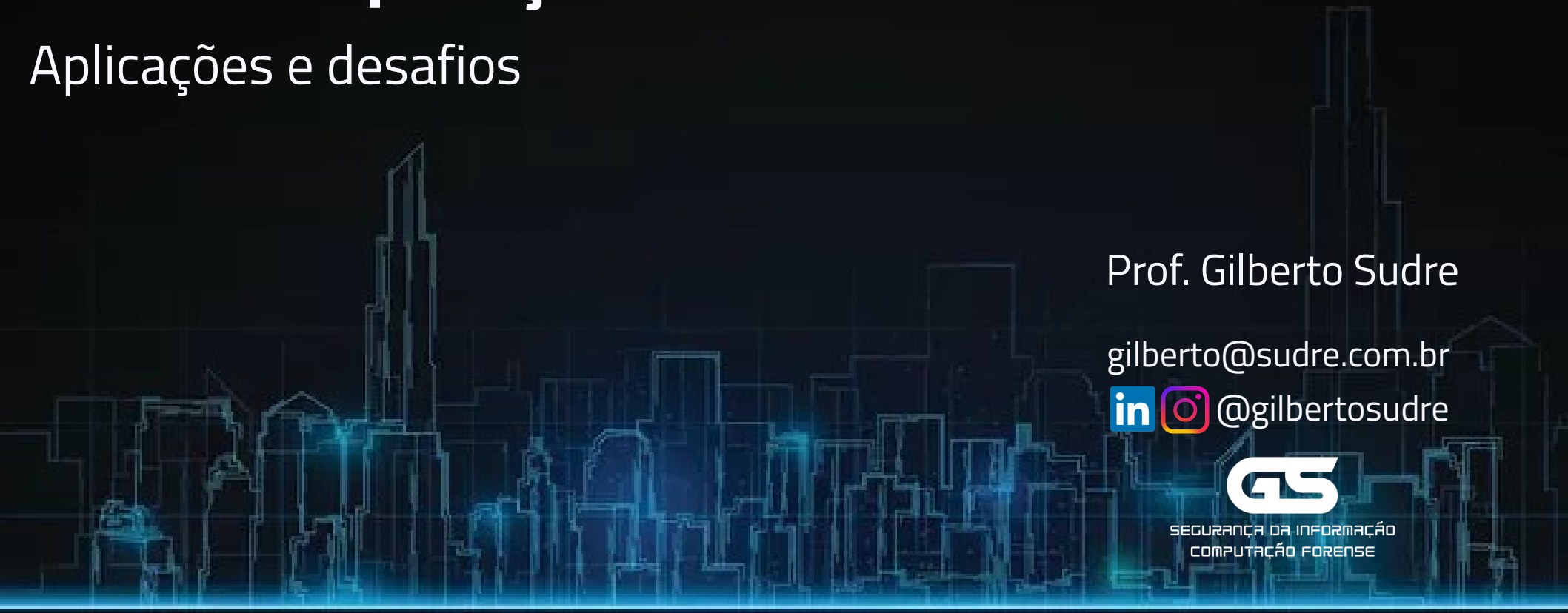
IA e a Computação Forense

Aplicações e desafios



Prof. Gilberto Sudre

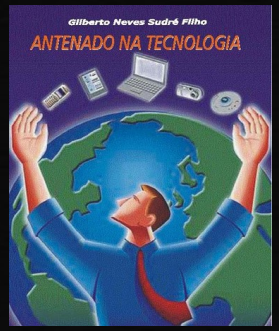
gilberto@sudre.com.br

@gilbertosudre

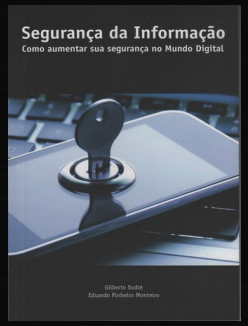
SEGURANÇA DA INFORMAÇÃO
COMPUTAÇÃO FORENSE

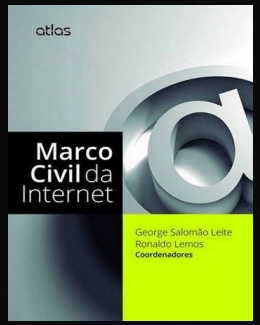
Comitê CB21

Instrutor


Gilberto Neves Sudré Filho
ANTENADO NA TECNOLOGIA


Internet:
O Encontro
de 2 Mundos
Crônicas provocantes sobre a nova Internet


Segurança da Informação
Como aumentar sua segurança no Mundo Digital


atlas
Marco
Civil da
Internet
George Salomão Leite
Ronaldo Lemos
Coordenadores


Redes de Computadores
Tecnologia em Análise e Desenvolvimento de Sistemas


PROCESSO
JUDICIAL
ELETRÔNICO


VOLUME.03
A TECNOLOGIA
COMPU
TAÇÃ
SOCI
EDA
DE
&
ORGANIZADORES
Cristiano Maciel
José Viterbo


Tratado de
Computação Forense
Autores revisores
Gustavo P. Vilar
Eduardo Gusmão
Deivison Franco
Luiz R. Grochocki
Autores colaboradores
Alexandre Vrubel
Diego Fuschini
Eder Gonçalves
Gabriel Nunes
Gilberto Sudré
Gustavo H. M. de Arruda
Joice Dantas
Leandro Barcelos
Luciano L. Kuppens
Luiz F. dos Santos
Mateus de C. Polastro
Patricia Peck Pinheiro
Pedro M. S. Eleutério
Pedro Sanchez
Rafael Barão
Rodrigo Bacelar
Rodrigo Lange
Tony Rodrigues
Organizador
Jesus Antonio Velho

Esta palestra contém informações e opiniões pessoais do palestrante. As visões expressas durante a apresentação são de responsabilidade exclusiva do deste e não representam necessariamente as opiniões ou posições da organização

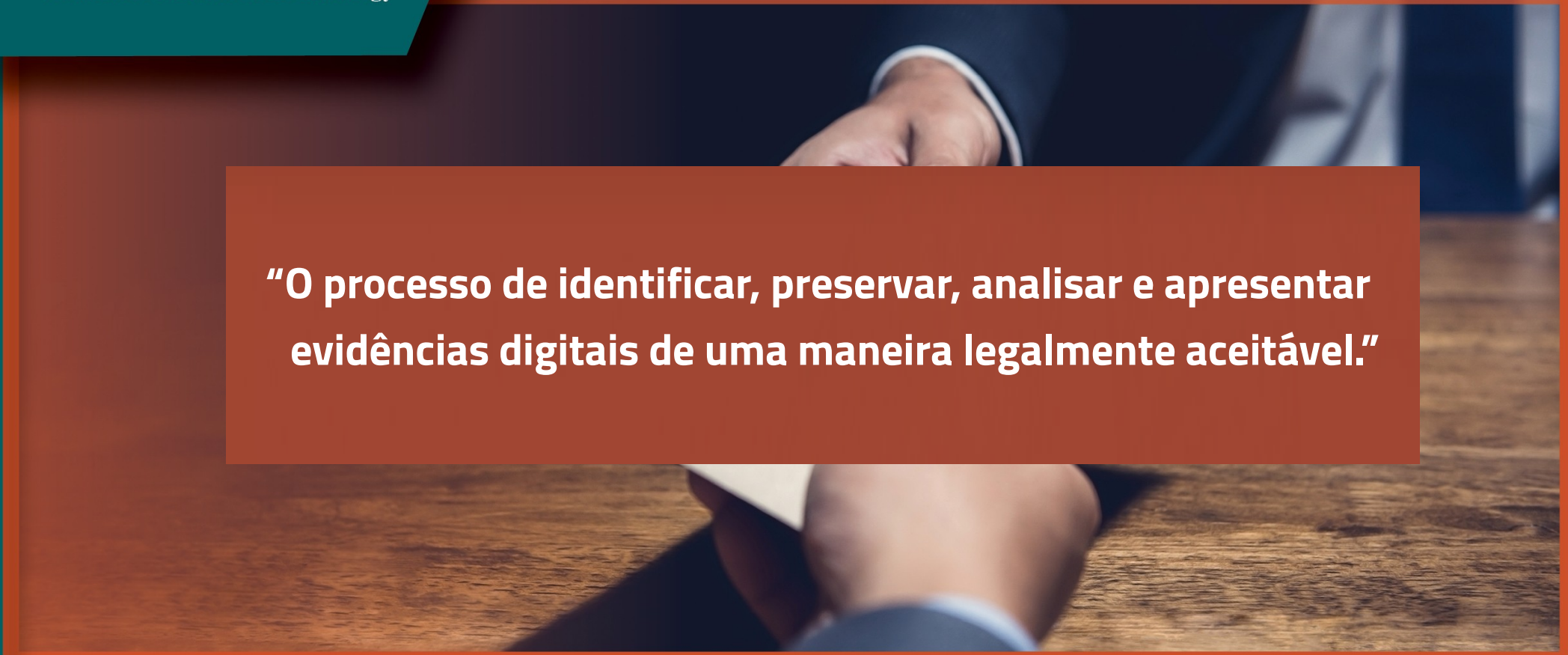
Computação Forense

Computação Forense

Ciência que visa a proteção, investigação, recuperação, coleta, identificação e análise de evidências aplicadas dentro de um processo legal

Estes procedimentos visam recriar, o cenário completo acerca dos fatos ocorridos no mundo digital

Australian Government
Australian Institute of Criminology



“O processo de identificar, preservar, analisar e apresentar evidências digitais de uma maneira legalmente aceitável.”

Evidência Digital

Toda investigação de um crime digital tem como base as evidências e informações coletadas

As evidências e informações estão em um disco rígido, celular, e-mail, e registros de uma rede social

Antes do incidente de segurança

- Adoção de Medidas de Segurança
- Registros dos tratamentos de dados
- Evitar o não-repúdio
- Coleta de Logs adequados
- Documentação atualizada
- Análise dos riscos tecnológicos existentes
- Gestão de identidades e acessos

Após o incidente de segurança

Tomar as medidas adequadas

Determinar origem e responsável pelo incidente

Identificar extensão/impacto e titulares envolvidos

Após o incidente de segurança

Coletar as evidências sobre o Incidente antes de recuperar ou alterar o sistema

De forma profissional e técnica

Importante preservar a Cadeia de Custódia

Inteligência Artificial

Inteligência Artificial

Refere-se à capacidade de máquinas executarem tarefas que normalmente requerem inteligência humana.

Inteligência Artificial

Aprendizado de Máquina (Machine Learning)

Os sistemas aprendem a partir dos dados

Redes Neurais Artificiais

Inspiradas na estrutura do cérebro humano.

Usadas para tarefas complexas como reconhecimento de padrões

Inteligência Artificial

Processamento de Linguagem Natural (PLN)

Habilidade de computadores entenderem, interpretarem e gerarem linguagem humana.

Visão Computacional

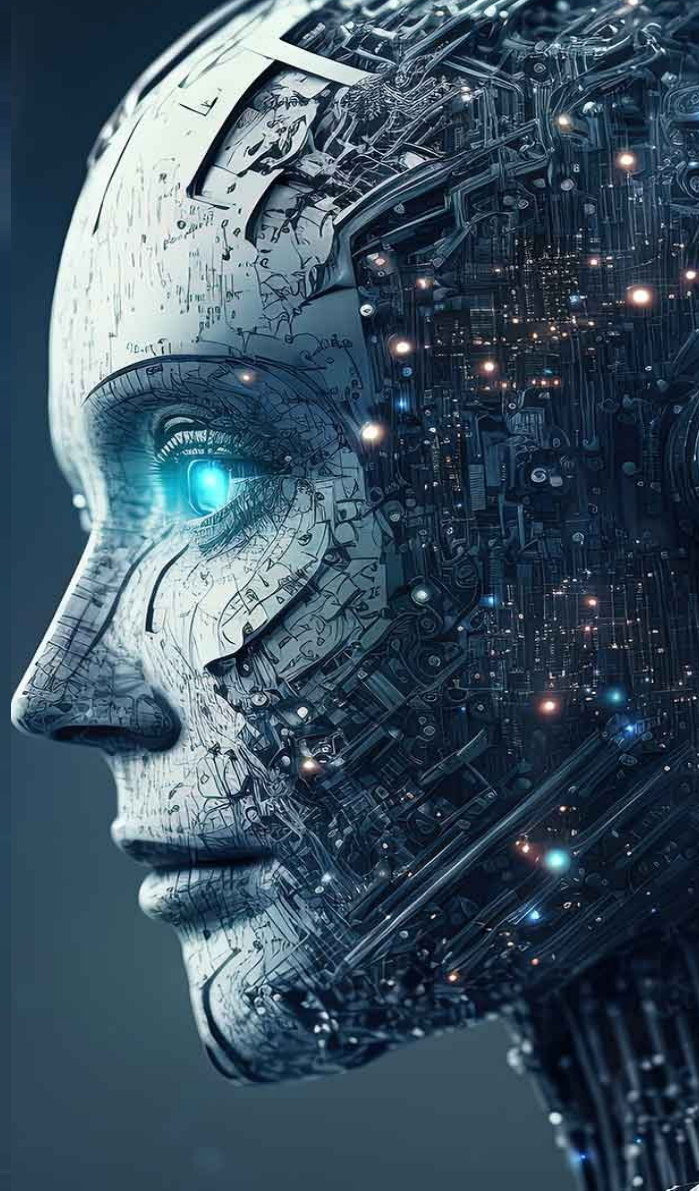
Capacidade dos computadores de interpretar e entender o conteúdo visual.

Aplicações incluem reconhecimento facial e análise de imagens.

Inteligência Artificial

O uso de tecnologias como Inteligência Artificial está crescendo na preparação e criação de ataques

- Clonagem de voz
- Deep Fakes (Vídeos e Fotos)
- Criação de exploits



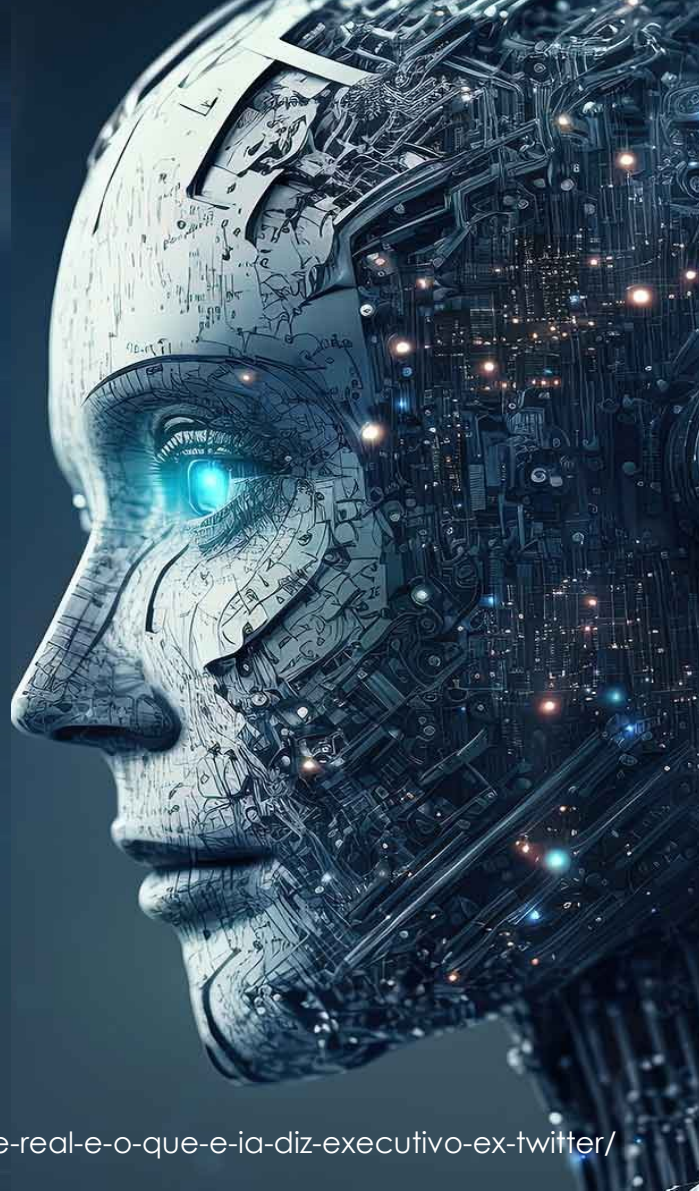
Inteligência Artificial

Nós não saberemos dizer o que é real e o que é IA, diz executivo ex-Twitter

Ex-dono do Twitter acredita que em alguns anos será praticamente impossível dizer se uma imagem é real ou fruto de uma IA generativa

Por **Leandro Costa Criscuolo**, editado por **Bruno Capozzi** | 26/06/2024 04h06

Imagem: TSViPhoto/Shutterstock



https://olhardigital.com.br/2024/06/26/internet-e-redes-sociais/nos-nao-saberemos-dizer-o-que-e-real-e-o-que-e-ia-diz-executivo-ex-twitter/

Inteligência Artificial

Cibercrime

Fraudador imita voz de CEO da Ferrari com deep fake

Da Redação

30/07/2024

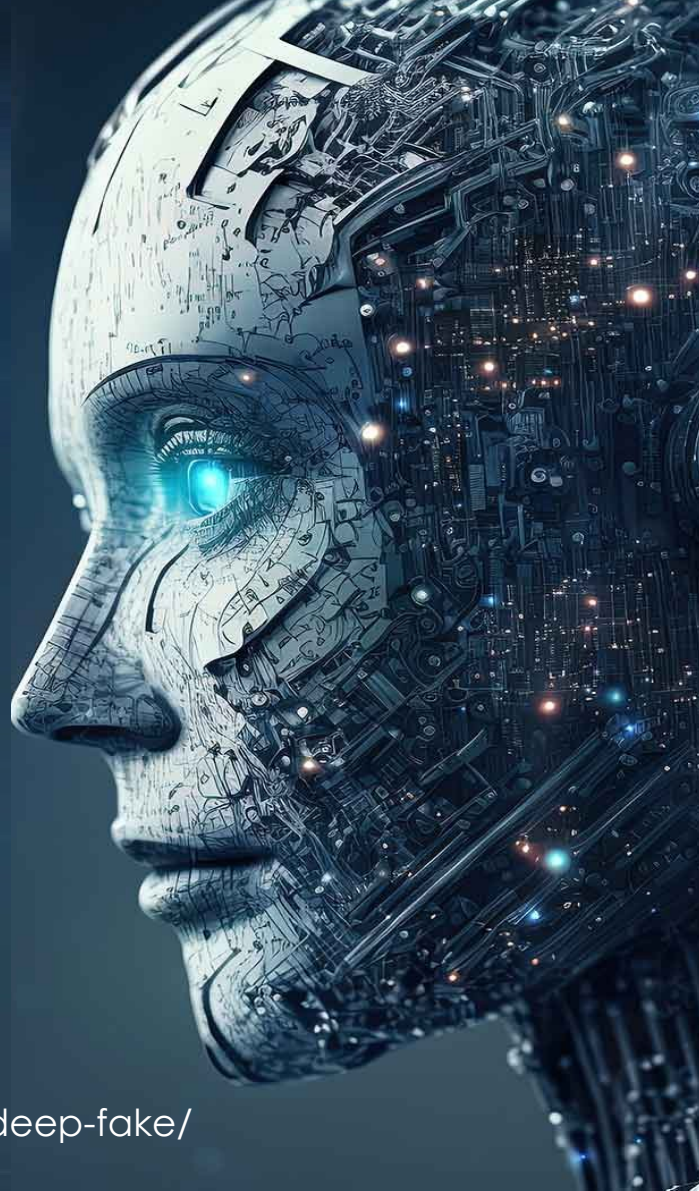
Um ataque com voz construída em deep fake foi descoberto e derrubado por um executivo da Ferrari: numa comunicação por meio do WhatsApp, a pessoa utilizou uma voz com o padrão do presidente da empresa, Benedetto Vigna, para construir um cenário de aquisição de outra companhia, o que certamente poderia terminar em grande prejuízo para a Ferrari.

Leia também

Ataques de BEC e custos de ransomware dobram em um ano

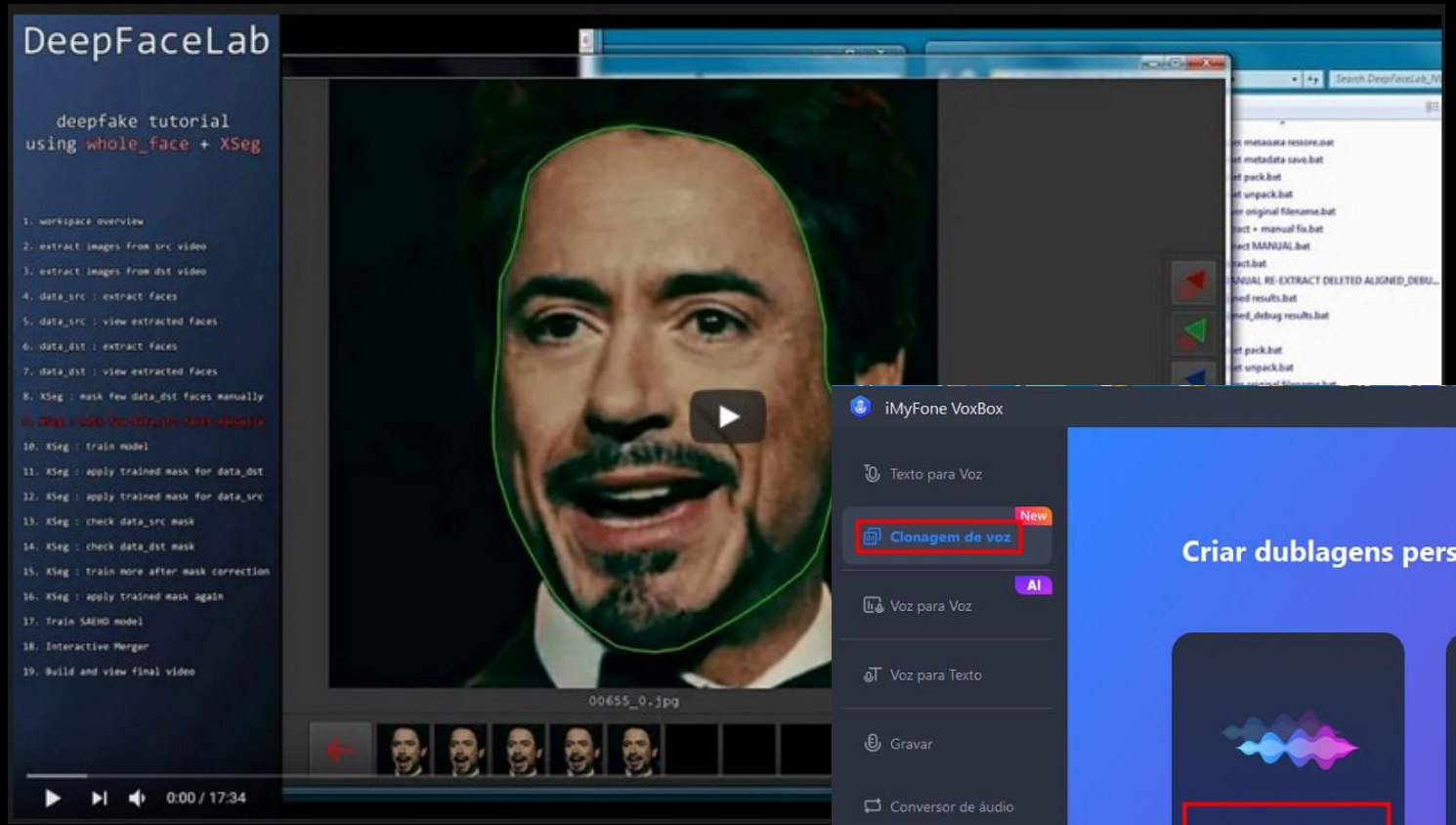
Volume de incidentes de BEC dobra com aumento de phishing

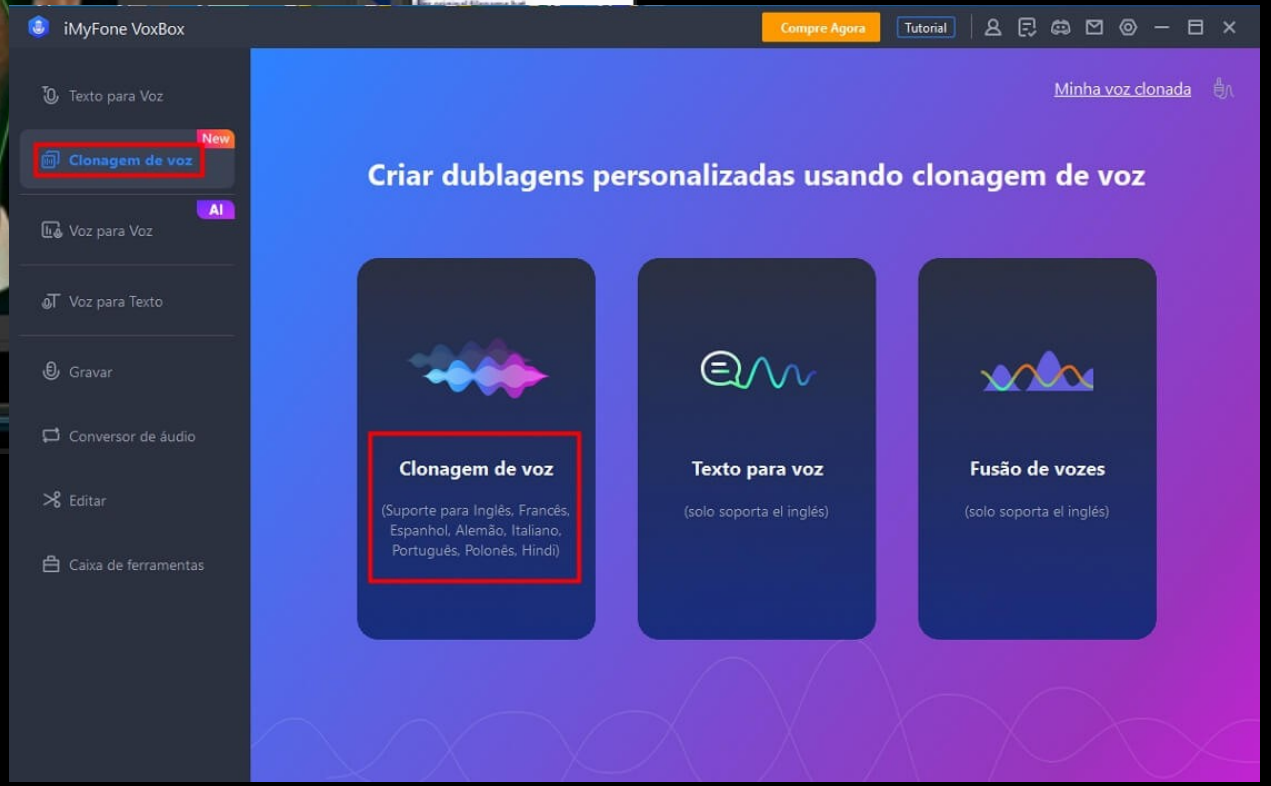
"Prepare-se, estamos prestes a fazer uma grande aquisição e você precisa assinar alguns documentos. Máxima discrição", dizia a primeira de uma série de mensagens comunicadas por telefone por uma pessoa que parecia ter a mesma voz do CEO de Maranello. As informações foram obtidas pela Bloomberg de pessoas familiarizadas com o assunto, que não identificaram o executivo.



https://www.cisoadvisor.com.br/fraudador-imita-voz-de-ceo-da-ferrari-com-deep-fake/


#FalaBrasil
FALA BRASIL
09:16
ATIRADOR ESTÁ FORAGIDO
FALA BRASIL
UMA PESSOA MORRE E CINCO FICAM FERIDAS
EM TIROTEIO DENTRO DE ESTAÇÃO DE METRÔ


DeepFaceLab
deepfake tutorial
using whole_face + XSeg
1. workspace overview
2. extract images from src video
3. extract images from dst video
4. data_src : extract faces
5. data_src : view extracted faces
6. data_dst : extract faces
7. data_dst : view extracted faces
8. XSeg : mask few data_dst faces manually
10. XSeg : train model
11. XSeg : apply trained mask for data_dst
12. XSeg : apply trained mask for data_src
13. XSeg : check data_src mask
14. XSeg : check data_dst mask
15. XSeg : train more after mask correction
16. XSeg : apply trained mask again
17. Train SAEHD model
18. Interactive Merger
19. Build and view final video
00655_0.jpg
0:00 / 17:34


iMyFone VoxBox
Compre Agora
Tutorial
Texto para Voz
Clonagem de voz
New
Voz para Voz
AI
Voz para Texto
Gravar
Conversor de áudio
Editar
Caixa de ferramentas
Minha voz clonada
Criar dublagens personalizadas usando clonagem de voz
Clonagem de voz
(Suporte para Inglês, Francês, Espanhol, Alemão, Italiano, Português, Polonês, Hindi)
Texto para voz
(solo soporta el inglés)
Fusão de vozes
(solo soporta el inglés)

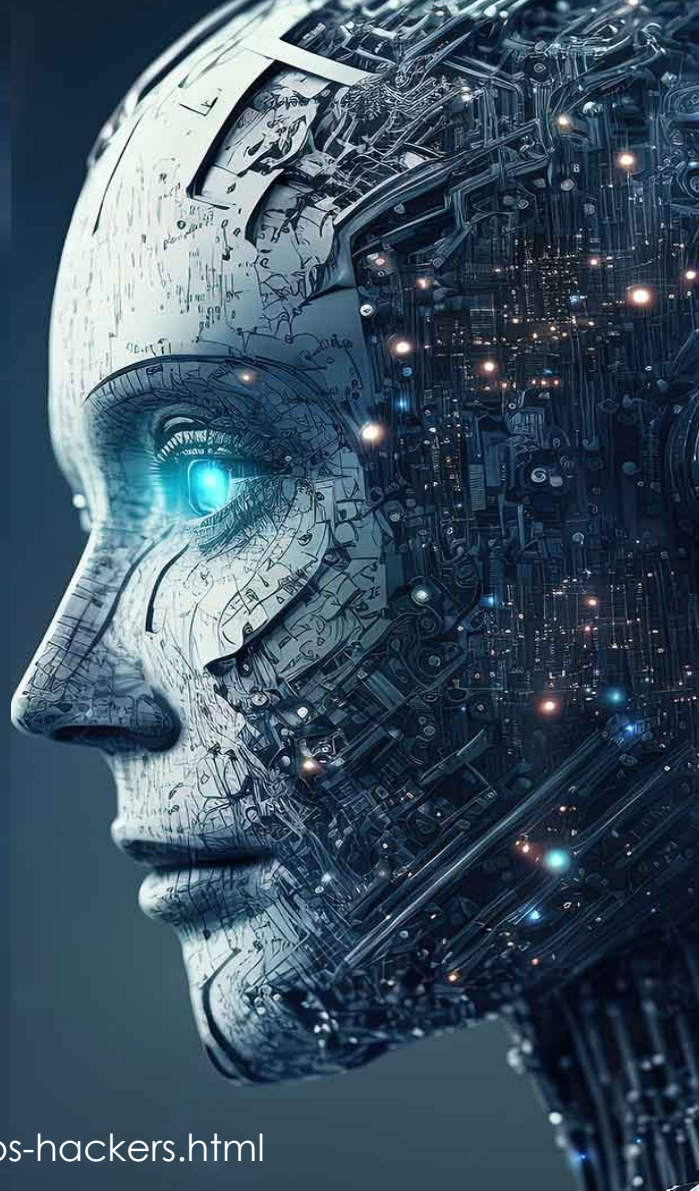
Inteligência Artificial

GPT-4 pode tirar trabalho aos hackers

Gosto Partilhar 14 pessoas gostam disto. Regista-te para veres aquilo de que os teus amigos gostam.

Investigadores descobriram que o modelo GPT-4 consegue explorar vulnerabilidades através da leitura dos "security advisories".

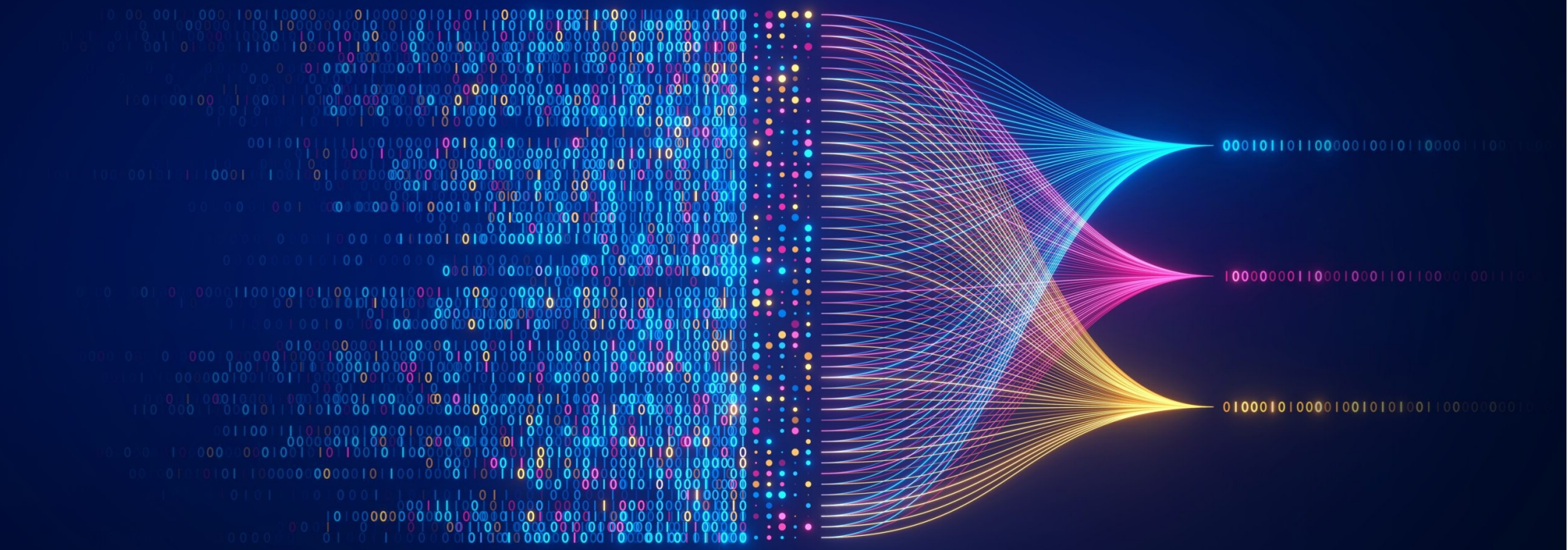
Muito se fala de que os sistemas AI vão tornar muitos empregos obsoletos, e nem sequer os hackers estão livres desse risco. O GPT-4 da OpenAI conseguiu criar exploits em 87% dos casos, com base em 15 vulnerabilidades one-day críticas descritas nos habituais security advisories.



https://abertoatedemadrugada.com/2024/04/gpt-4-pode-tirar-trabalho-aos-hackers.html

Como a IA pode ajudar na Computação Forense?

Análise de grande volume de dados



Análise de grande volume de dados

Inteligência artificial e análise de grande volume de dados são estratégias de investigação de crimes praticados na internet em Sergipe

Follow

Técnicas aumentam a capacidade de identificação de investidas criminosas e são utilizadas para evitar novos casos no estado

Quando o assunto são os crimes praticados com o uso da internet, as investigações tomam nova forma e demandam a utilização de ferramentas e mecanismos que acompanham a movimentação dos criminosos no ambiente digital. É o caso da inteligência artificial e da análise de grandes volumes de dados, que são ferramentas e técnicas que já vêm sendo utilizadas pelo Departamento de Crimes Contra o Patrimônio (Depatri), unidade especializada da Polícia Civil de Sergipe.

https://www.policiacivil.se.gov.br/inteligencia-artificial-e-analise-de-grande-volume-de-dados-sao-estrategias-de-investigacao-de-crimes-praticados-na-internet-em-sergipe/

Detecção de Padrões e Anomalias

Análise de Comportamento de Usuário

Análise de Comportamento de Usuário

Google investe em inteligência artificial para prever comportamento humano

Peter Welchering(cn)

Gigante aposta em pesquisa de inteligência artificial para adivinhar o que o internauta quer, ou qual decisão ele tende a tomar. Desafio está em melhorar qualidade e precisão de análise de dados.

Foto: Fotolia/

Por trás das novas aquisições da Google estão metas muito bem definidas para fortalecer a marca. Há quase três anos na presidência, Eric Schmidt definiu que a competitividade no mercado só pode ser mantida por meio do avanço do setor de inteligência artificial (IA).

https://dw.com/pt-br/google-investe-em-intelig%C3%AAncia-artificial-para-prever-comportamento-humano/a-17410656

Detecção de Fraudes Financeiras

Detecção de Fraudes Financeiras

CRYPTO ID

ÚLTIMAS NOTÍCIAS | QUEM SOMOS | RECEBA NOVIDADES | FALE CONC

CERTIFICADO DIGITAL | ID | IOT | OT | IA | IAM | CYBER | BIO | OPEN

As principais aplicações de IA no combate às fraudes financeiras

10 de janeiro de 2024

Instituições bancárias têm a obrigação de identificar e bloquear transações que não estejam alinhadas com o perfil do cliente, diz STF

Em um cenário de crescente complexidade e sofisticação das fraudes financeiras, a Inteligência Artificial (IA) emergiu como uma ferramenta indispensável ao setor na proteção de seus ativos e na manutenção da confiança dos clientes.

A IA oferece soluções eficazes e proativas para a detecção e prevenção de atividades fraudulentas, redefinindo como as instituições enfrentam esse desafio.

Desafio esse que virou obrigação; em decisão recente, o STF defendeu que as organizações devem ser responsáveis por identificar e bloquear transações que não condizem com o histórico do consumidor.

De acordo com a pesquisa "State of AI in Financial Services 2022", conduzida pela Nvidia, 78% dos profissionais do setor financeiro afirmam adotar ativamente a Inteligência Artificial (IA) por meio de aplicações como *machine learning*, com o intuito de aprimorar suas operações e enfrentar desafios relacionados a fraudes.

Machine learning diz respeito ao uso de algoritmos para organizar dados. É como ensinar um computador a reconhecer coisas por conta própria, por exemplo, mostrando milhares de fotos de notas e moedas para que ele saiba a diferença. Em vez de programar cada regra, a máquina aprende observando os exemplos.

SPOTLIGHT

Entenda o Incidente de Segurança no Siafi que fez o Tesouro exigir a autenticação exclusivamente com Certificados Digitais ICP-Brasil

No Siafi os certificados ICP-Brasil vão conferir Integridade, autenticidade, conformidade, confidencialidade, disponibilidade, legalidade e irretratabilidade.

22 de abril de 2024

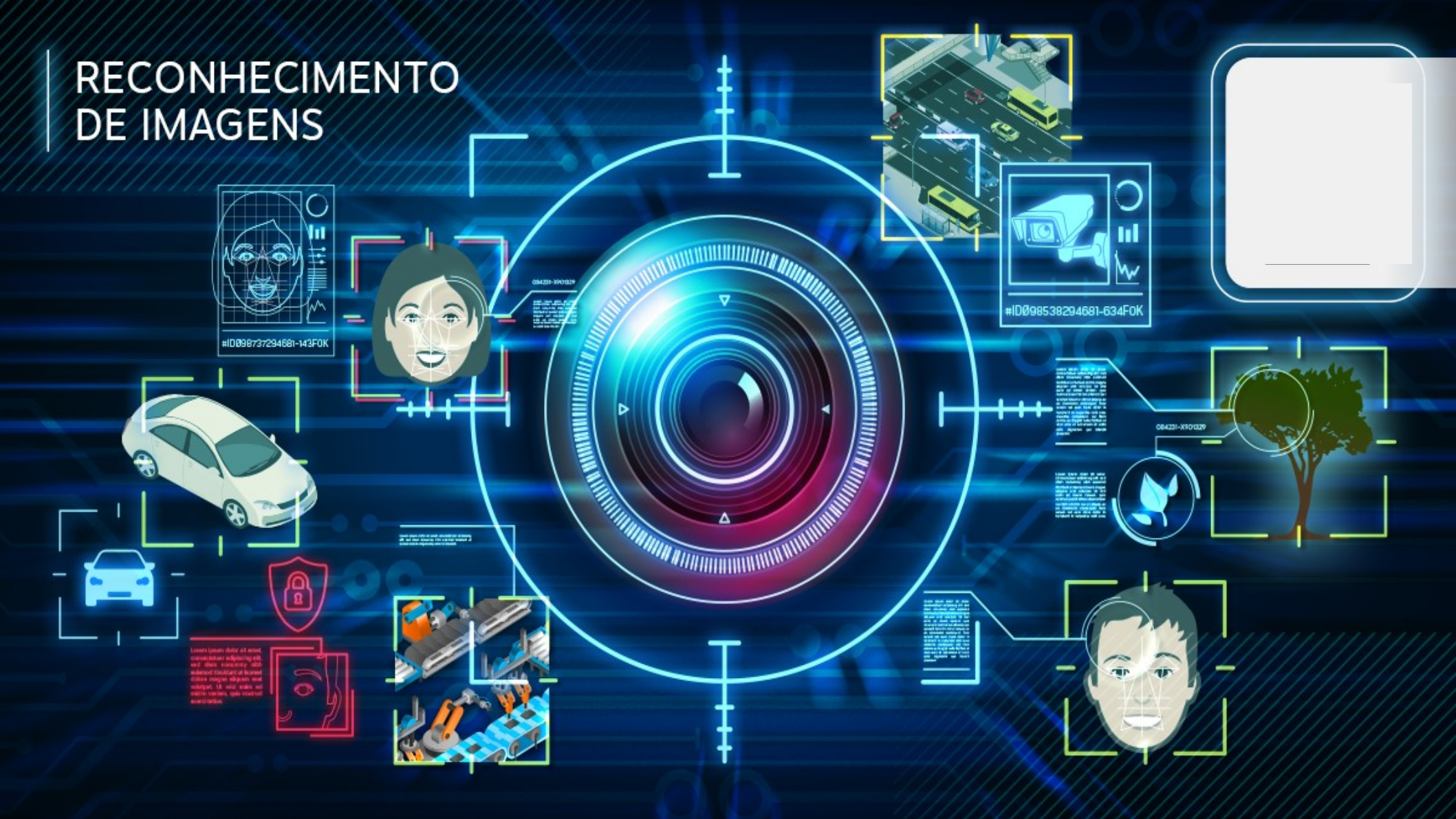
O Halving do Bitcoin: Entendendo o Evento que Redefine a Oferta da Criptomoeda. Por Susana Taboas

Uma visão geral do que é o

https://cryptoid.com.br/criptografia-identificacao-digital-id-biometria/as-principais-aplicacoes-de-ia-no-combate-as-fraudes-financeiras/

Automação de Tarefas Repetitivas

RECONHECIMENTO DE IMAGENS



RECONHECIMENTO DE IMAGENS

Empresas de IA se comprometem em remover material de abuso sexual infantil

Redação
23/04/24 • 19:20

As maiores empresas de tecnologia, como Google, Meta, OpenAI, Microsoft e Amazon, se comprometeram nesta terça-feira a revisar seus dados de treinamento de inteligência artificial para remover material de abuso sexual infantil (CSAM, em inglês) de seus futuros modelos de IA. As companhias prometem não utilizar esse material nos treinamentos, remover imagens ou links para fontes que tenham conteúdo abusivo, além de fazer "testes de resistência" com as IAs para garantir que não geraram CSAM, lançando as novas tecnologias após avaliação quanto à segurança infantil. A IA generativa tem contribuído para aumentar as preocupações com imagens falsas envolvendo pornografia infantil. (The Verge)

https://www.canalmeio.com.br/2024/04/23/empresas-de-ia-se-comprometem-em-remover-material-de-abuso-sexual-infantil/

Processamento de Linguagem Natural

Previsão e Antecipação de Ameaças

Previsão e Antecipação de Ameaças

Brazilian Journal of Technology | 30
ISSN: 2595-5748

Inteligência artificial e policiamento preditivo: possibilidades de inovação tecnológica para a Polícia Militar do Paraná no enfrentamento aos crimes violentos contra o patrimônio com emprego de explosivos

Artificial intelligence and predictive policing: possibilities of technological innovation for the Military Police of Parana state in confrontation against violent crimes property with explosives

DOI:10.38152/bjtv5n1-003

Recebimento dos originais: 30/11/2021
Aceitação para publicação: 27/12/2021

Ilson de Oliveira Junior
Mestrando em Engenharia Biomédica pela Universidade Tecnológica Federal do Paraná (UTFPR), Bacharel em Segurança Pública pela Academia Policial Militar do Guatupê, Bacharel em Direito pelo Centro Universitário Curitiba (UNICURITIBA), Especialização em Segurança Pública pela Academia de Polícia Militar de Minas Gerais
Instituição: Polícia Militar do Paraná
Endereço: Av. Mal Floriano Peixoto, 1401, Rebouças, CEP: 80230-110 - Curitiba - PR
E-mail: ilson.oliveira.jr@gmail.com

Franck Cione Coelho dos Santos
Mestre em Políticas Públicas pela Universidade Estadual de Maringá (UEM), Bacharel em Segurança Pública pela Academia Policial Militar do Guatupê Bacharel em Direito pelo Centro Universitário de Maringá (UNICESUMAR), Especialização em Segurança Pública pela Academia de Polícia Militar de Minas Gerais
Instituição: Polícia Militar do Paraná - 3 º CRPM
Endereço: Av. Guedner, 1218. CEP: 87050-390 - Zona 08 - Maringá - PR
E-mail: cionefranck@gmail.com

RESUMO
Os crimes violentos contra o patrimônio com emprego de explosivos são uma realidade

https://ojs.brazilianjournals.com.br/ojs/index.php/BJT/article/view/45351

Análise de Malware e Ameaças Cibernéticas

Análise de Malware e Ameaças Cibernéticas

Inteligência artificial: a arma secreta contra ataques cibernéticos no Brasil.

Leandro Andreazzi Gonçalves
EXECUTIVO DE CYBER DEFENSE
Publicado em 16 de nov. de 2023

+ Siga

O Brasil é um dos países mais vulneráveis a ataques cibernéticos no mundo. Em 2022, o país foi alvo de mais de 100 bilhões de tentativas de ataques cibernéticos, segundo levantamento da Fortinet. Isso representa cerca de 30% dos casos registrados em toda a América Latina e Caribe.

Os ataques cibernéticos podem causar grandes danos às empresas brasileiras, incluindo perda de dados, interrupção das operações e até mesmo falência. Por isso, é fundamental que as empresas brasileiras se protejam contra essas ameaças.

Uma das tecnologias que pode ajudar as empresas brasileiras a se proteger contra ataques cibernéticos é a inteligência artificial (IA). A IA pode ser usada para automatizar tarefas de segurança cibernética, identificar ameaças emergentes e responder a incidentes com mais rapidez e eficiência.

A IA pode ser usada para proteger as empresas brasileiras contra ataques cibernéticos de várias maneiras, incluindo:

https://pt.linkedin.com/pulse/intelig%C3%AAncia-artificial-arma-secreta-contra-ataques-leandro-xsicf

Perspectivas futuras

Perspectivas futuras

A IA pode ajudar na investigação digital com a previsão sobre novas tecnologias e técnicas assim como desafios a serem superados no futuro

gscomputacaoforense.com.br

gilberto@sudre.com.br

@gilbertosudre

SEGURANÇA DA INFORMAÇÃO
COMPUTAÇÃO FORENSE