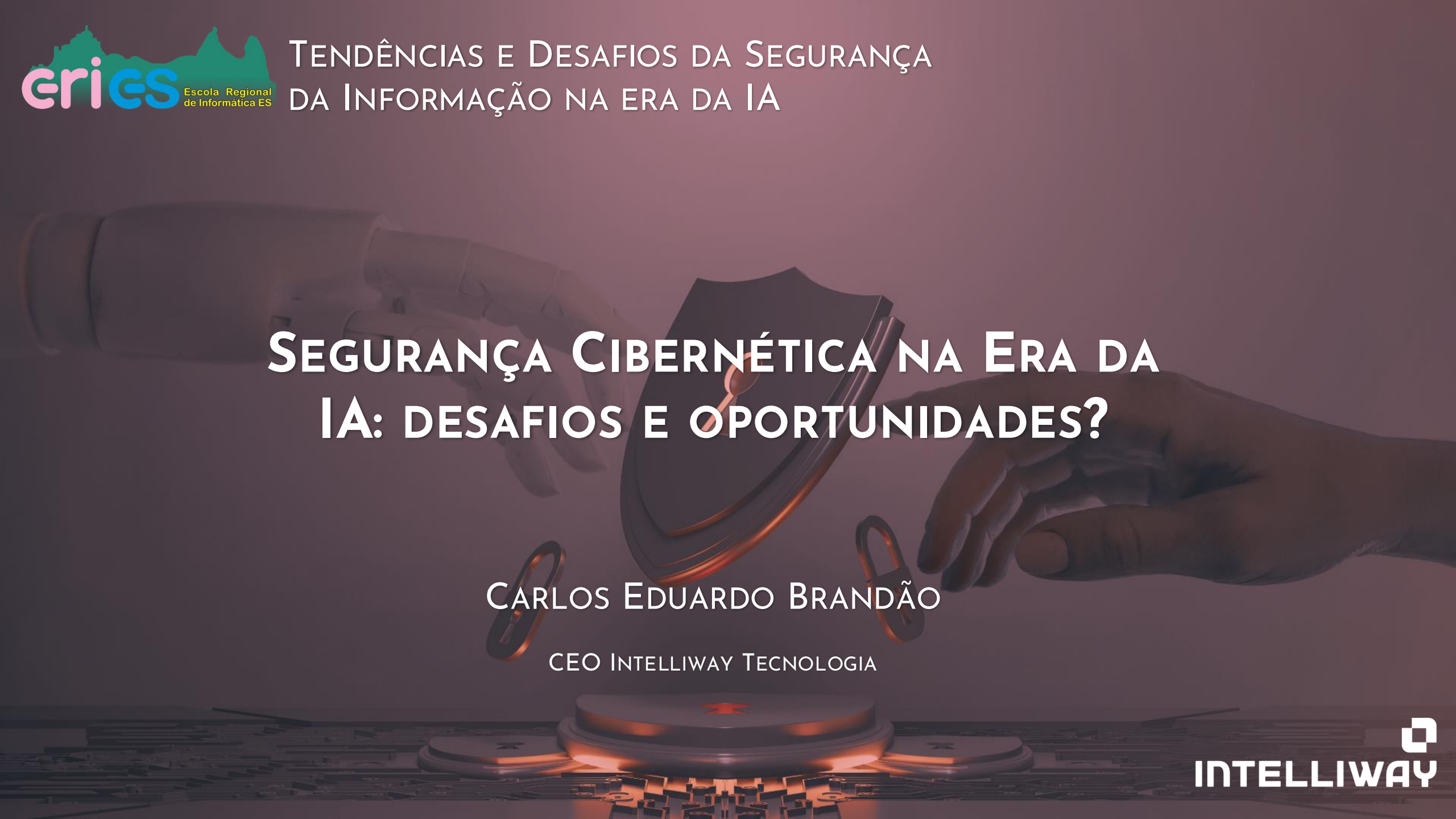


Segurança Cibernética na Era da IA: desafios e oportunidades?

Carlos Eduardo Brandão

CEO Intelliway Tecnologia

INTELLIWAY

Somos uma empresa especializada em **Inteligência Artificial** e **Cibersegurança** que integra tecnologias para construir um mundo mais seguro, inteligente e sustentável.

Integramos e desenvolvemos **soluções, serviços e produtos** estratégicos que **geram real valor** e **impulsionam o sucesso** dos seus negócios, preparando-o para o futuro.

Finep
INOVAÇÃO E PESQUISA

Nossa História

2017

- Intelliway é lançada
- Contratos nacionais e internacionais (CA) para empresas de porte
- Soluções precursoras em IA
- Referência em Segurança da Informação

2018

- Ampliamos nossas parcerias Tecnológicas em Cyber Security e IA
- Referência e Cases em IBM Watson
- Prêmio Projeto Destaque - Assistente Virtual Inteligente - Grupo Águia Branca;

2019

- Lançamos Serviços Gerenciados de Cyber Security e SOC
- Atuação em Minas Gerais
- Diversificação de Portfólio de Serviços
- Contratos nacionais e internacionais (UK)
- Atuação em GRC

2020

- Crescimento Superior a 100%
- Nova e ampla Sede
- Revista Forbes Tech: Case de IA aplicada ao Cidadão
- Prêmio Melhor Projeto e Gerente de Projeto PMI/ES
- Atuação em São Paulo

2021

- Crescimento Superior a 100%
- Case ForbesTech
- CIOReview: 20 empresas mais promissoras Latam
- Prêmio IT4CIO - Inovação no Setor Público
- Lançamento do SOC Intelliway

2022

- Crescimento Superior a 80%
- Atuação como CSIRT e SOC em Cyber Ataques Nacionais
- Premiações HDI em IA
- Ampliação da Sede
- Certificação ISO 9001
- Ampliação do SOC & MDR

2023

- Lançamentos EvaGPT & EvaDocs
- Vencedor da Concorrência FINEP em Inovação e IA: 2ª. rodada
- Atuação nos Setores de Energia, Óleo e Gás
- CIOReview: 20 empresas mais promissoras Latam

2024

- Lançamento EvaSpeech
- Cybersecurity for OT
- Fornecedor Referência 2024 (ArcelorMittal)
- Vencedor da Concorrência FINEP em Inovação e IA: 2ª. rodada
- Convênio de Pesquisa e Inovação: IFES-FACTO

INTELLIWAY

Clientes e Parceiros que **conhecem a diferença**

Clientes

ArcelorMittal, VALE, edp, Grupo Águia Branca, SICOOB, OPTEhub

Faculdade Multivix – Multiplicando Conhecimento, WINE, Lhoist, timenow, CMR Surgical, CRC Grupo Almaviva

Assembleia Legislativa Espírito Santo, Justiça Federal – Tribunal Regional Federal da 3ª Região, Justiça do Trabalho – TRT da 17ª Região (ES), Trustly, E-INVEST By PREVIERICSSON, VOCALCOM

FUCAPE Business School, Unimed, PORTOCEL, VERACEL, METRÔ, SunCoke Energy

Parceiros

CHECK POINT, Extreme networks, RAPID7, aruba, Cymulate, proofpoint.

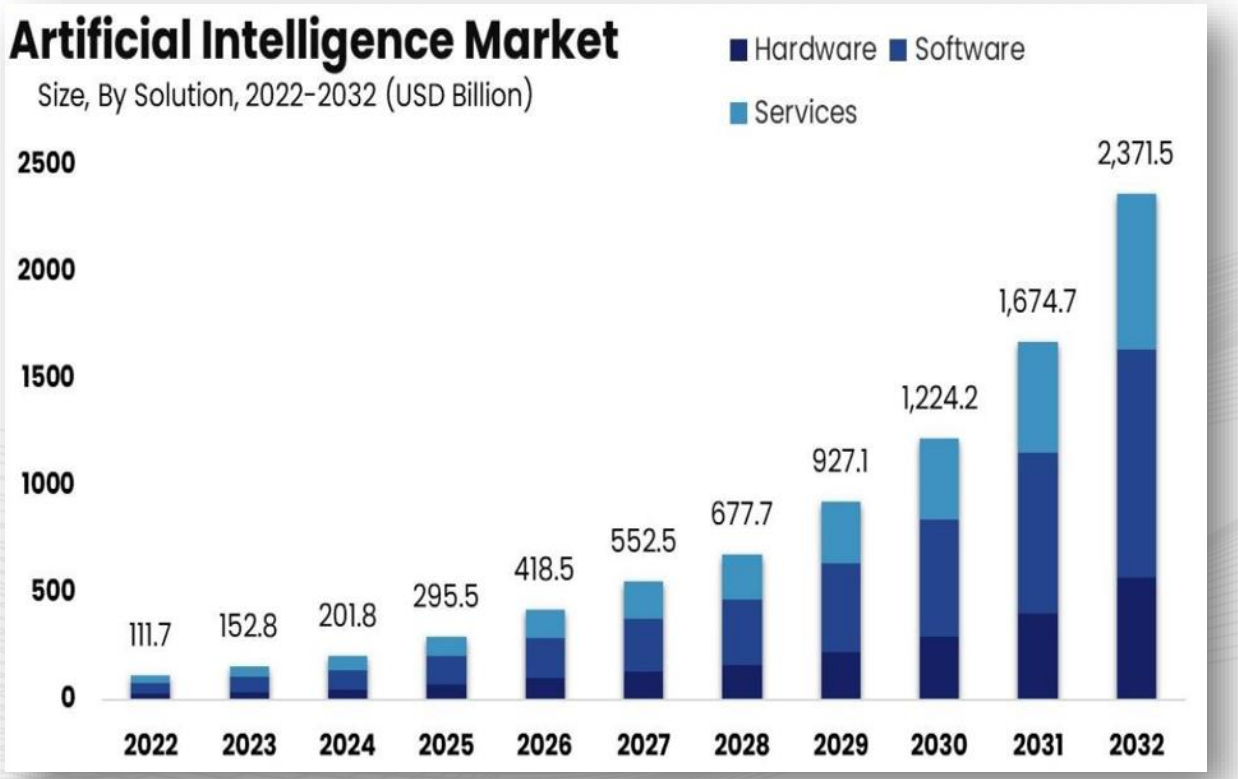
VERACODE, Infoblox, Hillstone Networks, ARMIS, Delinea, CLAROTY

mongoDB., VONAGE, IBM, NVIDIA, OneTrust – Privacy, Security & Governance, vicarius

Acronis, Google Partner, aws partner network, Microsoft, vmware, CloudSEK

INTELLIWAY

Artificial Intelligence & Cybersecurity



https://marketresearch.biz/report/artificial-intelligence-market/

"Artificial Intelligence Market size is expected to be worth around USD 2,371.5 Bn by 2032 from USD 111.7 Bn in 2022, growing at a CAGR of 36.8%.

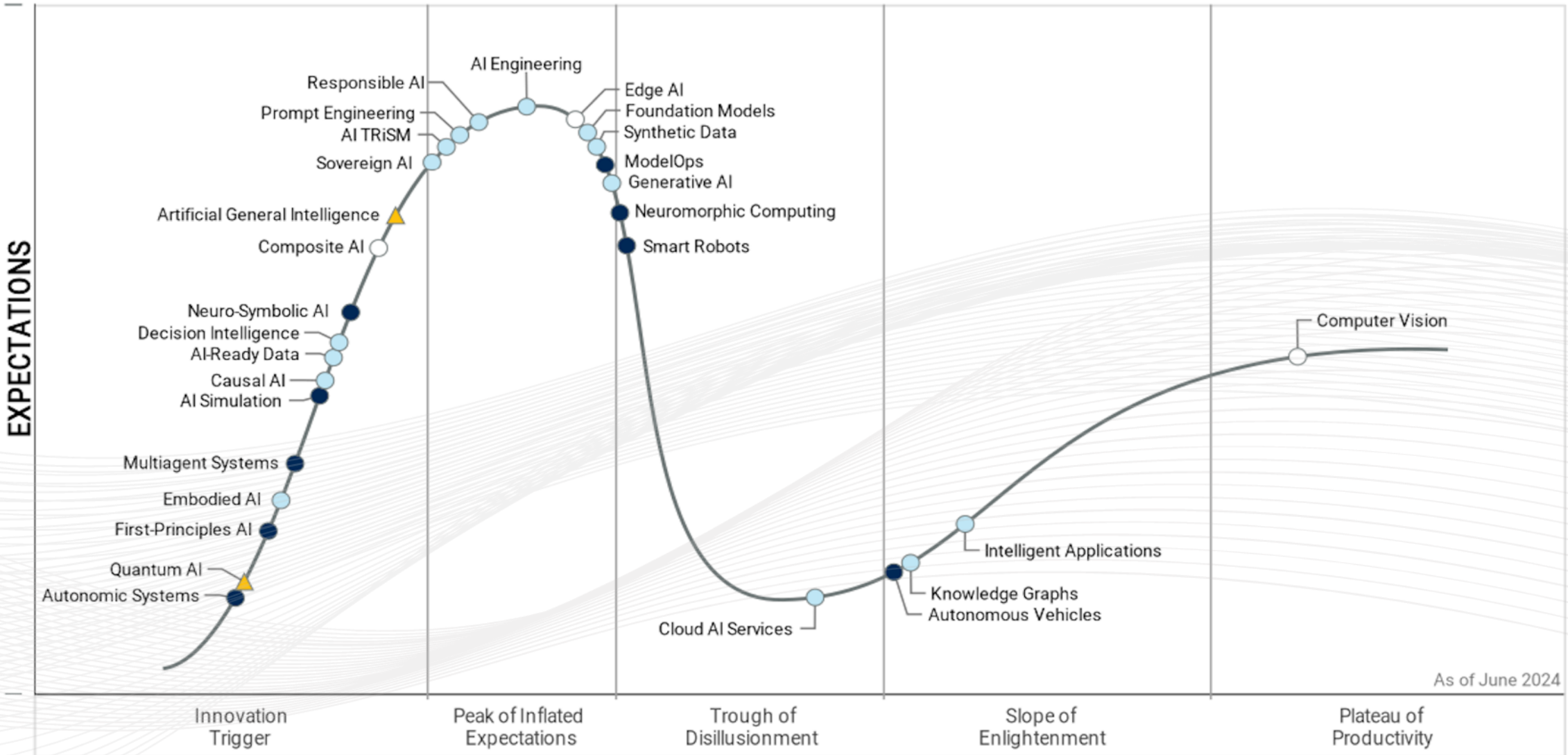
Driving Factors of the Artificial Intelligence Market

1. **Advanced Data Analytics**
2. **Automation**
3. **Personalized Customer Experience**
4. **Healthcare Innovation**
5. **Autonomous Vehicles**

Restraining Factors of the Artificial Intelligence Market

1. **Data Privacy and Security Concerns**
2. **Ethical and Bias Concerns**
3. **Talent Shortage**

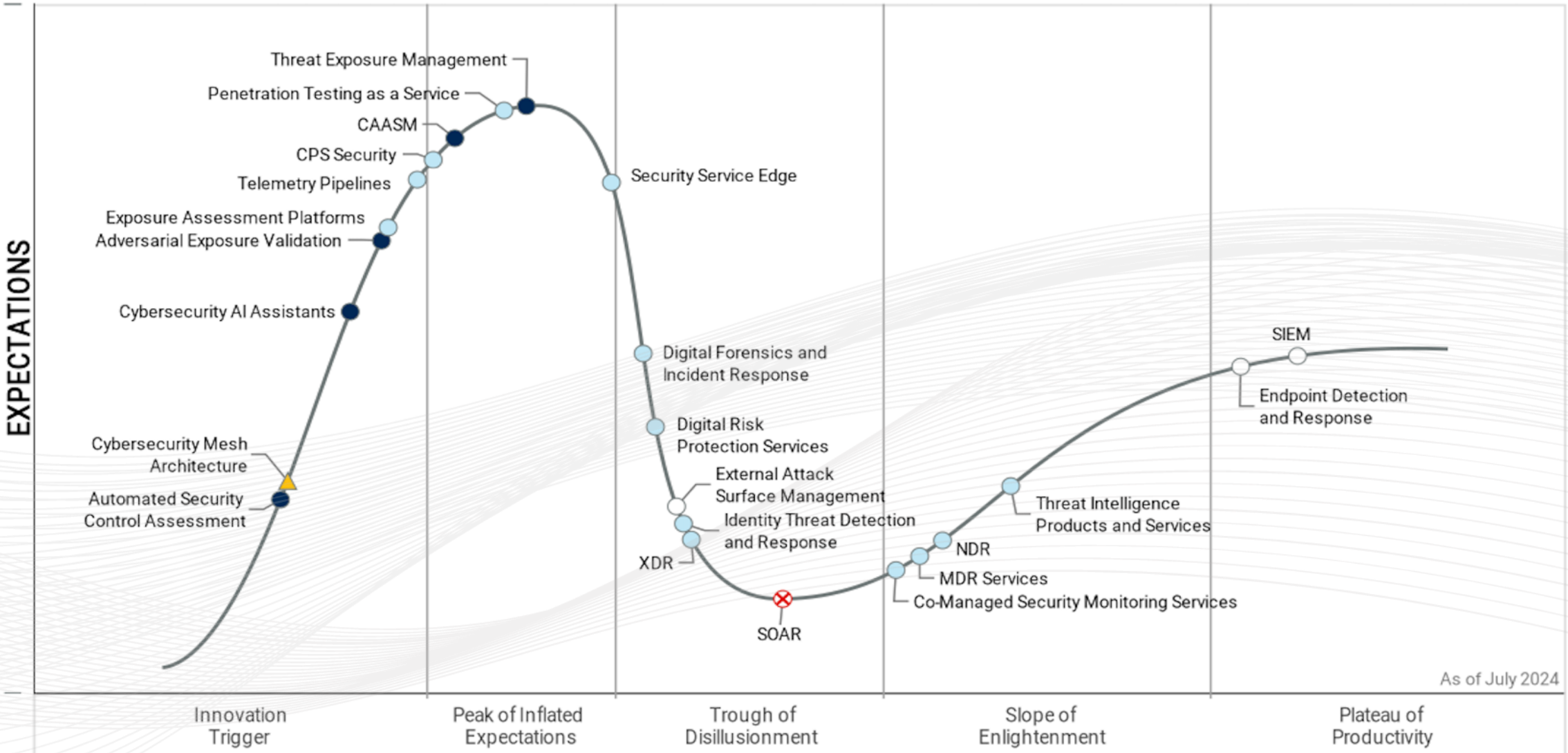
Hype Cycle for Artificial Intelligence, 2024



Gartner

INTELLIWAY

Hype Cycle for Security Operations, 2024

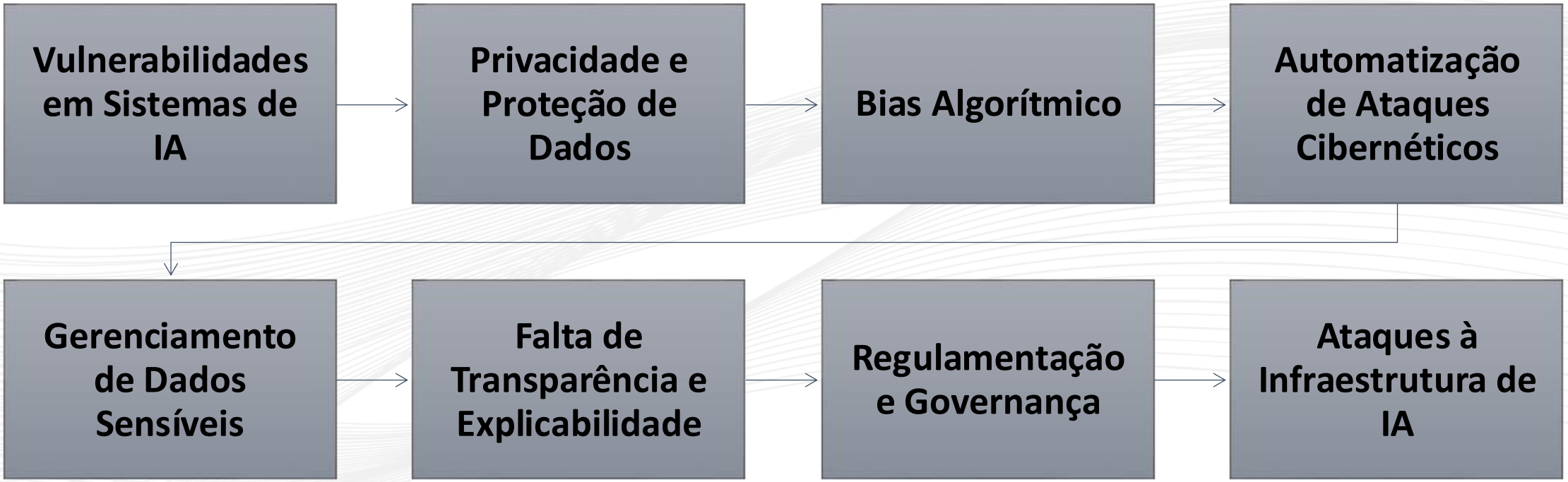


Plateau will be reached: ○ <2 yrs. ● 2–5 yrs. ● 5–10 yrs. ▲ >10 yrs. ⊗ Obsolete before plateau

Gartner

INTELLIWAY

DESAFIOS de Cybersecurity na era da IA



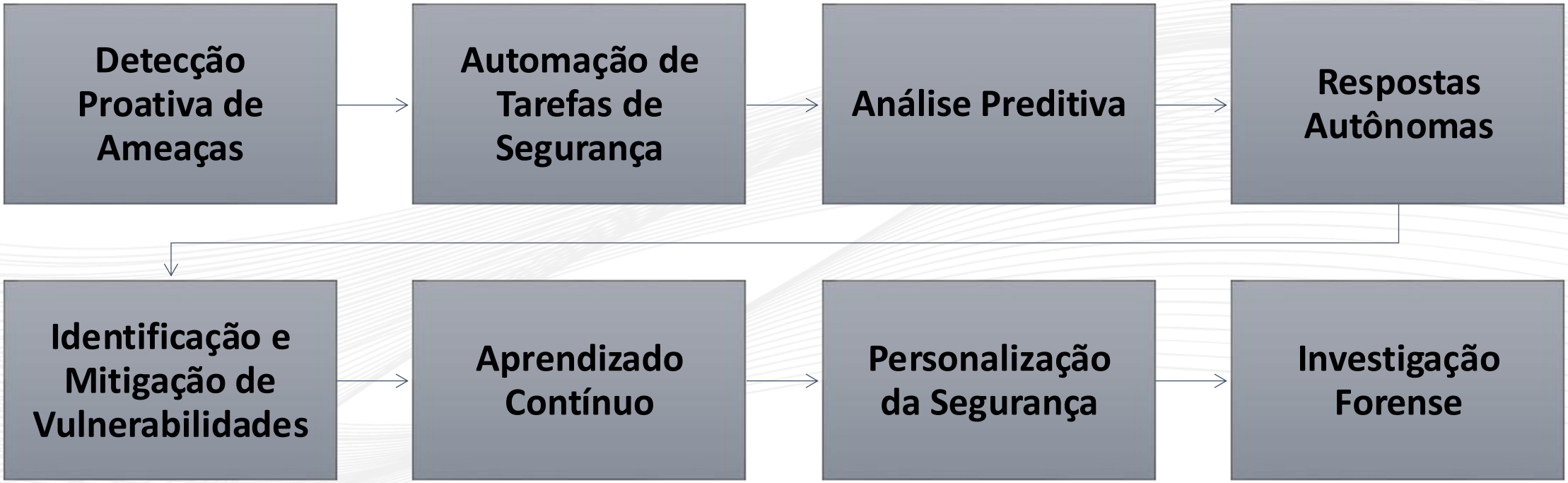
INTELLIWAY

CATEGORIAS DE ATAQUES a Segurança de Sistemas de IA

Adversarial Attacks	Data Poisoning	Model Inversion	Model Stealing
• Manipulação de entradas para enganar o modelo, fazendo-o gerar saídas incorretas.	• Inserção de dados maliciosos no treinamento do modelo para comprometer seus resultados.	• Reversão dos resultados de IA para descobrir dados sensíveis.	• Cópia do modelo de IA por meio de consultas repetidas para replicar ou explorar a tecnologia.
Evasion Attacks	**Trojan Attacks**	**Membership Inference**	**Exploraração de Falhas de Algoritmos**
• Modificação de entradas para evitar a detecção por sistemas de IA.	• Inserção de código malicioso no modelo, ativado por gatilhos específicos.	• Determinação de se dados específicos faziam parte do treinamento do modelo.	• Identificação de pontos falhos dos modelos e camadas de algoritmos de IA.

INTELLIWAY

OPORTUNIDADES de Cybersecurity na era da IA



INTELLIWAY

Autonomic Security Operations

Autonomic system refers to computing system that automatically manages itself(Sitaram D. and Manjunath G., 2012).

Autonomous system, on the other hand, is defined as system that can deal with the non-programmed or non-present situation and has the ability of particular self-management and self-guidance (Chen et. al., 2021).

4 Areas of Autonomic Computing

- Self-optimization
- Self-configuration
- Self-healing
- Self-Protection

AI / ML Autonomous Cyber Security (ACS): It functions autonomou much like the human immune system, providing continuous protection without requiring constant user intervention. This is beneficial as it reduc the burden on users and IT staff to manually detect and respond to threa

Constant Monitoring and Analysis: ACS continuously monitors and analyzes activities within the network or system. This proactive approac helps in early detection of anomalous behaviors that could indicate potential cyber threats.

Mitigation of Unknown Threats: It addresses both known and unkno threats, including zero-day attacks. This capability is crucial in today's evolving threat landscape where new vulnerabilities and attack methods constantly emerge.

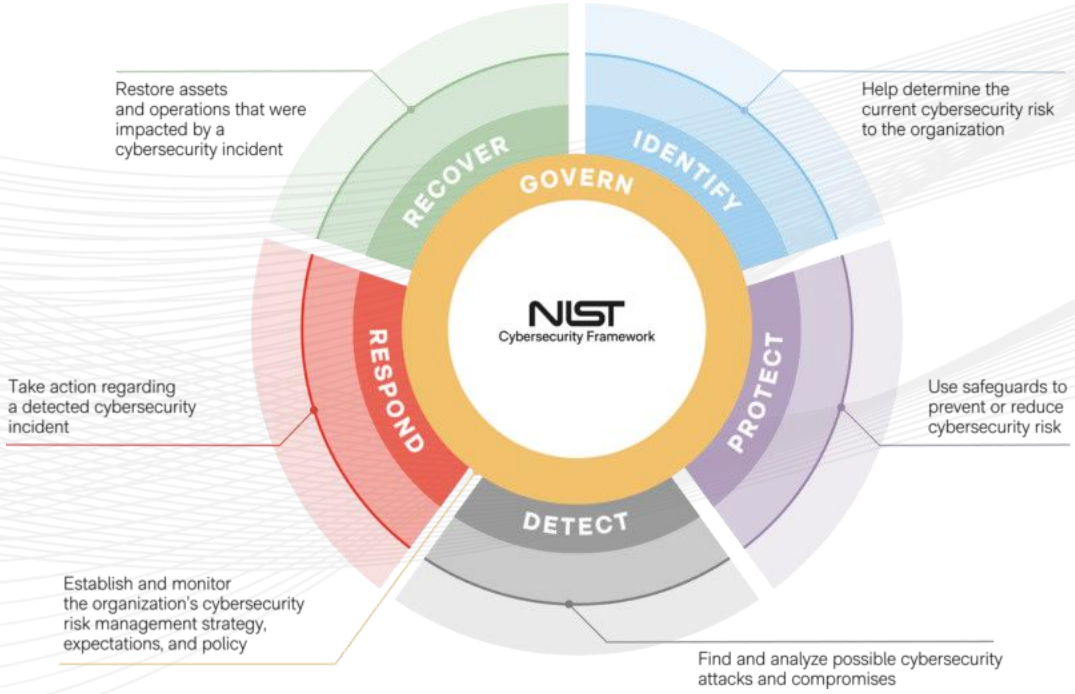
Versatility in Threat Handling: ACS responds to threats regardless of their origin (insider or outsider) or nature (natural or malicious). This versatility ensures comprehensive protection against a wide range of cyb threats.

Independence from User Involvement: Its ability to operate independently from user actions means that it can function effectively ev in scenarios where users may not be actively engaged or aware of poten threats.

Advanced AI/ML: ACS aims to provide robust, automated, and efficien protection against cyber threats, enhancing overall security posture whil minimizing the need for continuous human oversight and intervention.

INTELLIWAY

Autonomic Security Operations



AI / ML Autonomous Cyber Security (ACS): It functions autonomou much like the human immune system, providing continuous protection without requiring constant user intervention. This is beneficial as it reduc the burden on users and IT staff to manually detect and respond to threa

Constant Monitoring and Analysis: ACS continuously monitors and analyzes activities within the network or system. This proactive approac helps in early detection of anomalous behaviors that could indicate potential cyber threats.

Mitigation of Unknown Threats: It addresses both known and unkno threats, including zero-day attacks. This capability is crucial in today's evolving threat landscape where new vulnerabilities and attack methods constantly emerge.

Versatility in Threat Handling: ACS responds to threats regardless of their origin (insider or outsider) or nature (natural or malicious). This versatility ensures comprehensive protection against a wide range of cyb threats.

Independence from User Involvement: Its ability to operate independently from user actions means that it can function effectively ev in scenarios where users may not be actively engaged or aware of poten threats.

Advanced AI/ML: ACS aims to provide robust, automated, and efficien protection against cyber threats, enhancing overall security posture whil minimizing the need for continuous human oversight and intervention.

Fale Conosco

Acesse o QRCODE

ou https://www.intelliway.com.br/contato

https://www.instagram.com
/intelliway/

https://www.linkedin.com/company
/intelliway-ti-inteligente

Rua Roberto da Silva, 20, Sala 310,
Vitória-ES - CEP 29066-091