

2022 CIBERSEGURIDAD PRESENTE & FUTURO

ASIP Cybersecurity
Services





1. 100 Cybersecurity Experts
 2. Presence in **Europe, Latin America** and **Middle East**
 3. Global Cybersecurity for Multinational & Government
 4. **+500** GLOBAL Customers
 5. **+30%** Annual Growth
 6. International Recognized Certifications by Gartner
 7. Global Operations Facilities in 5 countries
-

01 | AIUKEN CORPORATE INTRO VIDEO



01 Our mission

Aiuken's mission is to continue developing its innovation, technologies, services and Security infrastructures to achieve the best level of security and secure access to the cloud, Internet and Systems Worldwide



Aiuken, is an international Cybersecurity Leader company focused on Information, Communications and Internet Security, specialized in Cloud Security services with high added value for Governments and Big Enterprises.

Our vision

Managed Cloud Security and Protection services for large companies, SMEs and Public Administration, and securing the digital transformation of our clients.

We provide the technologies, services and infrastructures that facilitates security and secure access to the CLOUD, Internet and Telecommunications Systems.

Objective

Best Security levels, Quality, Security as a Service

01 | Cybersecurity Today

New Digital Era. Everybody Welcome



New Digital Era. Everybody Welcome



New Digital Era. Everybody Welcome

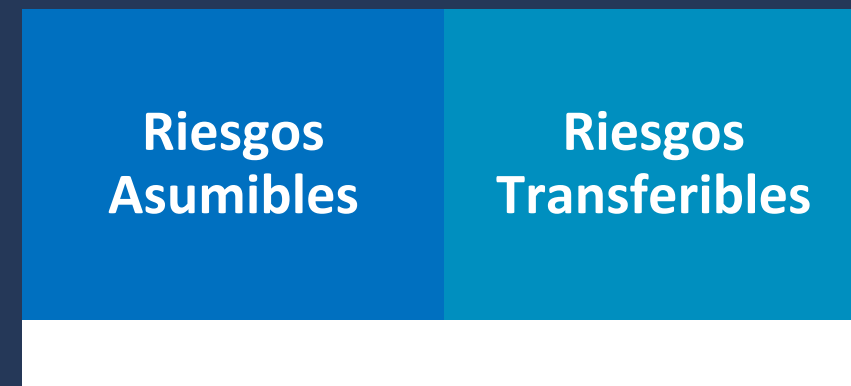


New Digital Era. Everybody Welcome



02 | CyberSecurity & Digital Transformation

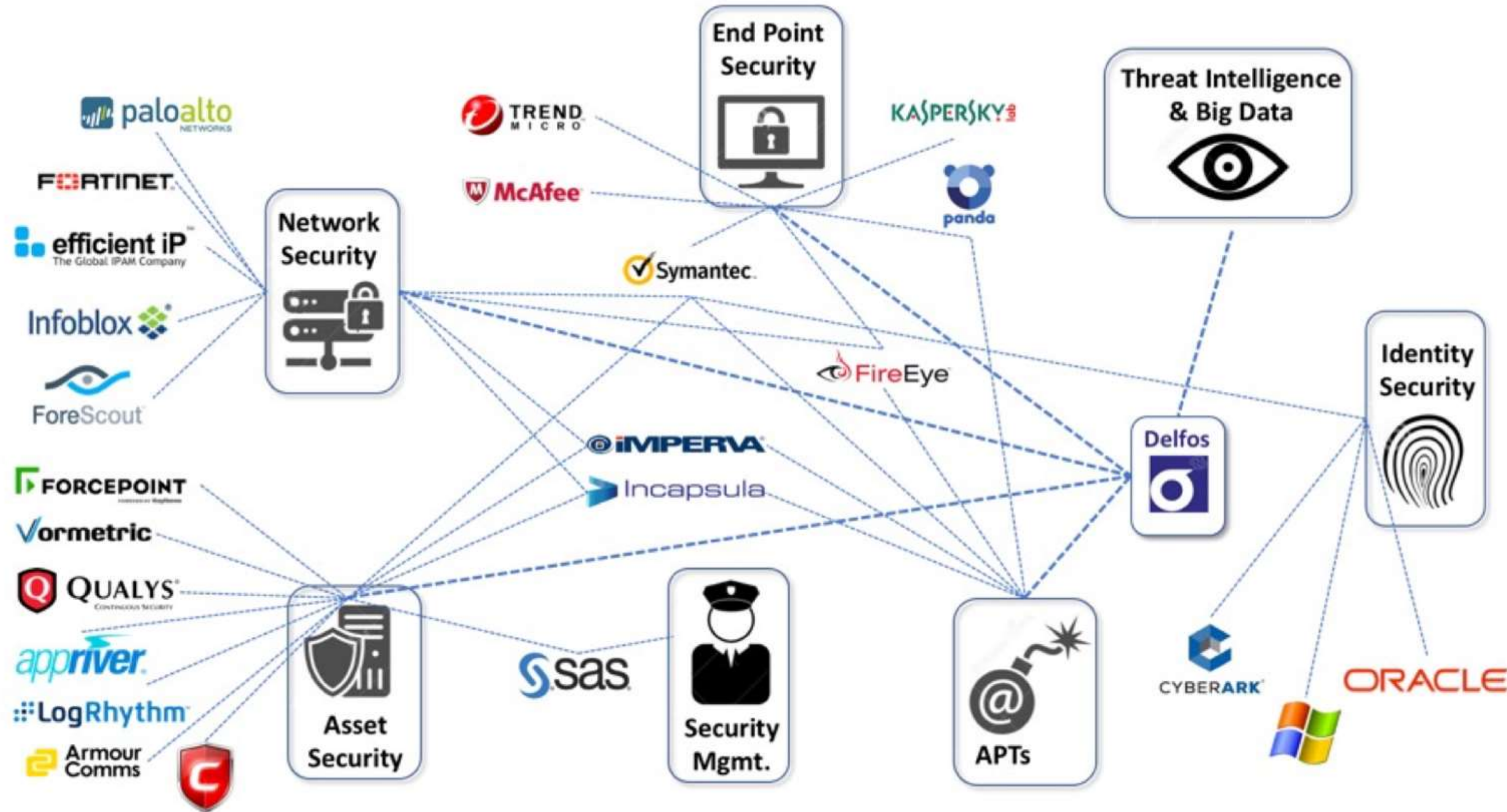
Digital Transformation Riesgo Exponencial



Imposible control humano

01 | Cybersecurity Now and Future Issues

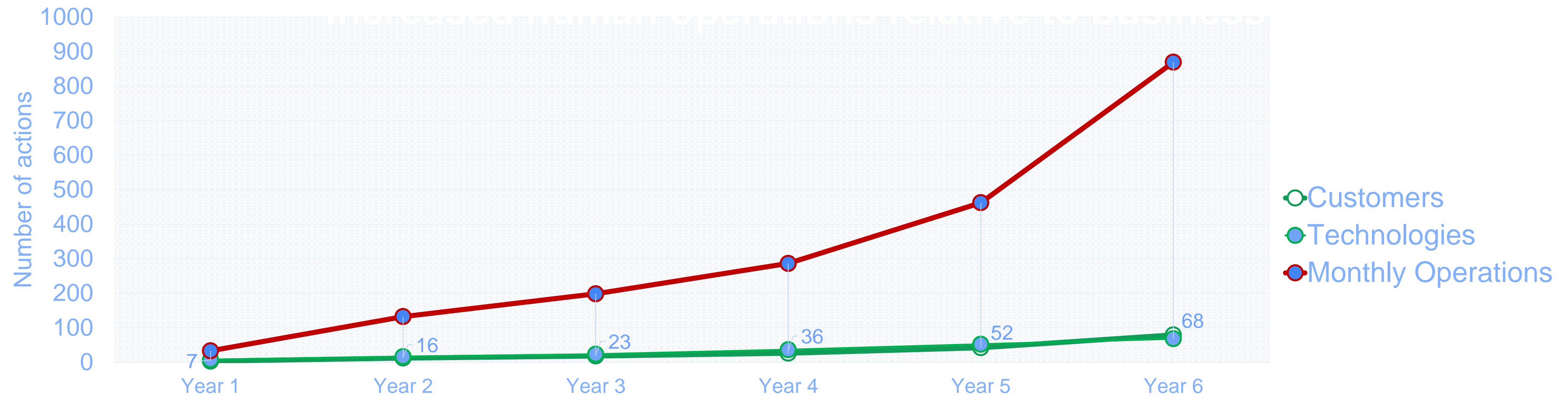
Complex scenarios. Not scalable operations.



Lot of technologies
Multiple dashboards
Multiple alerts consoles
Multiple ticketing systems
Multiple reporting systems

More expensive resources
More specific vendor specialists
Information disaggregation
Inefficient reporting management

Increased human operations relative to business growth



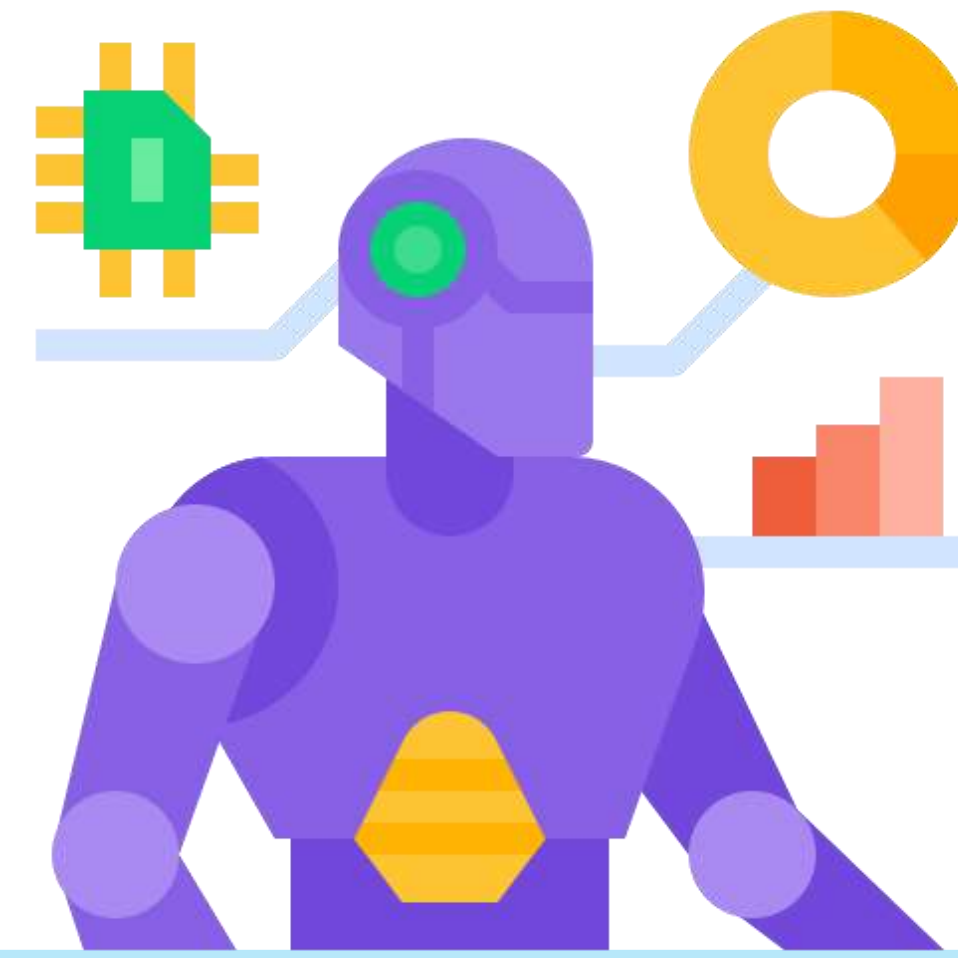
Human Operations

- Alerts management
- Incidents management
- Tickets scalation
- Reports elaboration
- Investigations
- Devices integrations
- Use cases implementation
- Dashboards elaboration



H U M A N S

- Slow on alerts triage
- Slow on scoring calculation
- A single task at same time
- Work at 8 hours shifts
- Failures under pressure
- Limited and expensive
- Need to sleep and eat



R O B O T S

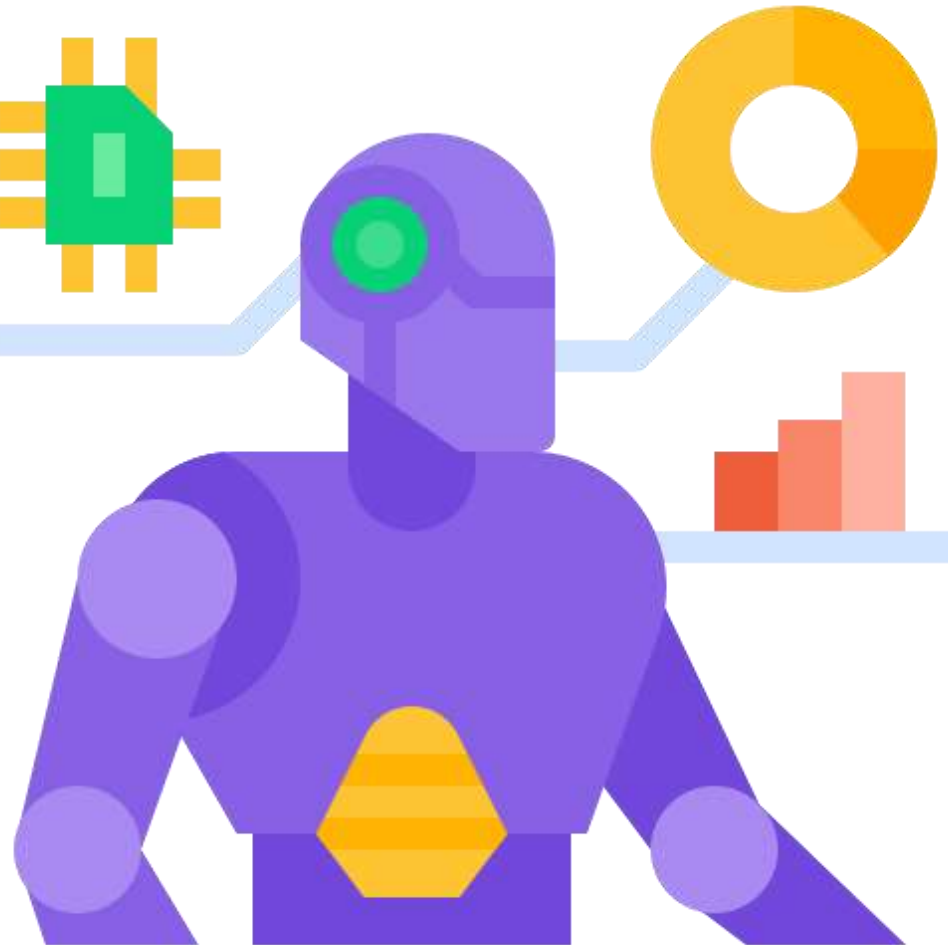
- Alerts triage at machine speed
- Scoring calculation at machine speed
- Thousands of tasks at same time
- Work 24 x 7 x 365
- Always just as accurate
- Unlimited and cheap
- Don't sleep and don't eat

We need to exclude humans from Cybersecurity Operations



H U M A N S

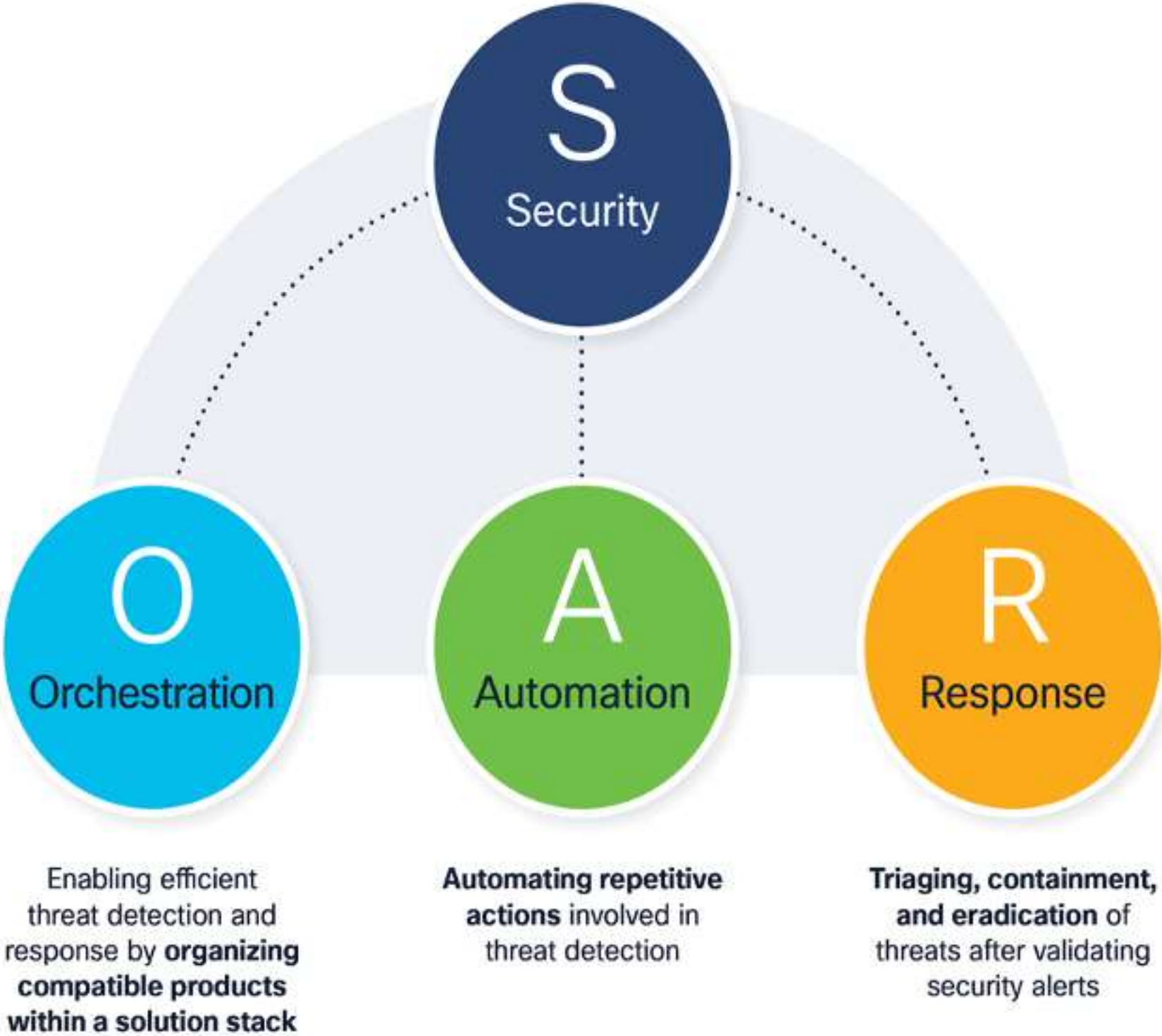
R O B O T S



03 | Inteligencia Artificial El Futuro



Gartner



1
7

Aiuken Cloud SOC / MDR Services

Gartner positions us as an MDR service provider in its global market guide.

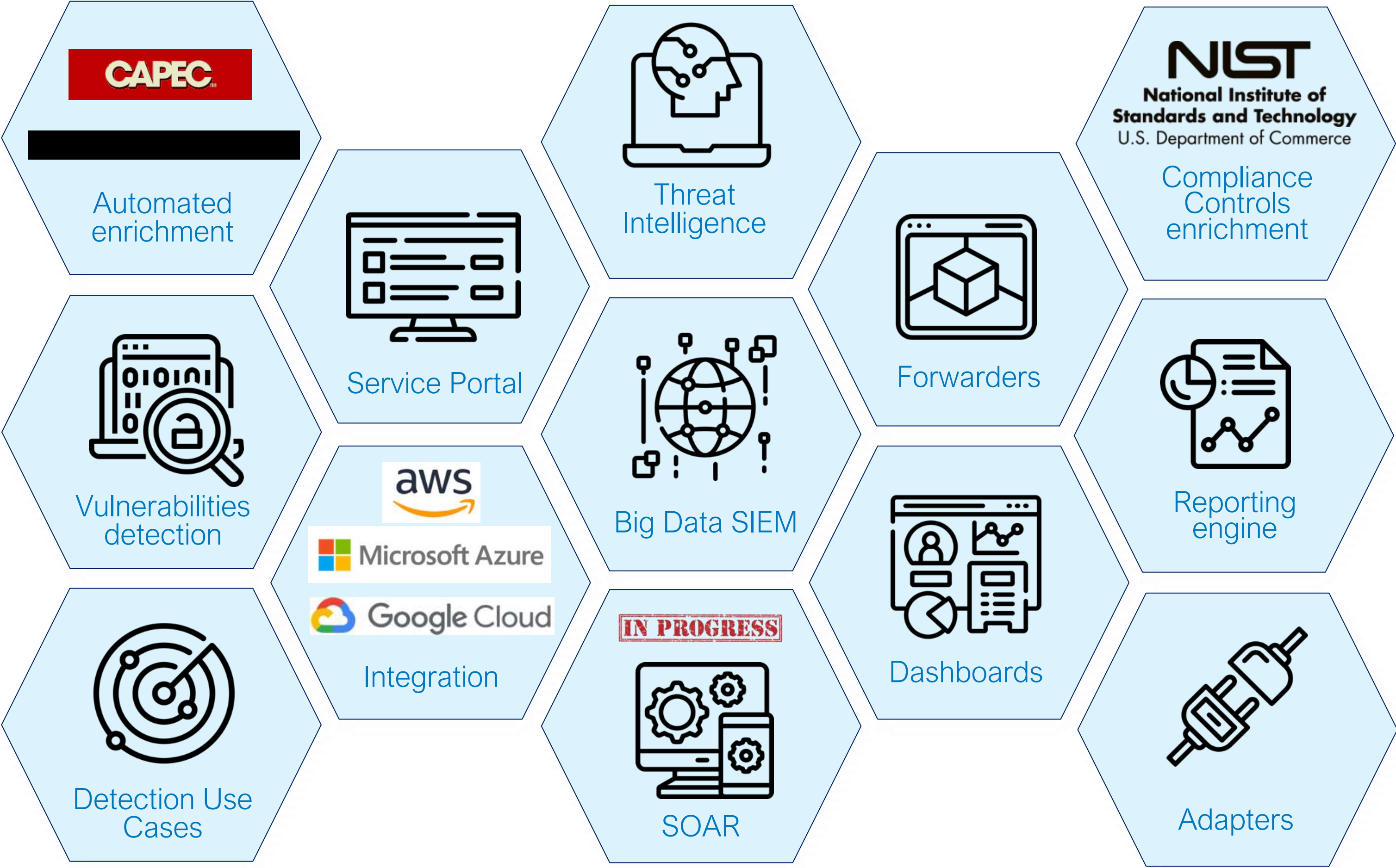
A diagram showing a continuous cycle of three stages: DETECT (with a shield icon), RESPOND (with a target icon), and MANAGE (with a group of people icon). The stages are connected by arrows in a circular flow, with a central white circle.

The Aiuken Cybersecurity logo and the Gartner logo are displayed side-by-side at the bottom of the slide.



Managed Detection
and Response (MDR)

03 | AIUKEN AI + SOAR PLATFORM = ASIP

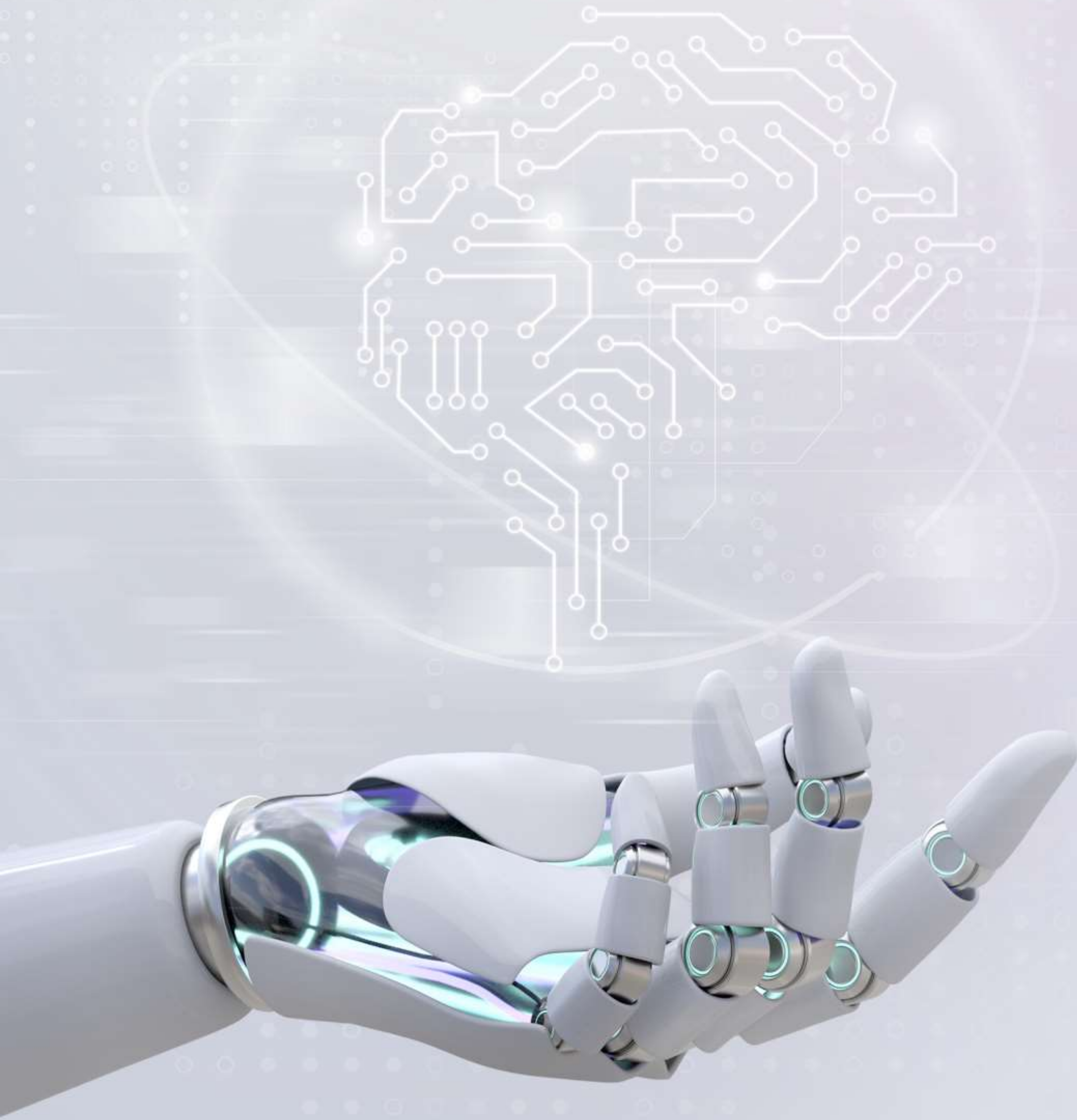


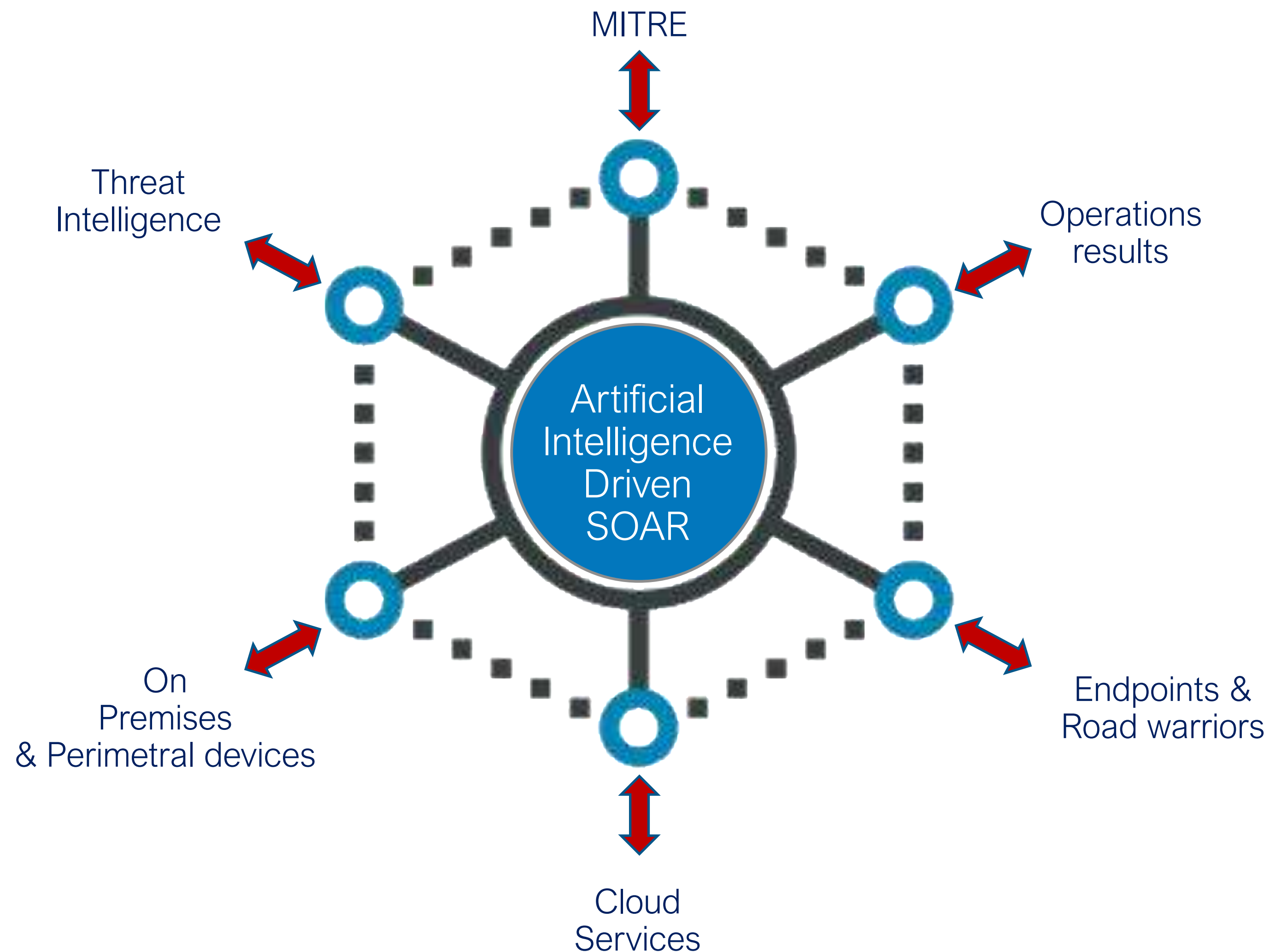
Autonomous Security Operations Center

Automatic Detection
Automatic Triage
Automatic Mitigation

Automatic provision
Automatic operations
Scalable business

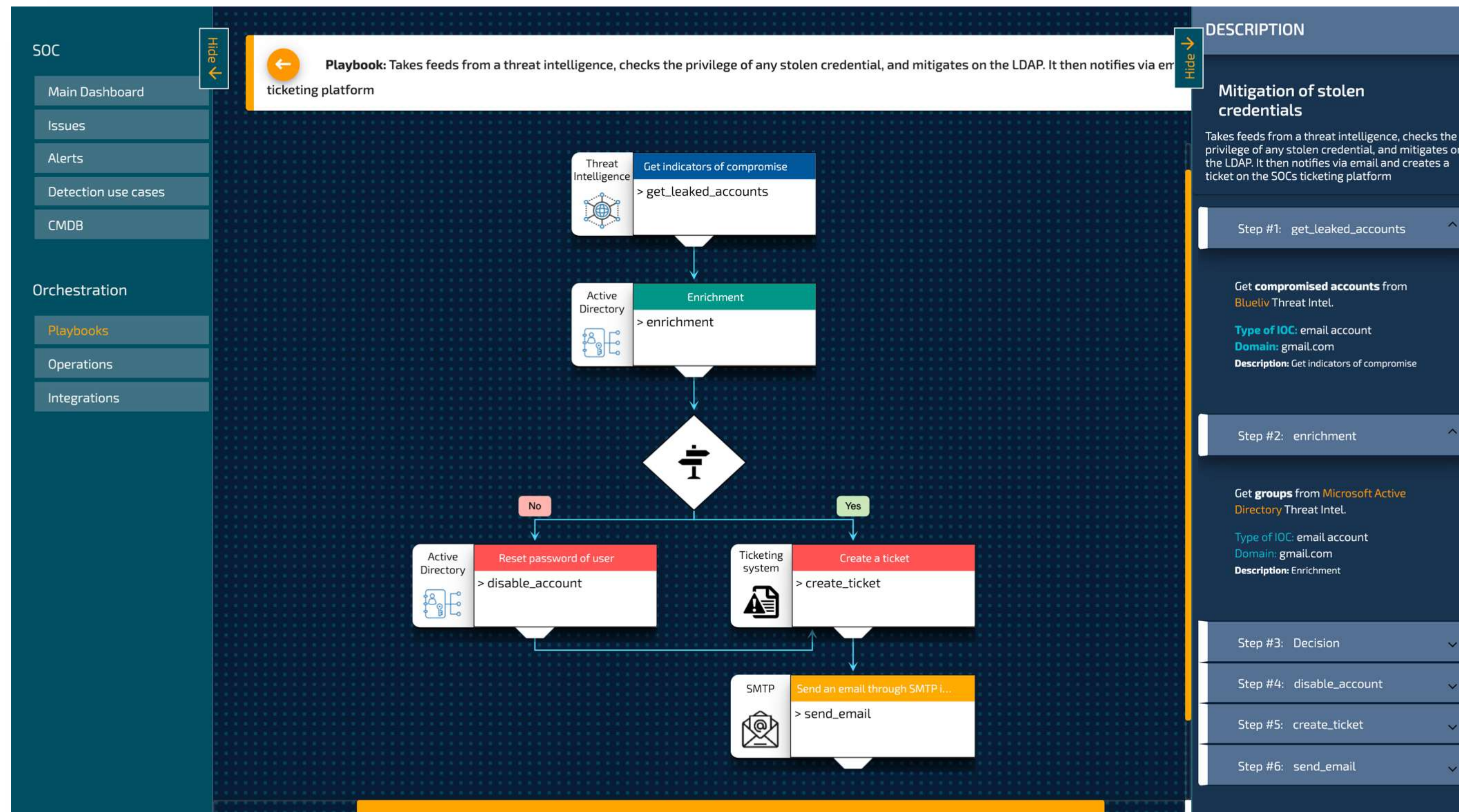
No human intervention required
Fully automatic, Artificial Intelligence
Driven, from The Cloud





- Multi-Customer autonomous SOC
- Driven by Artificial Intelligence. Feed by cloud Data Lake currently in production
- Unattended Triage within MITRE framework
- Unattended Mitigation in endpoints and cloud services
- Unattended resolution & ticket scalation to customers

04 | SOAR (Auto-Mitigation)



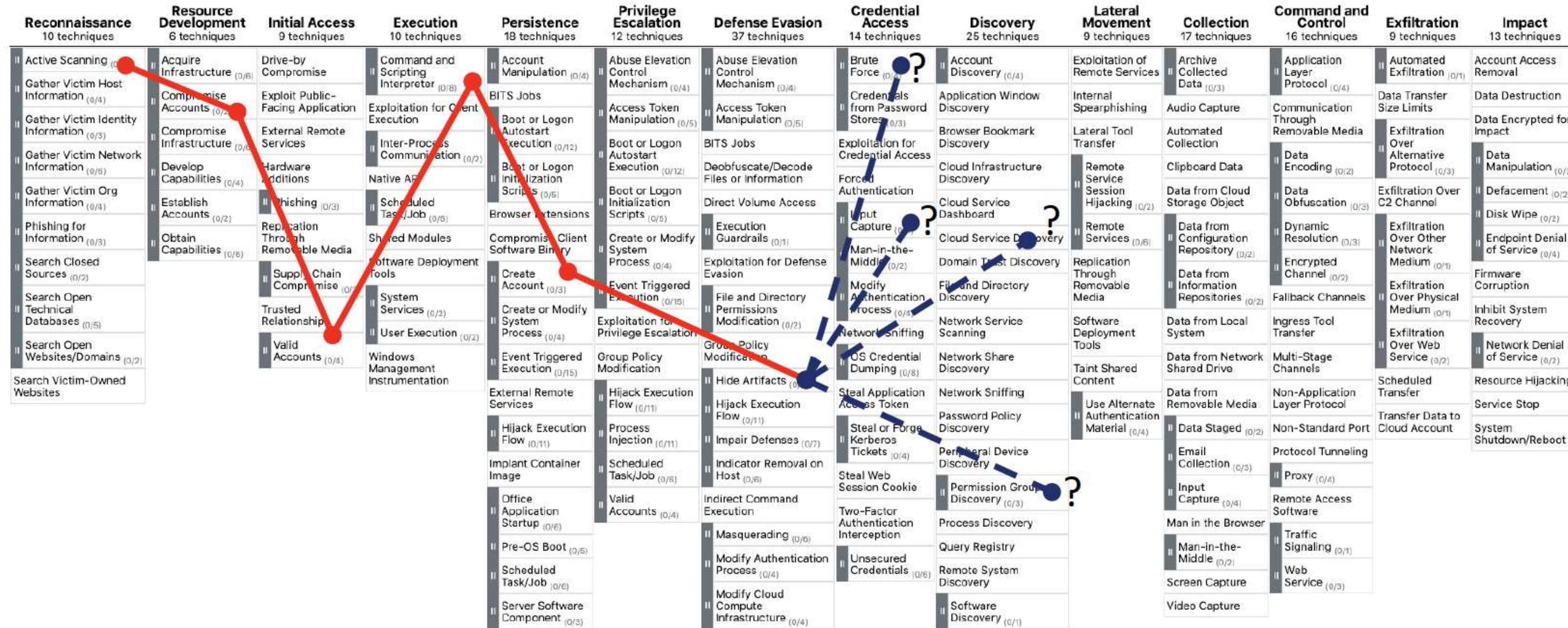
- Multi-customer playbooks: pipelines abstracted from vendors and devices
- One single playbook per use case for all SOC customers
- Easy SOC playbook maintenance: scalable operations



04

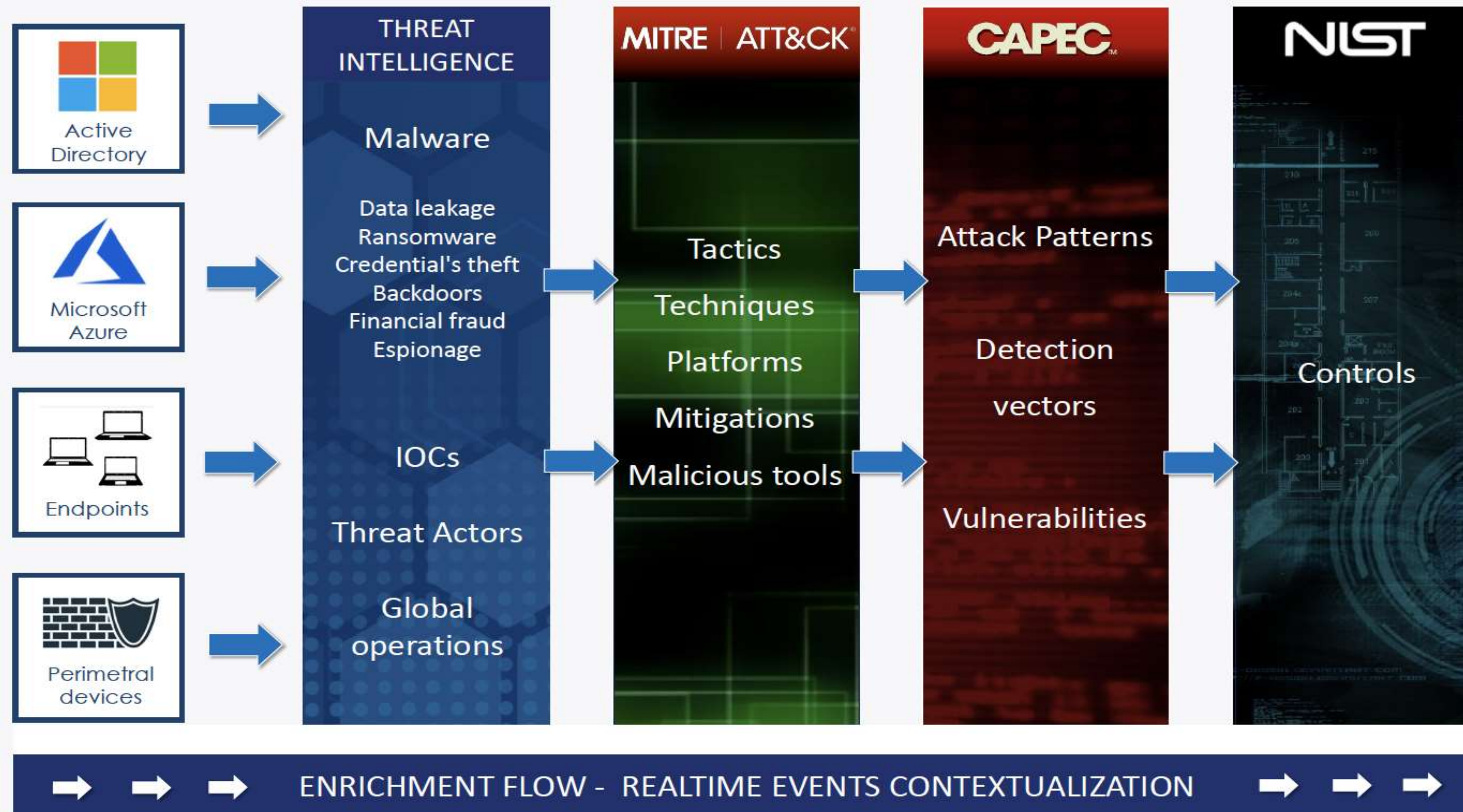
The Roadmap to
the future

Malicious next actions prediction: connecting the dots



What are the possible next malicious activities?
What are the probabilities?

Real-time events enrichment & context



MULTI CLOUD SOC



Ese momento... Que no podremos evitar





Martine is teleworking during COVID-19

Malicious individuals can put you in a stressful or emergency situation and ask you to take unusual actions: large money transfers, extracts from HR databases, confidential client documents, etc.

You may feel more isolated to verify the legitimacy of this request, **here are a few tips to help you get through this:**

Climate of **authority** and **stress** from the requester



Often by **phone call**, but also by **email**

CEO Fraud

In this scam, someone uses an authority report to ask you to perform an **important** and **unusual** action in the context of an emergency.



Targets

everyone is a potential target (especially administrative staff, finance and HR dept.)



Unusual actions

abnormal / excessive situation for the target (e.g. large money transfer or list of confidential data)



Urgent timing

crisis situation that cannot wait (out of usual processes)

Calm things down and sweep doubts away

by validating the information before taking any action







