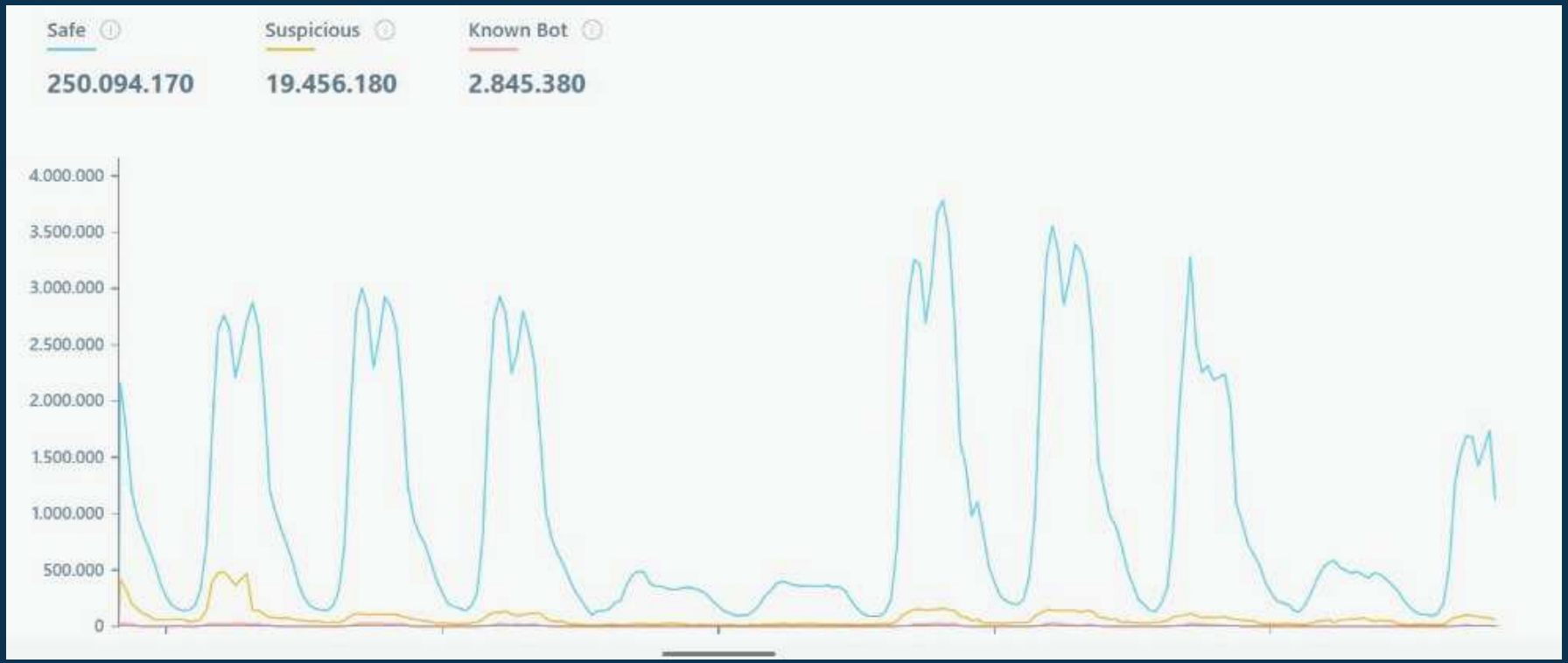

hCaptcha
Enterprise
A Biometria Comportamental e a Inteligência Artificial: Uma Aliança Contra Fraudes
Uma combinação poderosa para proteger os usuários e as organizações de tentativas de fraude online.
MAURO PICCININI
Sales Engineer


A ameaça da fraude online
Bots, ameaças de risco e automações maliciosas estão se tornando cada vez mais sofisticados


"O custo global da fraude online está estimado em US$ 48 bilhões em 2023" (Fonte: Juniper Research)
Um problema crescente que exige soluções eficazes.

Característica de um ataque de Ator Suspeito ou de Risco




Biometria
Comportamental

Como a biometria comportamental e a IA podem melhorar a experiência do usuário

Torna a autenticação mais rápida e fácil

Através de uma abordagem baseada em padrões de interação do usuário e análise de dados para identificar usuários legítimos e evitar que bots, ameaças de risco e automações maliciosas acessem sistemas e dados.

Uma maneira de identificar usuários legítimos com base em como eles interagem com sistemas e dispositivos.

Como essas tecnologias combinadas podem proteger os usuários e as organizações de tentativas de fraude online

Uma abordagem baseada em padrões de interação do usuário

Uma maneira de identificar usuários legítimos com base em como eles interagem com sistemas e dispositivos.

Desafio cognitivo

Uma forma de autenticação que requer que o usuário execute uma tarefa simples, como responder a uma pergunta de segurança ou completar um quebra-cabeça.

Como a biometria comportamental e a IA protegem a privacidade

Os dados de comportamento do usuário devem ser criptografados e armazenados com segurança.

Privacidade de Dados

Uma preocupação essencial ao usar tecnologias de autenticação.

Integração da Segurança da Informação, Área de Fraudes e Desenvolvimento de Sistemas / Aplicações

As equipes devem trabalhar em conjunto para garantia de mitigação de ações fraudulentas

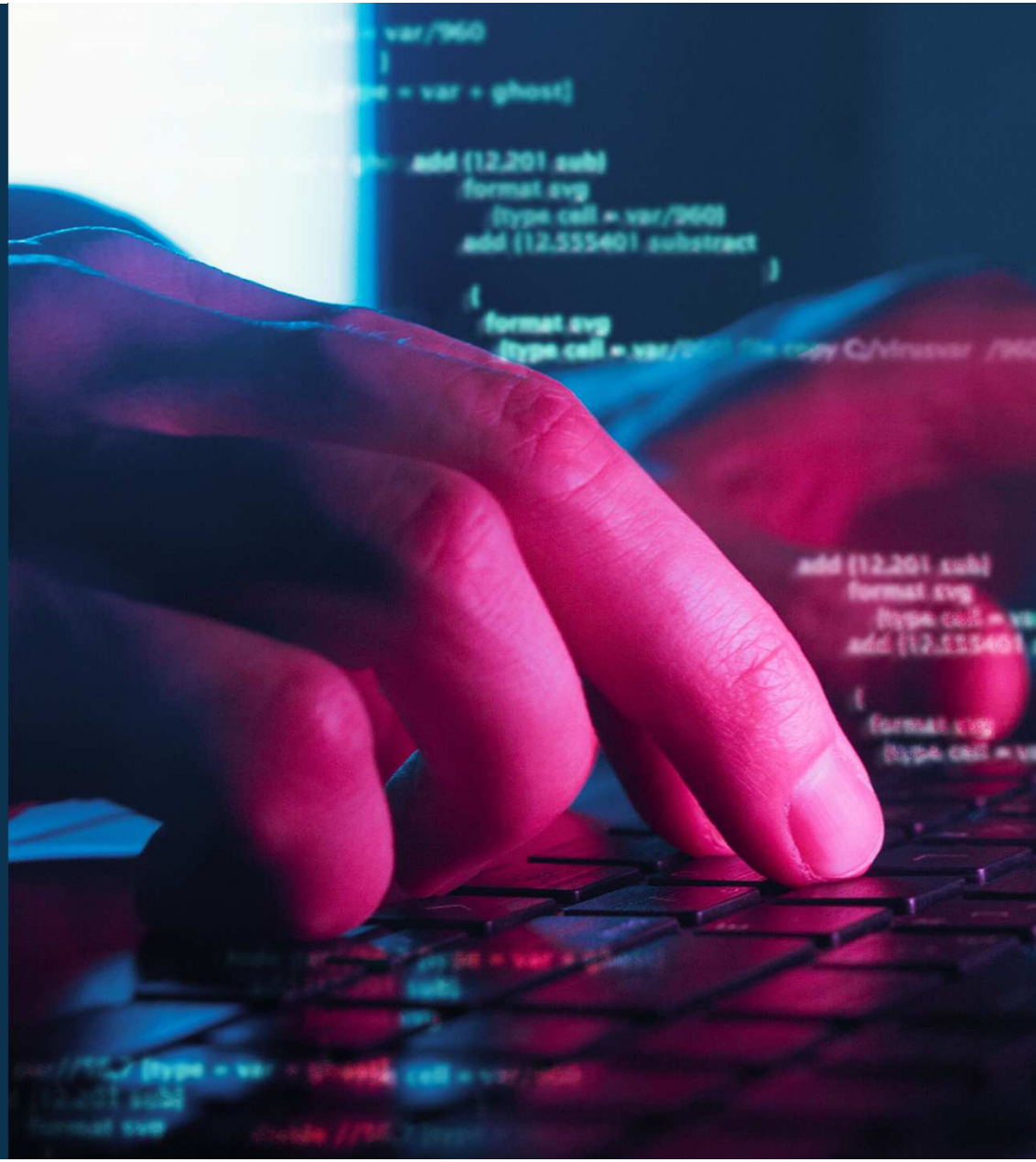
Integração com a segurança da informação

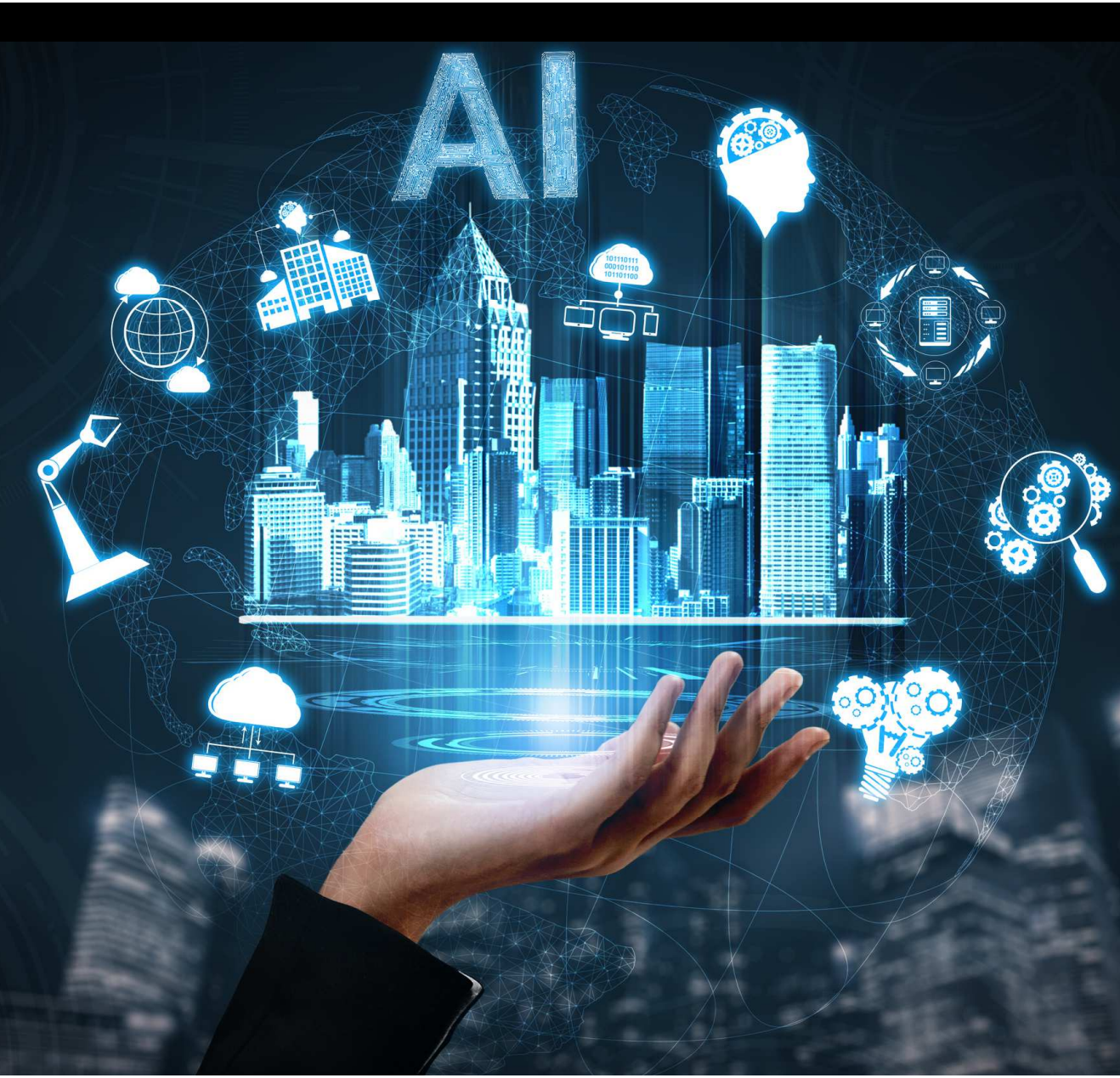
O uso da IA possibilita análises “After the Fact” para identificar assinaturas de atores suspeitos e de risco

O uso de ML possibilita que os modelos de IA sejam retroalimentados e que passam a ser preditivas em tempo real para evitar que um ator malicioso ou de risco, humano ou automação tenha acesso aos ativos sensíveis das aplicações

Integração com a área de Fraudes

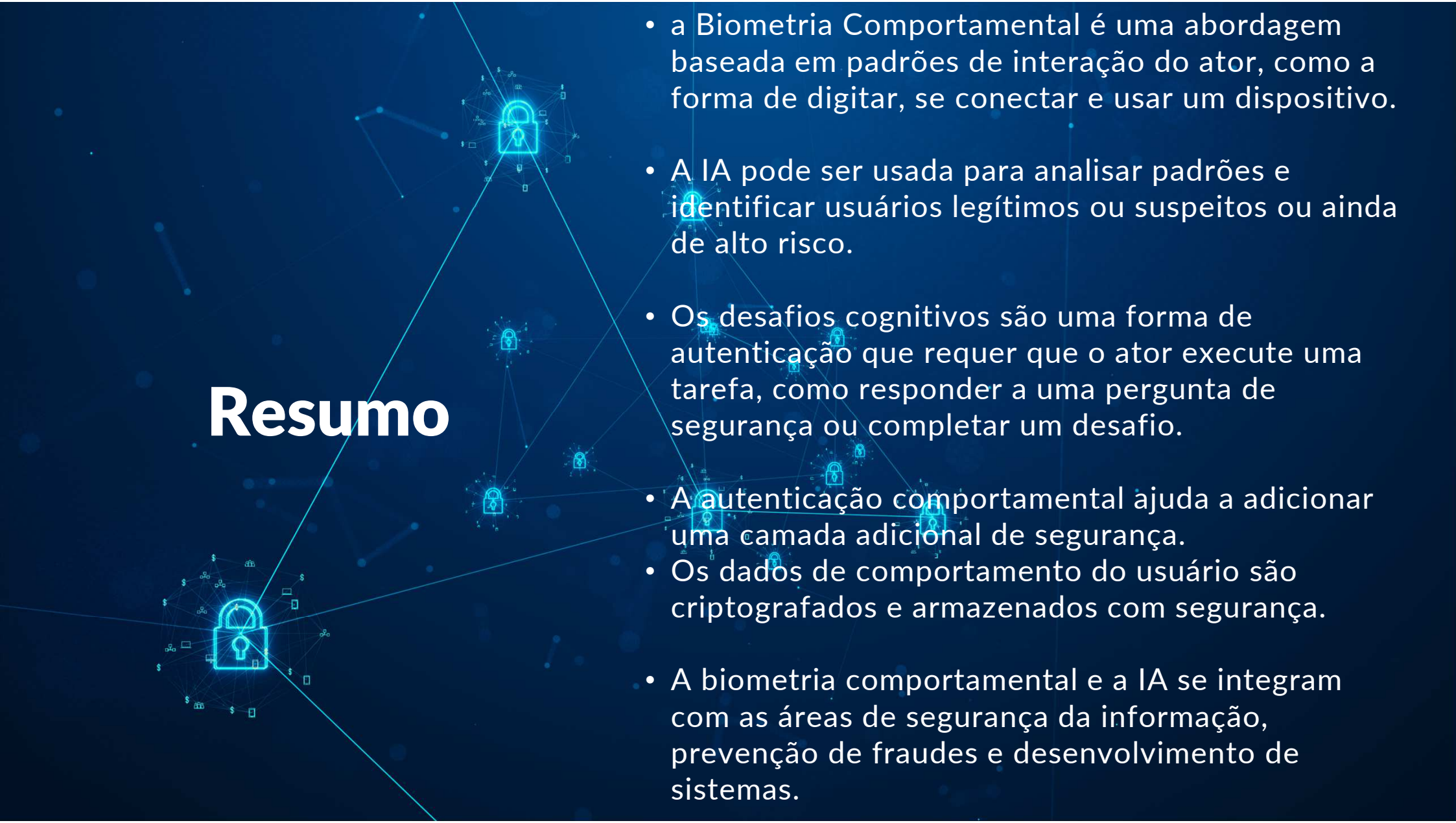
Qualificação de ações de fraude serão analisadas através dos modelos de IA e ML e com isto pode-se atribuir risco a partir das assinaturas existentes e as micro mudanças que aprimoram os ataques.
Os alertas de risco serão identificados e ações poderão ser colocadas em prática para sua mitigação.





Integração com o Desenvolvimento de Sistemas e Aplicações

Garante uma autenticação tomando como base score de risco de um ator em tempo de aplicação com avaliação em tempo real e garantindo que somente atores legítimos tenham acesso a APIs, acessem aplicações WEB ou em dispositivos móveis de forma eficiente e segura



Resumo

- a Biometria Comportamental é uma abordagem baseada em padrões de interação do ator, como a forma de digitar, se conectar e usar um dispositivo.
- A IA pode ser usada para analisar padrões e identificar usuários legítimos ou suspeitos ou ainda de alto risco.
- Os desafios cognitivos são uma forma de autenticação que requer que o ator execute uma tarefa, como responder a uma pergunta de segurança ou completar um desafio.
- A autenticação comportamental ajuda a adicionar uma camada adicional de segurança.
- Os dados de comportamento do usuário são criptografados e armazenados com segurança.
- A biometria comportamental e a IA se integram com as áreas de segurança da informação, prevenção de fraudes e desenvolvimento de sistemas.


Mauro Guglielmo Piccinini
SALES ENGINEER, INTUITION MACHINES - hCAPT...
+5511963055225
Obrigado