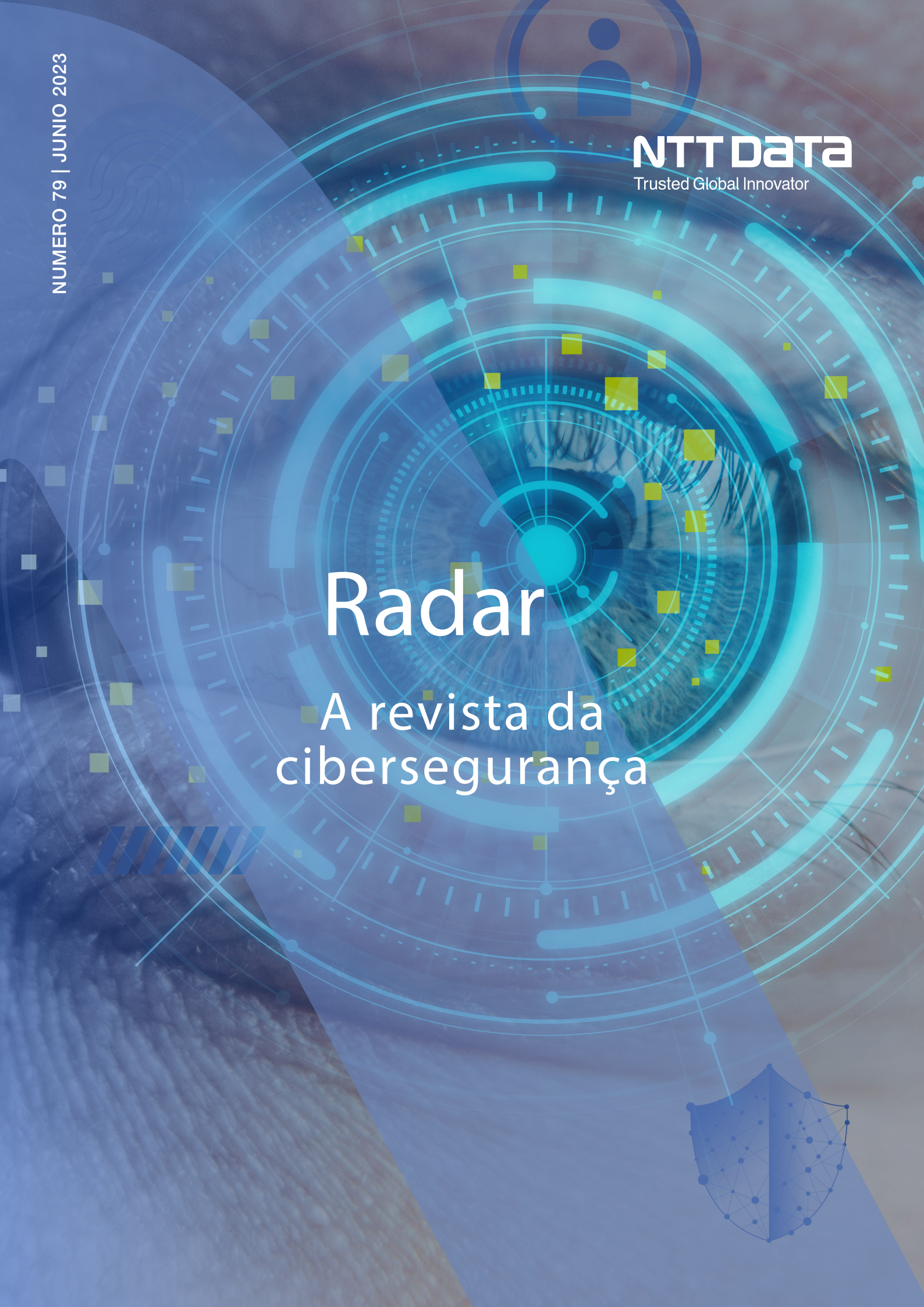
NUMERO 79 | JUNIO 2023

NTT DATA
Trusted Global Innovator



Radar

A revista da cibersegurança

TEREMOS IAG (INTELIGÊNCIA ARTIFICIAL GENERATIVA) ATÉ O FIM DE 2023?

O desenvolvedor Sigi Chen, citando fontes anônimas, twittou há algumas semanas *"Fui informado de que o GPT-5 está programado para concluir o treinamento em dezembro e que o OpenAI espera que alcance a IAG"*.

Mas o que é exatamente a IAG?

IAG ou Inteligência Artificial Generativa é quando uma IA aprende e compreende tarefas ou conceitos comumente executados por humanos. Diferentemente da IA especializada ou restrita, que se concentra em tarefas específicas e é projetada para uma finalidade específica, a IAG pode se adaptar e lidar com problemas novos e desconhecidos, demonstrando um nível de autonomia e flexibilidade cognitiva semelhante ao dos seres humanos. Diferentemente da inteligência artificial, que se baseia em conjuntos de dados em constante expansão para realizar tarefas mais complexas, a IAG exibirá os mesmos atributos relacionados diretamente ao cérebro humano, sendo descrita como um tipo de IA que pode entender, aprender e realizar tarefas intelectuais de forma muito semelhante ao cérebro humano. **Em outras palavras, IAG é a capacidade da IA de aprender da mesma forma que os humanos.**

A IA refere-se a uma máquina que pode copiar habilidades cognitivas humanas, como resolução de problemas e aprendizagem. Mas um ser humano precisa primeiro programar a máquina para que ela possa aprender com os padrões do passado para criar novas informações ou resolver um problema. Enquanto a IA é pré-programada para executar uma tarefa que um ser humano pode executar, mas de forma mais eficiente, a IAG espera que a máquina seja tão inteligente quanto um ser humano. Até o momento, a IAG é um objetivo na pesquisa de inteligência artificial, mas ainda não foi alcançado.

Como todas as tecnologias, a IAG tem seu lado positivo (aumento da produtividade ao acelerar os processos ativados pela IA e liberar as pessoas do trabalho repetitivo, impulsionar a economia global ou ajudar a fazer novas descobertas científicas) e seu lado, digamos, "imprevisto ou negativo" (difusão de bots de aparência humana extremamente convincentes em plataformas de redes sociais, concentração dessa tecnologia em poucas mãos, demissão de empregos, uso indevido).

Justamente para evitar esses últimos efeitos indesejados, mais trabalho deve ser feito para tornar esses sistemas mais precisos, seguros, interpretáveis e transparentes. Para isso, é preciso trabalhar com legisladores e promover o desenvolvimento de sistemas sólidos de governança de IA, que devem incluir, no mínimo: autoridades reguladoras novas e competentes dedicadas à IA, bem como supervisão e monitoramento de sistemas de IA de alta capacidade e grandes volumes de capacidade computacional. Nesse sentido já temos algumas iniciativas como **A Lei de Inteligência Artificial (AI Act)**, que é um regulamento proposto em 21 de abril de 2021 pela Comissão Europeia cujo objetivo é introduzir um quadro regulamentar e jurídico comum para a inteligência artificial, mas é evidente que mais trabalho precisa ser feito nesse sentido.

Resta saber se o ChapGPT 5 vai finalmente obter o IAG ou não, e como acontece com outras questões de tecnologia de ponta como a supremacia quântica (o momento em que um processador quântico é capaz de realizar uma determinada tarefa que não possa ser executada por qualquer computador clássico em um tempo razoável), há todo tipo de opinião, desde quem pensa que já se conseguiu (principalmente por cientistas chineses) até quem, muito mais cético, pensa que nunca se conseguirá. A verdade é que há muita gente e esforço por trás de todas essas questões e pelo menos no que diz respeito à IAG, poderemos descobrir no fim deste mesmo ano com o ChapGPT-5…!!! e esperemos que tenha sido preenchido o posto publicado dias atrás pela OPEN AI procurando um "engenheiro para um interruptor de morte" (ou desligamento) que deveria estar ciente de desconectar os servidores em caso de catástrofe….

Maria Pilar Torres Bruna
Cybersecurity Director na NTTDATA Europe & Latam

CIBERCRÔNICA

Iniciamos esta nova edição do RADAR com a seguinte mensagem: a segurança on-line continua sendo uma preocupação constante para empresas e usuários em todo o mundo. Recentemente, o consultor e analista de redes sociais Matt Navarra relatou no Twitter que hackers invadiram páginas verificadas do Facebook para publicar anúncios que distribuem malware.

Um dos sites hackeados, o Meta Ads, enganou os usuários para que baixassem uma ferramenta de administração "mais profissional e segura" devido a problemas de segurança no navegador. No entanto, em vez de baixar uma ferramenta legítima, o link redirecionava os usuários para uma página da Web infectada por malware. A outra página hackeada se apresentava como sendo o Google AI e direcionava os usuários a links falsos para acessar o chatbot de inteligência artificial do Google. Ambas as páginas podem comprar anúncios do Facebook e distribuir links de download suspeitos.

> "Portanto, é importante nunca confiar em links de supostos sites oficiais que são enviados a você por e-mail ou SMS".

Felizmente, ambas as páginas hackeadas foram desativadas e a Meta lançou um programa de verificação chamado "Meta Verified" para aumentar a segurança da plataforma. No entanto, os usuários do Facebook e do Instagram que pretendam ter uma proteção proativa da conta terão de pagar um mínimo de doze euros por mês.

Este incidente destaca a importância da segurança on-line e a necessidade de as empresas implementarem medidas de segurança mais sólidas para proteger seus usuários dos hackers. No entanto, não é apenas a segurança das plataformas de mídia social que precisamos levar em consideração.

Por outro lado, com a temporada de impostos em andamento, os golpistas também estão aproveitando a oportunidade para enganar as pessoas por meio de e-mails e mensagens em massa com golpes em que tentam enganar alguém para que caia na armadilha. Esses ataques, conhecidos como phishing, consistem em enviar mensagens massivamente como se centenas de milhares de anzóis estivessem sendo lançados, na esperança de que alguém caia na armadilha.
Os golpistas usam táticas enganosas, muitas vezes alegando que a Receita irá devolver o dinheiro. Essas mensagens também podem incluir links para sites fraudulentos que parecem oficiais, mas são projetados para roubar informações pessoais, como números de cartão e códigos de segurança. Esses sites são falsificações que usam logotipos e tipografias da Receita para parecer um site oficial.
É aconselhável procurar o site da Agência Tributária ou onde quer que o usuário queira acessar, entrar no site oficial e autenticar-se a partir dele para procurar possíveis notificações.

Em resumo, a segurança on-line continua sendo uma preocupação constante. Com a temporada de impostos em andamento, é importante sermos cautelosos e ficarmos atentos aos e-mails e mensagens que recebemos, pois muitos deles podem ser fraudulentos. As empresas também devem implementar medidas de segurança mais sólidas para proteger seus usuários contra hackers.

Vale destacar também a seguinte notícia. O Instituto Nacional de Cibersegurança (INCIBE) alerta para uma nova tática fraudulenta em que a identidade do Seguro Social é falsificada por meio de smishing.

O objetivo desse golpe é obter os dados pessoais das vítimas por meio de um site fraudulento que contém um formulário. As mensagens de texto indicam que é necessário atualizar o cartão de saúde usando o link anexado no corpo da mensagem.
Se o usuário clicar na URL, ele será redirecionado para um site malicioso que pede para preencher um formulário com as seguintes informações: nome, sobrenome, e-mail e data de nascimento. Uma vez inseridos esses dados, os cibercriminosos terão acesso a todas as informações necessárias para realizar ataques cibernéticos e enganar as vítimas.

Por outro lado, o INCIBE alerta que não está descartada a existência de outras campanhas semelhantes por meio de e-mails solicitando as mesmas informações. Além disso, as mensagens de texto relatadas até agora contêm erros ortográficos em sua redação, o que levanta suspeitas sobre sua autenticidade.

Outra notícia curiosa, agora que o uso de IAs está na moda, e especificamente o chatGPT, é a que a Meta trouxe à tona que detectou, na rede, links para aplicativos que simulam ser ChatGPT com malware.
A Meta revelou algumas das ações realizadas durante o primeiro trimestre de 2023 para enfrentar as ameaças detectadas em seus aplicativos voltados para pessoas físicas e jurídicas. Essas ameaças incluem campanhas de malware nas quais os criminosos cibernéticos falsificam os aplicativos do ChatGPT, bem como a identificação de nove redes antagônicas envolvidas em operações de espionagem cibernética.
Em seu comunicado no site, a Meta detalha que um dos tipos de ataque mais relevantes neste período foram as campanhas de malware nas quais os cibercriminosos se aproveitam de temas populares, como a tecnologia de Inteligência Artificial (IA) generativa com ChatGPT, para atrair a atenção dos usuários.
Especificamente, a empresa informa que, desde março, seus analistas identificaram cerca de dez famílias diferentes de malware que falsificam aplicativos do ChatGPT e ferramentas semelhantes. Campanhas relacionadas a golpes com criptomoedas também foram detectadas.

Nessas campanhas, agentes maliciosos criaram extensões de navegador maliciosas disponíveis em lojas oficiais da web, oferecendo ferramentas falsas relacionadas à IA. Às vezes, essas extensões até incluíam recursos reais do ChatGPT junto com o malware, para se camuflar e evitar levantar suspeitas.
No entanto, a equipe de pesquisadores da Meta conseguiu bloquear mais de mil extensões maliciosas dessas campanhas de malware para impedir que os usuários as compartilhassem em seus aplicativos. A empresa também relatou essas campanhas maliciosas para outros aplicativos de compartilhamento de arquivos do setor, para que eles também possam tomar as medidas adequadas.

Também foi detectado um novo golpe que consiste em se passar pela empresa FedEx para extrair os dados bancários dos clientes. O golpe é realizado mediante o envio de um e-mail fraudulento no qual, com a desculpa de efetuar um pagamento para receber uma encomenda da FedEx, redireciona, por meio de um link, para uma pesquisa e dois formulários que solicitam dados pessoais e bancários.
Se o destinatário tiver recebido uma mensagem de e-mail supostamente da FedEx solicitando o pagamento para receber uma encomenda, mas não tiver compartilhado suas informações pessoais, é recomendável que o usuário marque o e-mail como spam e exclua-o de sua caixa de entrada.

POR QUE AS IAS PODEM AJUDAR NO TRABALHO DIÁRIO DE UM FUNCIONÁRIO DE CIBERSEGURANÇA E QUE PAPEL ELAS DESEMPENHAM?

Por: NTT DATA Europa & Latam

A inteligência artificial (IA) é um ramo da informática e da ciência da computação que se concentra em desenvolver sistemas ou programas que podem executar tarefas que, em geral, exigem inteligência humana, como aprendizagem, percepção, raciocínio e resolução de problemas. Os sistemas de IA utilizam técnicas e algoritmos que lhes permitem aprender com a experiência e melhorar seu desempenho ao longo do tempo. Essas técnicas incluem, por exemplo, aprendizagem automática (machine learning), processamento de linguagem natural (natural language processing), visão computacional (computer vision) e robótica, entre muitas outras.

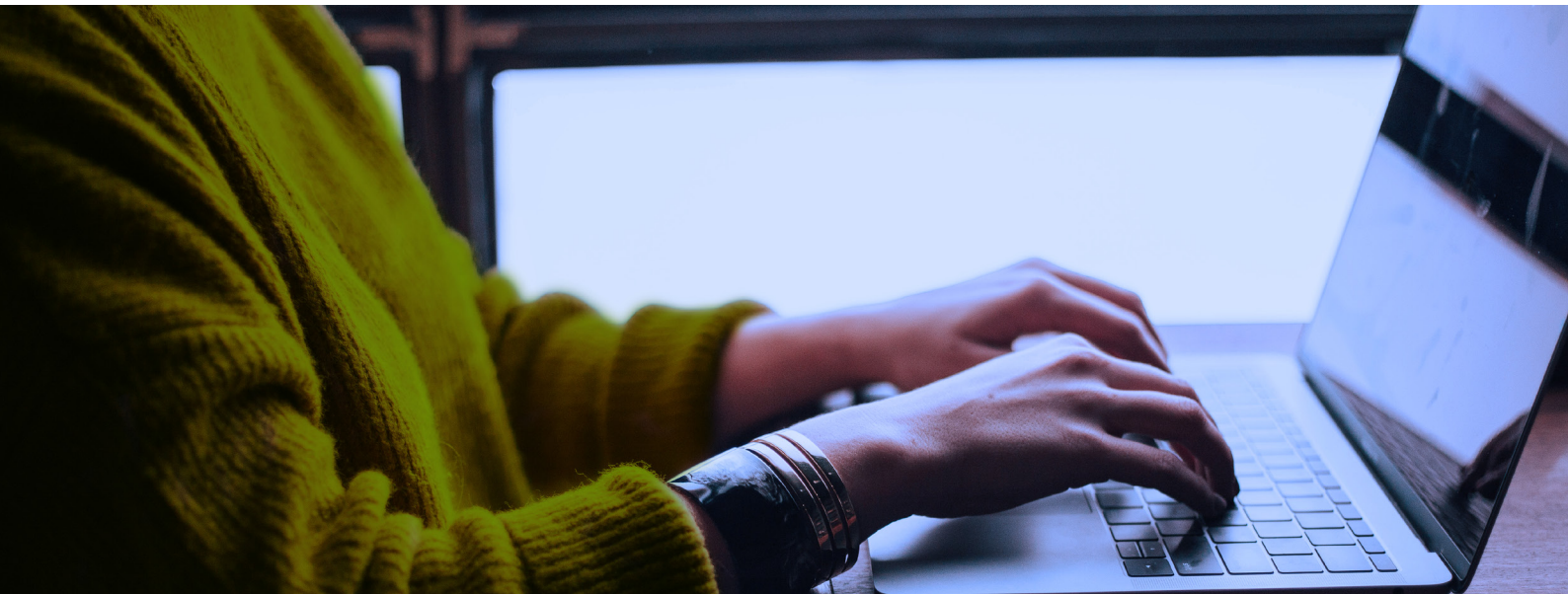
A IA é aplicada em uma ampla variedade de áreas, como medicina, educação, indústria, comércio e entretenimento. Seu potencial para melhorar a eficiência e a qualidade de vida é enorme, embora também coloque importantes desafios éticos e sociais que devem ser abordados.

Que tipos de IAs existem atualmente?

Embora quando pensamos em inteligências artificiais, ChatGPT ou DALL-E 2 venham à mente, elas não são as únicas. Existem vários tipos de inteligência artificial, cada uma com sua própria abordagem e aplicação. Alguns dos tipos mais comuns de IA incluem:

- **Sistemas especialistas:** são sistemas que utilizam conhecimentos específicos de especialistas humanos em uma determinada área para tomar decisões e executar tarefas. São usados em áreas como medicina, engenharia e gestão empresarial.
- **Aprendizagem automática:** é um tipo de IA que utiliza algoritmos para permitir que os sistemas aprendam e melhorem por meio da experiência. É usada em aplicativos como detecção de fraude, reconhecimento de padrões e tomada de decisão.
- **Redes neurais:** são sistemas de IA que imitam a estrutura e o funcionamento do cérebro humano. São usadas em aplicativos de reconhecimento de imagem e fala, bem como na tomada de decisões em tempo real.
- **Processamento de linguagem natural:** é um tipo de IA que permite que os sistemas entendam e respondam à linguagem humana. É usado em aplicativos como chatbots e assistentes virtuais.
- **Robótica:** É um campo da IA que se concentra no desenvolvimento de robôs inteligentes e autônomos que podem realizar tarefas físicas em ambientes complexos.

Cada tipo de IA pode dar origem a uma infinidade de aplicativos diferentes, já que cada uma pode ser treinada para desempenhar diferentes funções.



Como são treinados no campo da cibersegurança?

As inteligências artificiais (IA), como o ChatGPT, não são necessariamente projetadas para a área da cibersegurança especificamente, mas podem ser treinadas para executar tarefas relacionadas à segurança em informática.

Treinar uma IA para cibersegurança envolve ensiná-la a reconhecer padrões e anomalias nos dados e a tomar decisões com base nessas informações. Isso é alcançado por meio da alimentação da IA com grandes quantidades de dados de segurança, como registros de atividade de rede, registros de eventos de segurança, registros de aplicativos e dados de ameaças conhecidas.

Uma vez que a IA tenha sido treinada para identificar padrões e anomalias, ela pode ser aplicada a várias tarefas de cibersegurança, como detectar invasões, identificar malware, monitorar a atividade da rede, prever comportamentos maliciosos e responder automaticamente a eventos de segurança.

Para manter a IA de cibersegurança eficaz, ela precisa ser atualizada regularmente com novos dados e técnicas de ameaça. Também é importante que as decisões tomadas pela IA sejam monitoradas e ajustadas conforme necessário para garantir precisão e eficácia na proteção dos sistemas de informática e dos dados.

Para o ChatGPT, o modelo GPT-3.5 é treinado em uma grande quantidade de dados não estruturados de diferentes fontes, incluindo páginas da web, livros, artigos de notícias, fóruns e redes sociais, com o objetivo de aprender padrões e associações em linguagem natural. Por meio desse treinamento contínuo, o modelo torna-se cada vez mais preciso e eficaz em sua capacidade de compreender e gerar linguagem natural.

Como essas IAs podem ajudar os perfis de cibersegurança?

As inteligências artificiais podem ajudar na criação de perfis de cibersegurança de várias maneiras, já que permitem analisar grandes quantidades de dados de segurança em tempo real, identificar padrões e anomalias e tomar decisões automatizadas para detectar e responder a ameaças à segurança.

Abaixo estão algumas maneiras pelas quais as inteligências artificiais podem ajudar os perfis de cibersegurança:

1. **Detecção de ameaças:** As IAs podem analisar grandes quantidades de dados de segurança em tempo real e detectar padrões ou comportamentos suspeitos em atividades de rede ou sistemas de informática. Ao identificar esses comportamentos, as IAs podem alertar as equipes de segurança para investigar e responder à ameaça.
2. **Análise de vulnerabilidades:** As IAs podem analisar sistemas e aplicativos para detectar vulnerabilidades conhecidas ou desconhecidas. As equipes de segurança podem usar essa informação para identificar e corrigir vulnerabilidades antes que elas sejam exploradas por invasores.
3. **Identificação de malware:** As IAs podem analisar padrões de comportamento de software e detectar malware que se infiltrou em um sistema de informática. Isso pode ajudar as equipes de segurança a identificar rapidamente a ameaça e tomar medidas para mitigá-la.
4. **Gestão de incidentes de segurança:** As IAs podem ajudar na gestão de incidentes de segurança, fornecendo uma resposta rápida e automatizada a eventos de segurança. Por exemplo, as IAs podem tomar medidas para impedir um ataque ou bloquear comportamentos suspeitos enquanto a equipe de segurança investiga o incidente.
5. **Monitoramento contínuo:** As IAs podem monitorar continuamente a atividade da rede e os sistemas de informática para detectar e responder a ameaças em tempo real. Isso pode ajudar as equipes de segurança a manter uma postura de segurança mais proativa e eficaz.

Em resumo, as IAs podem ajudar os perfis de cibersegurança na detecção de ameaças, análise de vulnerabilidade, identificação de malware, gestão de incidentes de segurança e monitoramento contínuo. Ao automatizar estas tarefas e permitir respostas mais rápidas e precisas a eventos de segurança, as IAs podem melhorar significativamente a postura de segurança de uma organização.

APLICAÇÕES DA INTELIGÊNCIA ARTIFICIAL NA CIBERSEGURANÇA

Por: NTT DATA Europa & Latam

A segurança cibernética tornou-se uma das principais preocupações de indivíduos, empresas e instituições governamentais em todo o mundo. Com a crescente quantidade de dados e dispositivos conectados à rede, o cibercrime aumentou exponencialmente nos últimos anos. Felizmente, a inteligência artificial (IA) pode ser uma ferramenta valiosa na luta contra o crime cibernético.

A IA tem o potencial de revolucionar a cibersegurança de várias maneiras. Em primeiro lugar, os algoritmos de aprendizagem automática podem analisar grandes quantidades de dados para identificar padrões e anomalias no tráfego de rede e nos registros de atividades. Esses padrões podem ajudar e alertar os profissionais de segurança antes que ocorra um incidente que ponha em risco a infraestrutura da organização.

Além disso, a IA pode ser usada em mecanismos de verificação de vírus e para melhorar a detecção de malware. Os algoritmos de aprendizagem automática podem analisar o código de um programa e comparar a amostra com um conjunto de dados conhecido para determinar se é software malicioso. Esses algoritmos podem detectar padrões de comportamento em sistemas que indicam uma infecção por malware.

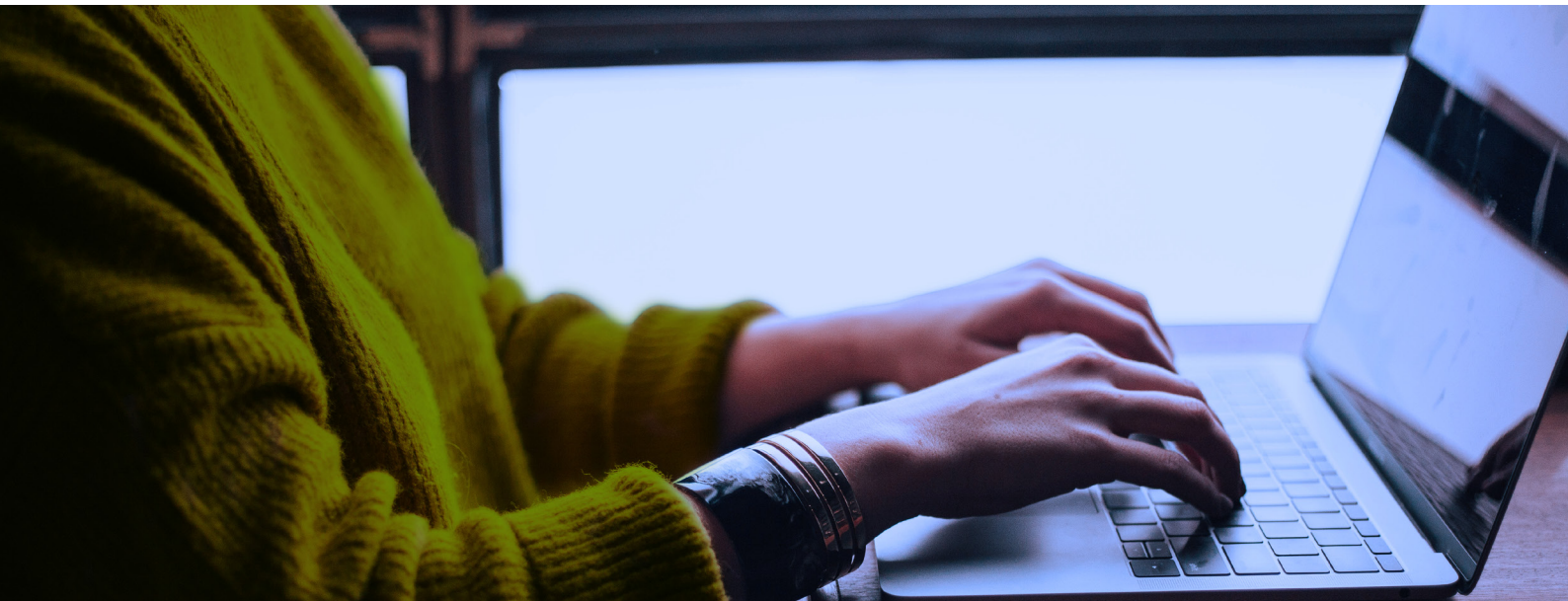
Outra aplicação importante da IA na cibersegurança é a identificação de ameaças internas. Frequentemente, os ataques de informática podem vir de dentro da própria organização, seja por negligência ou intencionalidade. A IA pode analisar padrões de comportamento de funcionários para detectar atividades suspeitas e alertar profissionais.

A IA também pode ser utilizada para melhorar a autenticação e a identificação do usuário. Os sistemas de autenticação baseados em IA podem analisar o comportamento do usuário, como padrões de digitação e como ele interage com a interface do usuário, para determinar se um usuário é legítimo ou impostor.

Em última análise, a IA pode ajudar a melhorar a capacidade de resposta a incidentes de segurança, integrando-a com mecanismos de automatização. Os sistemas de IA podem ser programados para tomar medidas imediatas quando um comportamento suspeito é detectado, como desconectar um dispositivo da rede ou bloquear o acesso a uma conta. Isso pode ajudar a prevenir danos antes que eles ocorram e limitar a propagação do ataque.

Apesar dos potenciais benefícios da IA na cibersegurança, também há preocupações sobre o seu uso. Em particular, a privacidade e a ética são questões importantes a serem consideradas. A IA pode ser utilizada para coletar e analisar grandes quantidades de dados sobre os usuários, levantando preocupações quanto à privacidade. Isso pode incluir a implementação de políticas claras e transparentes sobre o uso da IA, bem como a adoção de práticas de privacidade e segurança sólidas.

Outra preocupação é a possibilidade de invasores usarem a IA para realizar ataques cibernéticos mais sofisticados.



Além disso, os sistemas de IA usados em cibersegurança devem ser rigorosamente testados e avaliados para garantir sua eficácia e confiabilidade. Os perfis de segurança devem trabalhar de forma colaborativa com os desenvolvedores de IA para garantir que os sistemas sejam capazes de detectar uma ampla gama de ameaças e se adaptar a novos riscos à medida que eles surgirem.

Existem diversas ferramentas de cibersegurança que utilizam inteligência artificial para melhorar sua eficácia na detecção e prevenção de ataques cibernéticos. Alguns exemplos dessas ferramentas são os seguintes:

1. **Darktrace:** esta ferramenta usa algoritmos de aprendizagem automática para analisar padrões de tráfego de rede e detectar ameaças em tempo real. É capaz de detectar até mesmo as ameaças mais sofisticadas, como ataques zero-day e ameaças internas.

2. **Cylance:** é uma ferramenta Endpoint Protection Platform (EPP) que utiliza inteligência artificial para identificar e prevenir ataques de malware. A ferramenta utiliza um mecanismo de aprendizagem automática para analisar o código dos programas e determinar se são maliciosos ou não.

3. **Palo Alto Networks:** pode ser usado para melhorar a detecção de ameaças e a prevenção de ataques. A ferramenta utiliza algoritmos de aprendizagem automática para analisar o tráfego de rede e detectar padrões suspeitos.

4. **McAfee:** utiliza inteligência artificial para melhorar a detecção e prevenção de ataques de malware e ameaças internas. A ferramenta utiliza algoritmos de aprendizagem automática para analisar o comportamento do usuário e detectar atividades suspeitas.

É importante ressaltar que a IA não é uma solução perfeita para cibersegurança. Embora possa ajudar a detectar e prevenir ataques, ela não pode substituir completamente os profissionais qualificados. Portanto, deve ser utilizada como uma ferramenta complementar para melhorar a eficácia da segurança cibernética e não como uma única solução.

TENDÊNCIAS

CIBERSEGURANÇA DA INTERNET DAS COISAS (IOT)

A Internet das coisas (IoT) revolucionou a maneira como interagimos com nossas casas e dispositivos. No entanto, esta inovação também apresenta riscos significativos para nossa privacidade e segurança. O crescente número de dispositivos IoT, estimados em mais de 55 milhões em 2023, apresenta inúmeros desafios em termos de segurança.

Muitos desses dispositivos não possuem recursos de segurança adequados e aqueles que possuem geralmente não são configurados e mantidos adequadamente pelos usuários, deixando a porta aberta para possíveis violações de segurança.

Além da segurança, a privacidade também é um grande problema na IoT. Os dispositivos inteligentes coletam dados sobre os usuários, incluindo informações pessoais, como planejamento de sua casa e seus hábitos diários. Frequentemente, esses dados são enviados para terceiros além do fabricante original, o que pode ser uma preocupação para quem se preocupa com sua privacidade. Apesar desses riscos, é possível controlar o acesso dos dispositivos aos dados, embora isso possa limitar a funcionalidade dos dispositivos.

Os dispositivos IoT também podem ter impactos negativos na segurança das empresas, já que os dados armazenados costumam ser mais sensíveis e as empresas têm a responsabilidade legal de protegê-los. No entanto, muitas empresas ignoram os riscos de segurança da IoT. Houve casos de hackers que acessaram bancos de dados por meio de dispositivos de IoT, como em um cassino em que os hackers conseguiram acessar 10 GB de dados por meio do termostato do aquário. Os setores de saúde e fabricação são especialmente vulneráveis, pois os dispositivos IoT usados podem afetar a segurança e a privacidade dos pacientes e dos processos de produção.

Agora que você tem uma ideia de quão vulneráveis os dispositivos IoT podem ser, quais seriam as medidas ou recomendações que podem ser tomadas?

- Considerar se é necessário ter os dispositivos conectados o tempo todo;
- Criar uma rede separada apenas para dispositivos IoT e protegê-la com uma senha forte, atualizar o firmware e fechar as portas que são vetores de transmissão comuns;
- Utilizar senhas fortes e exclusivas para dispositivos IoT, alterar senhas de fábrica e habilitar a autenticação multifator, se possível;
- Verificar frequentemente se há atualizações de segurança para dispositivos IoT e aplicá-las;
- Utilizar um programa antimalware que proteja especificamente os dispositivos IoT.

Em resumo, segurança e privacidade são questões críticas na IoT que devem ser tratadas adequadamente para garantir que os usuários possam usufruir das diversas vantagens que essa tecnologia oferece.

VULNERABILIDADES

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

Gitlab

CVE-2023-2478
Data: 05/05/2023

Descrição. Em 8 de maio, o Gitlab lançou uma atualização de segurança causada por uma vulnerabilidade crítica encontrada em várias versões do Gitlab Community Edition (CE) e do Gitlab Enterprise Edition (EE). O identificador CVE-2023-2478 foi atribuído a esta vulnerabilidade.
Por meio de sua exploração e sob certas circunstâncias, um usuário do Gitlab pode usar um endpoint do GraphQL para anexar um executável malicioso a qualquer projeto. Esta falha de segurança ocorre devido à atribuição incorreta de permissões para acessar recursos críticos do sistema
Link: https://about.gitlab.com/releases/2023/05/05/critical-security-release-gitlab-15-11-2-released/#malicious-runner-attachment-via-graphql https://www.incibe.es/incibe-cert/alerta-temprana/avisos/vulnerabilidad-en-community-edition-ce-y-enterprise-edition-ee-de-gitlab
Produtos afetados.

- Esta vulnerabilidade afeta as seguintes versões do Gitlab Community Edition (CE) e Gitlab Enterprise Edition (EE) de 15.4 a 15.9.7; de 15.10 a 15.10.6; de 15.11 a 15.11.2.

Solução: A principal solução para resolver esta vulnerabilidade é atualizar para as versões mais recentes, conforme apropriado: 15.11.2; 15.10.6; 15.9.7.

Aruba

CVE-2023-22779,-2023-22780, -2023-22781, -2023-22782, -2023-22783, -2023-22784, -2023-22785, -2023-22786, -2023-22787, -2023-22788, -2023-22789, -2023-22790, -2023-22791
Data: 09/05/2023

Descrição. Um total de 13 vulnerabilidades foram descobertas em produtos Aruba, 8 delas de gravidade crítica, 4 altas e uma média. As classificadas como de alta gravidade correspondem a várias vulnerabilidades de injeção de comandos remota e a uma vulnerabilidade de negação de serviço.
Por outro lado, as 8 vulnerabilidades críticas consistem em um estouro de buffer presente em vários serviços utilizados pelo protocolo de gestão de pontos de acesso da Aruba (PAPI). Por meio de sua exploração, um invasor pode executar códigos remotamente com permissões de administrador.
Por fim, a vulnerabilidade de gravidade média permitiria que um invasor divulgasse informações confidenciais em uma rede Wi-Fi com uma configuração específica. No entanto, os cenários em que essa vulnerabilidade pode ser explorada são complexos e dependem de fatores fora do controle do invasor.
Link:https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-006.txt%20 https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-aruba-products-could-allow-for-arbitrary-code-execution_2023-049
Produtos afetados. As vulnerabilidades afetam os seguintes produtos da Aruba:
• ArubaOS: 8.6.0.19 e Aruba Access Points com o software InstantOS e ArubaOS 10:

- ArubaOS 10.3.x: versões 10.3.1.0 e anteriores;
- Aruba InstantOS 8.10.x: versões 8.10.0.4 e anteriores;
- Aruba InstantOS 8.6.x: versões 8.6.0.19 e anteriores;
- Aruba InstantOS 6.5.x: versões 6.5.4.23 e anteriores;
- Aruba InstantOS 6.4.x: versões 6.4.4.8-4.2.4.20 e anteriores

Solução: A Aruba Network emitiu atualizações de segurança para os produtos afetados, por isso é recomendável atualizar para a versão mais recente disponível

PATCHES

Microsoft

Data: 09-05-2023

Descrição. A Microsoft lançou uma série de atualizações de segurança correspondentes ao mês de maio de 2023, corrigindo um total de 38 vulnerabilidades conhecidas: 6 críticas de execução de código remoto, 33 altas, 1 moderada e 9 sem classificação de gravidade. Entre elas, estão três zero-day, duas delas exploradas ativamente:

- CVE-2023-29336: Esta vulnerabilidade presente no Kernel Win32k, permite que um invasor obtenha permissões SYSTEM, o nível mais alto de privilégios dentro de um sistema Windows.
- CVE-2023-24932: usando esta vulnerabilidade, um invasor com permissões de administrador ou acesso físico ao equipamento pode instalar uma política de inicialização maliciosa. Este tipo de malware, denominado UEFI bootkits, é invisível para as ferramentas de segurança, pois é executado no estágio inicial da inicialização do computador.
- CVE-2023-29325 – Esta vulnerabilidade permitiria que um invasor executasse remotamente um código no equipamento por meio de e-mails especialmente criados.

Link:https://msrc.microsoft.com/update-guide/releaseNote/2023-May
https://www.cisecurity.org/advisory/critical-patches-issued-for-microsoft-products-may-9-2023_2023-048

Produtos afetados: Alguns dos produtos afetados são: Microsoft Bluetooth Driver; Microsoft Edge (Chromium-based); Microsoft Office Excel; Microsoft Office SharePoint; Microsoft Office Word; Microsoft Teams; Visual Studio Code; Windows Secure Boot; Windows Win32K. A lista completa dos produtos afetados pode ser consultada no seguinte link: https://msrc.microsoft.com/update-guide

Solução: Recomenda-se atualizar os produtos correspondentes para a versão mais recente disponível.

SAP

Data: 09/05/2023

Descrição. A SAP publicou o patch de segurança mensal, em que corrige um total de 25 vulnerabilidades conhecidas: 2 de gravidades críticas, 9 altas, 10 médias e 3 baixas, além da atualização recorrente da SAP Business Client, que apresenta os últimos patches do Chromium. Entre elas, estão vulnerabilidades de divulgação de informações, escalonamento de privilégios, negação de serviço ou corrupção de memória. Mais detalhes sobre a vulnerabilidade crítica que afeta a BusinessObjects Business Intelligence Platform são fornecidos abaixo:

- CVE-2023-28762: usando esta vulnerabilidade, um invasor com permissões de administrador pode obter o token de login de qualquer usuário sem necessidade de interação de sua parte. Uma vez obtido o token, o invasor pode se passar pelo usuário e acessar ou modificar informações, além de impedir o funcionamento parcial ou total do sistema.

Link: https://onapsis.com/blog/sap-patch-day-may-2023
https://www.incibe.es/incibe-cert/alerta-temprana/avisos/actualizacion-de-seguridad-de-sap-de-mayo-de-2023

Produtos afetados: Os produtos afetados são os seguintes: SAP 3D Visual Enterprise License Manager, versão 15; SAP BusinessObjects Intelligence Platform, versões 420 e 430; SAP AS NetWeaver JAVA, versões SERVERCORE 7.50, J2EE-FRMW 7.50 e CORE-TOOLS 7.50; SAP IBP EXCEL ADD-IN, versões 2211, 2302 e 2305; SAP PowerDesigner (Proxy), versão 16.7; SAP Commerce, versões 2105, 2205 e 2211; SAP GUI for Windows, versões 7.70 e 8,0; SAP Commerce (Backoffice), versões 2105 e 2205; SAPUI5, versões SAP_UI 750, SAP_UI 754, SAP_UI 755, SAP_UI 756, SAP_UI 757 y UI_700 20.

Solução: Recomenda-se atualizar os produtos para a versão mais recente disponível conforme indicado pelo fabricante: https://support.sap.com/en/my-support/knowledge-base/security-notes-news.html

EVENTOS

“Cyber Security International Radar” (CSI Radar)

12-16 de junho de 2023

A empresa Medina Media Events organizará o evento “Cyber Security International Radar” (CSI Radar) em Sevilha. Este evento será realizado de 12 a 16 de junho, onde será dada visibilidade a todos os projetos e soluções em nível nacional e internacional para melhorar a segurança de empresas, instituições e indivíduos. Esta agenda é híbrida, com dois dias presenciais (Palacio de Exposiciones y Congresos de Sevilla) e três virtuais, reunindo mais de 40 palestrantes.

Link: CSI Radar - CSI Radar

III Congresso de Segurança Digital e Ciberinteligência: C1b3rwall

20 a 22 de junho de 2023

O III Congresso de Segurança Digital e Ciberinteligência (C1b3rwall) começa no dia 20 de junho no formato presencial, e vai até o dia 22 de junho. O evento é organizado pela Universidade de Salamanca e pela Polícia Nacional na Escola Nacional de Polícia de Ávila. Este congresso nasceu em 2019 e a última edição reuniu mais de 5000 profissionais relacionados às tecnologias da informação e comunicação, forças e órgãos de segurança, forças armadas, professores universitários e estudantes.

Link: Congresso - C1b3rWall (policia.es)

15º Encontro da Segurança Integral (Seg2)

22 de junho de 2023

Este encontro organizado pelas revistas Red Seguridad e Seguritecnia acontecerá no dia 22 de junho. O evento será intitulado “O novo paradigma de segurança: A resposta aos desafios geopolíticos” e será no formato experiência de TV. Alguns dos tópicos que serão discutidos são a guerra na Ucrânia e a guerra digital, perigos do ciberespaço, regulamentos (5G, NIS2...) inspeções e gestão.

Link: 15º Encontro da Segurança Integral (Seg2) (seguritecnia.es)

XII Simpósio de Segurança GAP

17 a 22 de Abril de 2023

O grupo Aeroportuário (GAP), com o apoio da Segurilatam e a colaboração da Agência Federal de Aviação (AFAC), organizou o XII Simpósio de Segurança GAP em Guadalajara, México. Este evento será limitado a 300 lugares e a participação é apenas por convite pessoal. Os assuntos a serem discutidos neste congresso serão sistemas AVSEC, proteção perimetral, serviços de segurança privada e ciberameaças.

Link: XII Simpósio de Segurança GAP | Segurilatam

RECURSOS

BGP Boofuzzer

É uma ferramenta de código aberto para encontrar vulnerabilidades na implementação do BGP. Esta ferramenta permitirá que as empresas avaliem a segurança dos pacotes BGP que usam internamente, bem como utilizá-la para descobrir novas vulnerabilidades em implementações do BGP por pesquisadores.

LInk: https://noticiasseguridad.com/tutoriales/bgp-boofuzzer-herramienta-para-encontrar-vulnerabilidades-en-la-implementacion-de-bgp/

Goose Tool

É uma ferramenta gratuita que pode ajudar os defensores da rede a identificar possíveis atividades maliciosas em ambientes do Microsoft Azure, Azure Active Directory e Microsoft 365. A ferramenta disponibiliza novos métodos de autenticação e coleta de dados para usar no processo de defesa dos ambientes mencionados.

Link: https://noticiasseguridad.com/tutoriales/la-mejor-herramienta-gratuitita-para-la-deteccion-de-incidentes-ciberneticos-en-microsoft-azure-azure-active-directory-y-microsoft-365/

A Microsoft anuncia o Security Copilot

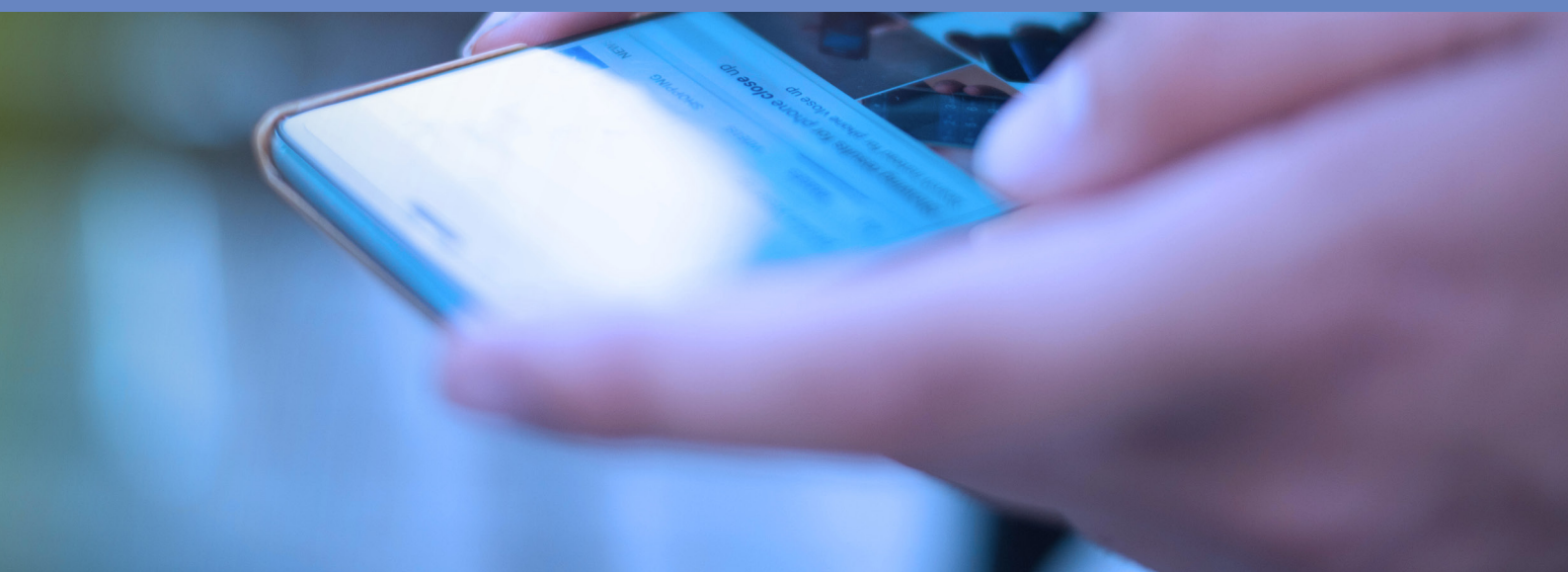
É uma ferramenta de cibersegurança que utiliza inteligência artificial para detectar e responder a ameaças no mundo digital. Seu objetivo é simplificar processos e aprimorar as capacidades das equipes de segurança das organizações. A ferramenta buscará aprender e melhorar continuamente para se adaptar ao cenário de ameaças em constante mudança e permitir que as equipes de segurança estejam preparadas e atualizadas para enfrentá-las com eficiência.

Link: https://cybersecuritynews.es/microsoft-anuncia-security-copilot-una-solucion-con-ia-para-dar-respuesta-ciberamenazas/

Cigent Secure SSD+

É uma unidade SSD que, graças a um sistema de IA, possui uma proteção sólida e intransponível contra todos os tipos de ransomware. Seu uso poderia significar a proteção final de todos os arquivos que estão armazenados dentro dele, o que mudaria tudo para organizações, governos e usuários.

Link: https://www.adslzone.net/noticias/seguridad/adios-malware-unidad-ssd-ia-evita-infecciones-ransomware/



RESPONSABLES CIBER

María Pilar Torres Bruna

Directora de Cibersegurança en NTT DATA Latam y Perú

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

Carla Passos Schwarzer

Directora de Cibersegurança en NTT DATA Brasil

marcelo.nascimento.junior@emeal.nttdata.com

Javier Mauricio Albarracin

Director de Cibersegurança en NTT DATA Colombia

javier.mauricio.albarracin.almanza@emeal.nttdata.com

Fernando Vilchis

Director de Cibersegurança en NTT DATA México

fernando.vilchisrivero@emeal.nttdata.com

Nestor Gerardo Ordoñez

Manager de Cibersegurança en NTT DATA EE.UU

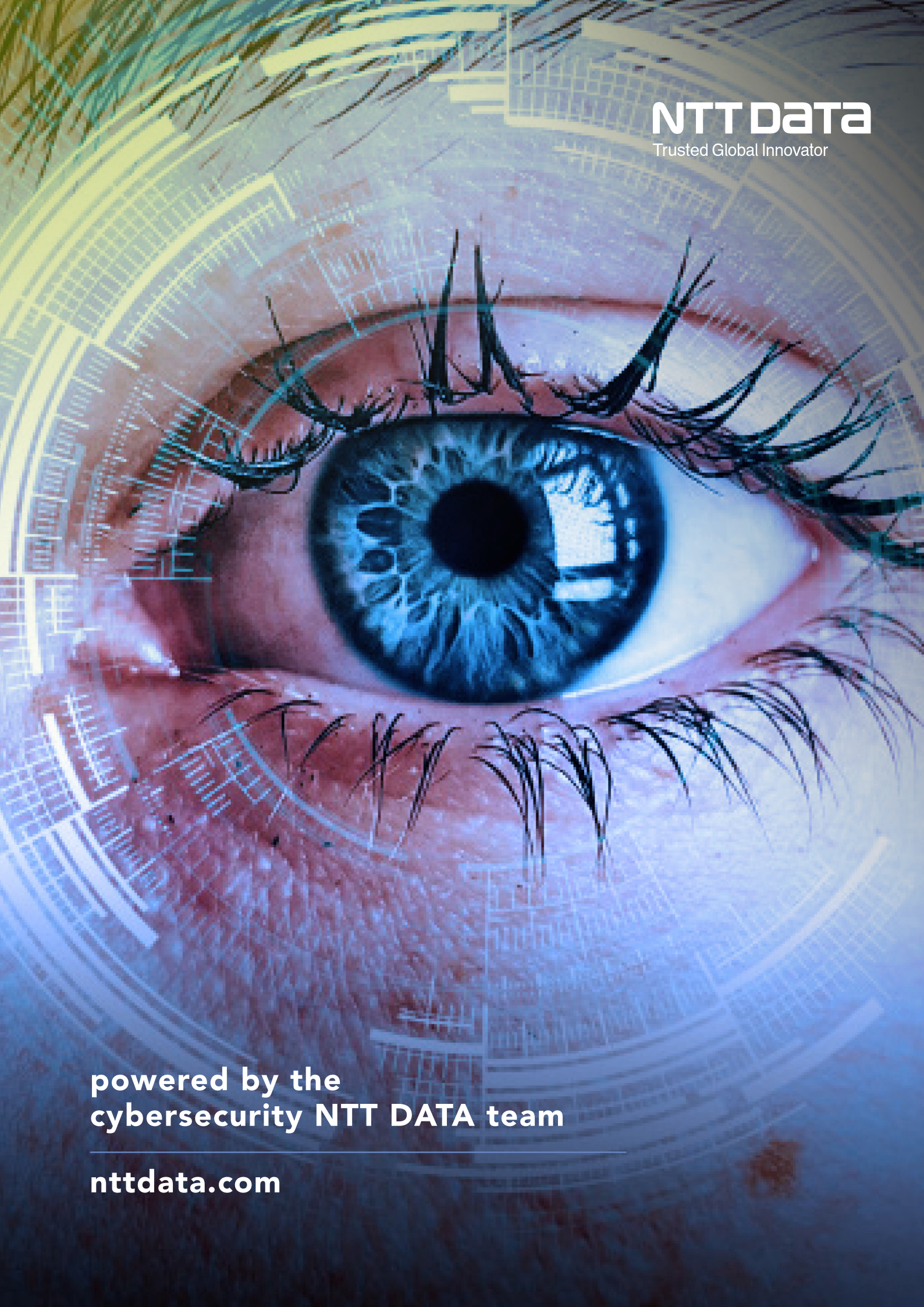
nestor.ordonez.ramirez@emeal.nttdata.com

Carolina Pizarro

Director de Cibersegurança en NTT DATA Chile

carolina.pizarrodiaz@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