://chromereleases.googleblog.com/2023/09/stable-channel-update-for-desktop_11.html
https://nvd.nist.gov/vuln/detail/CVE-2023-4863

Produtos afetados: A vulnerabilidade afeta todas as versões anteriores a 116.0.5845.187 para Mac e Linux e 116.0.5845.187/.188 para Windows.

Solução: O Google lançou uma atualização automática para as novas versões 116.0.5845.187 para Mac e Linux e 116.0.5845.187/.188 para Windows.

EVENTOS

FS-ISAC FinCyber Today Summit

De 1 a 4 de outubro de 2023

Esse encontro é um evento presencial de vários dias para profissionais de segurança de TI que trabalham em instituições financeiras. O evento apresenta uma visão geral de como os participantes podem aplicar novas tendências e práticas de segurança de TI na vida real para melhorar a proteção de suas organizações. O evento aborda diversos temas. Por exemplo, “Fraude, Identidade e Dinheiro”, “GRC e Resiliência” e “Intel e Ataques Globais”. Os participantes podem escolher o tema que melhor atenda às suas necessidades de negócios.

Link: 2023 FinCyber Today Summit (fsisac.com)

CSA Virtual Research Summit

17 de outubro de 2023

A CSA está organizando um evento especial para apresentar os projetos de pesquisa que definirão a segurança na nuvem no próximo ano. Com um olhar voltado para as importantes tendências da nuvem e da cibersegurança, o CSA Research Summit apresentará as últimas atualizações sobre projetos de pesquisa novos e existentes e fornecerá ferramentas e orientações essenciais para a comunidade que adota a nuvem. Com a consolidação definitiva da nuvem como o principal sistema de TI em todo o mundo, a segurança da nuvem é atualmente a base dos programas de cibersegurança.

Link: Summary - CSA Research Summit 2023

Treinamentos Blackhat

De 23 a 26 de outubro de 2023

A SecTor construiu uma reputação por reunir especialistas de todo o mundo para compartilhar suas pesquisas e técnicas mais recentes sobre ameaças clandestinas e defesas corporativas. A conferência oferece uma oportunidade única para que profissionais, gerentes e executivos de segurança de TI se relacionem com seus colegas e aprendam com seus mentores. Este ano, a SecTor está lançando o programa “Certified Pentester”, um exame prático de um dia.
Link: SecTor 2023 (blackhat.com)

SANS Cyber Solutions Fest 2023

De 25 a 27 de outubro de 2023

A conferência ajuda as organizações a planejar seus investimentos em segurança. Seu objetivo é conectar líderes de opinião e fornecedores do setor com tomadores de decisão e profissionais de segurança. O evento é gratuito e realizado totalmente on-line.
Link: Fall Cyber Solutions Fest 2023 | SANS Institute

RECURSOS

Relatório de pesquisa da plataforma de proteção de aplicativos Cloud Native

A Microsoft contratou a CSA para elaborar uma pesquisa e um relatório com o objetivo de entender melhor o conhecimento, as atitudes e as opiniões do setor em relação à segurança da CNAPP. A pesquisa foi realizada on-line em abril de 2023 e recebeu 1.201 respostas de profissionais de TI e segurança. O relatório tem como objetivo fornecer informações sobre as prioridades e os desafios de segurança na nuvem das organizações, revelar o estado atual da implementação do CNAPP e identificar os métodos e desafios atuais no gerenciamento da postura de segurança, na proteção da carga de trabalho na nuvem e em DevSecOps.

LInk: Cloud Native Application Protection Platform Report | CSA (cloudsecurityalliance.org)

CSA Assurance Education FAQ

O Cloud Certificate of Cloud Audit Knowledge (CCAK) e o STAR Lead Auditor Training são dois treinamentos de garantia que fazem parte do programa Security, Trust, Assurance and Risk (STAR) da CSA, o maior programa de segurança em nuvem do mundo.

Link: CSA Assurance Education FAQ | CSA (cloudsecurityalliance.org)

Configurações seguras em dispositivos industriais

As bases de hardware e software configuradas e instaladas no sistema são tão importantes quanto as bases de engenharia social ensinadas aos colaboradores, já que a corrente é quebrada pelo elo mais fraco, os seres humanos. Neste artigo, o INCIBE fornece, entre outras coisas, uma lista de boas práticas para o fortalecimento dos dispositivos OT.

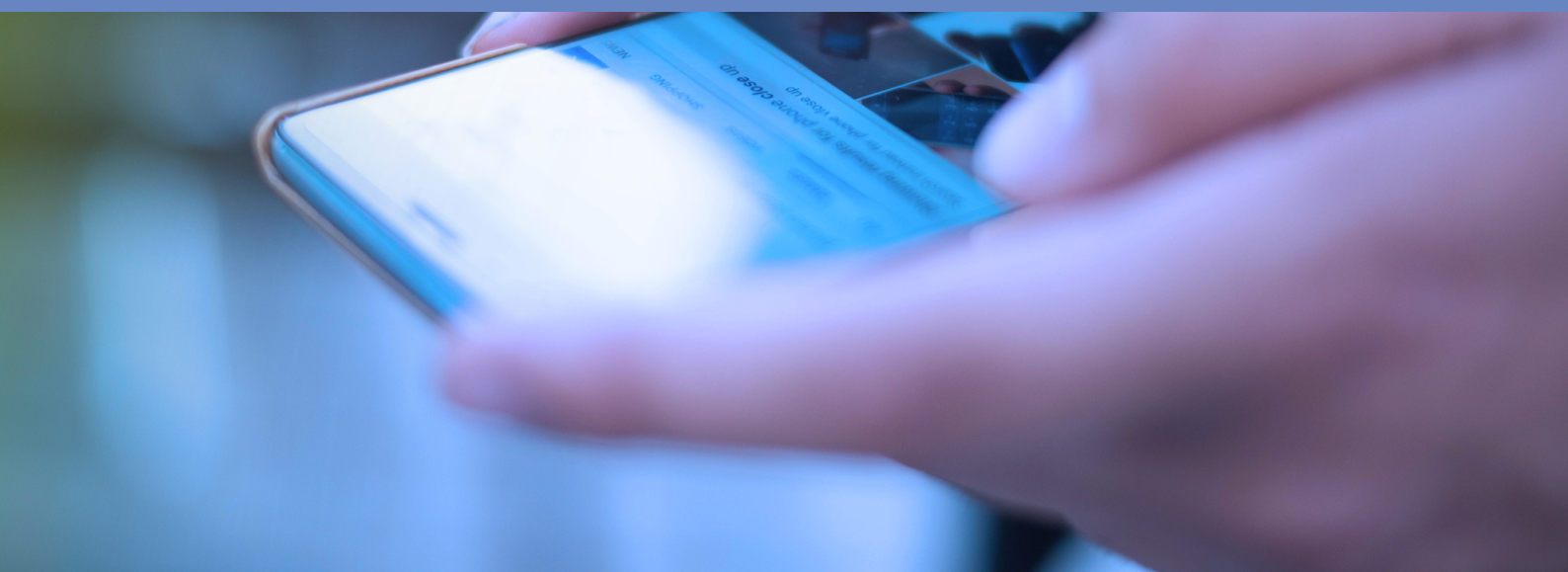
Link: Configurações seguras em dispositivos industriais | INCIBE-CERT | INCIBE

Acesso externo em SCI

O acesso externo é uma tecnologia que será cada vez mais implementada nas empresas devido aos seus benefícios, como a comodidade que oferece aos colaboradores e a redução de custos.

Mesmo assim, deve-se observar que, com essa tecnologia, devemos ter muita cautela, pois também pode causar diferentes problemas de cibersegurança para a empresa, como o acesso de usuários não autorizados ou o roubo de informações confidenciais, razão pela qual o uso de ferramentas como conexões VPN ou a implementação de equipamentos de monitoramento dedicados, como o SOC OT, são muito importantes para garantir a segurança do acesso remoto.

Link: Acesso externo no ICS: uma faca de dois gumes? | INCIBE-CERT | INCIBE



RESPONSABLES CIBER

María Pilar Torres Bruna

Directora de Cibersegurança na NTT DATA Latam y Perú

maria.pilar.torres.bruna@emeal.nttdata.com

Carla Passos Schwarzer

Directora de Cibersegurança na NTT DATA Brasil

carla.passosschwarzer@emeal.nttdata.com

Miguel Angel Garzon Ramirez

Manager de Cibersegurança na NTT DATA Colombia

miguel.angel.garzon.ramirez@emeal.nttdata.com

Fernando Vilchis

Manager de Cibersegurança na NTT DATA México

fernando.vilchisrivero@emeal.nttdata.com

Nestor Gerardo Ordoñez

Manager de Cibersegurança na NTT DATA EE.UU

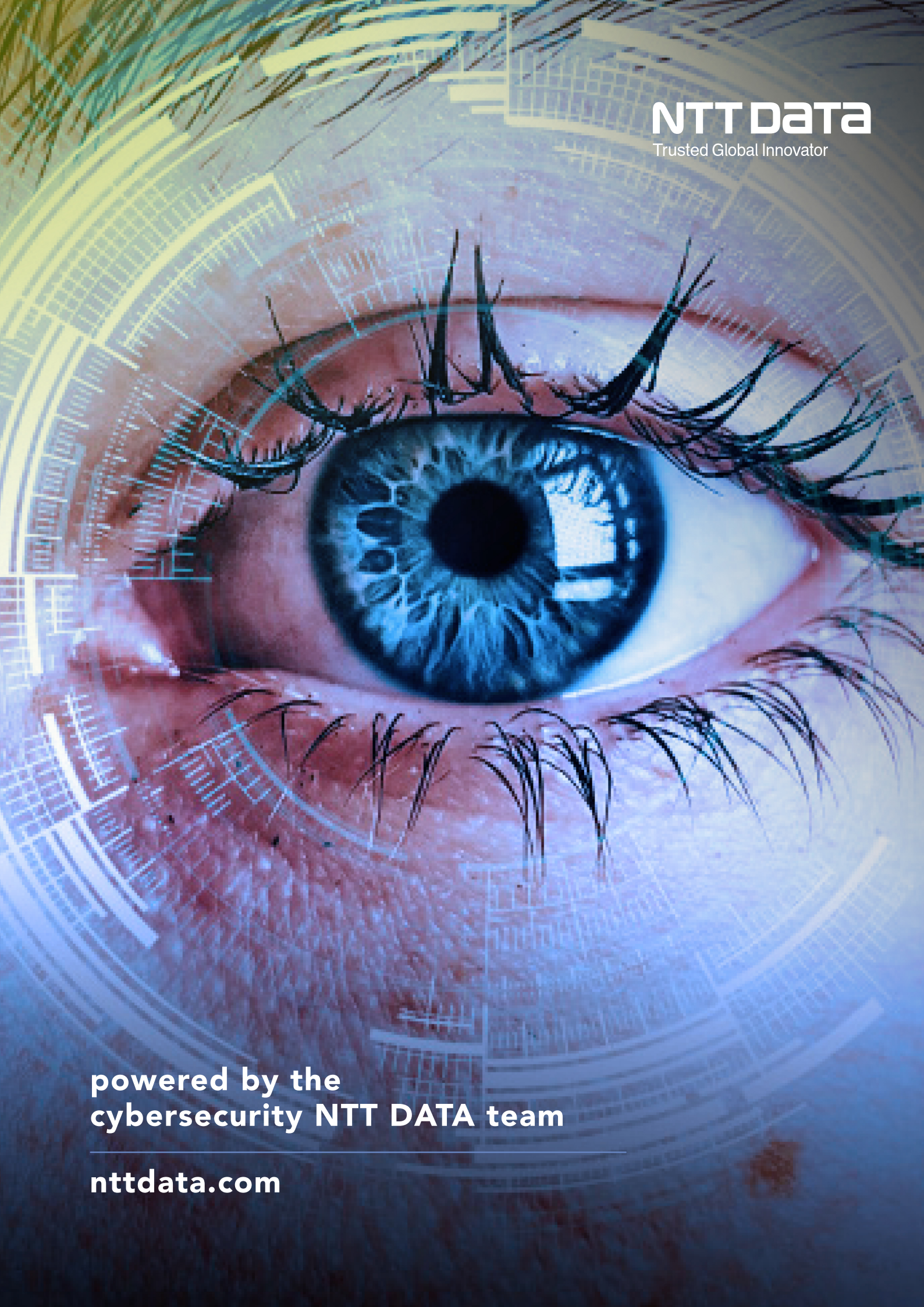
nestor.ordonez.ramirez@emeal.nttdata.com

Jose Uzcategui

Manager de Cibersegurança na NTT DATA Chile

jose.uzcategui@emeal.nttdata.com

Ou escreva para nossa caixa de correio principal: ciberseguridad_latam@emeal.nttdata.com


NTT DATA
Trusted Global Innovator
powered by the
cybersecurity NTT DATA team
nttdata.com