

CONGRESO · INTELIGENCIA ARTIFICIAL · 2026

Congreso AI LATAM

El encuentro de la comunidad de Inteligencia Artificial de
Latinoamérica.



31JUL



Toronto | Canada



ialatam.com



IA LATAM · Comunidad

Congreso AI LATAM



● ● ● CHARLA MAGISTRAL · TRACK DE IA

The path to Autonomous Cyber Defense

● JOSE CARLOS VARGAS MEDINA

TC1 Labs



- US usage
- State usage
- Global usage
- Country usage
- Job explorer



Anthropic Economic Index Report

See the analysis behind the numbers and what these patterns reveal about AI's economic impact.

[Read the report →](#)

Usage Index

Understand if a country uses Claude more (>1) or less (<1) than expected, based on its population.

Augmentation vs. automation

See how people prefer to work with Claude —collaborating together or fully delegating tasks.

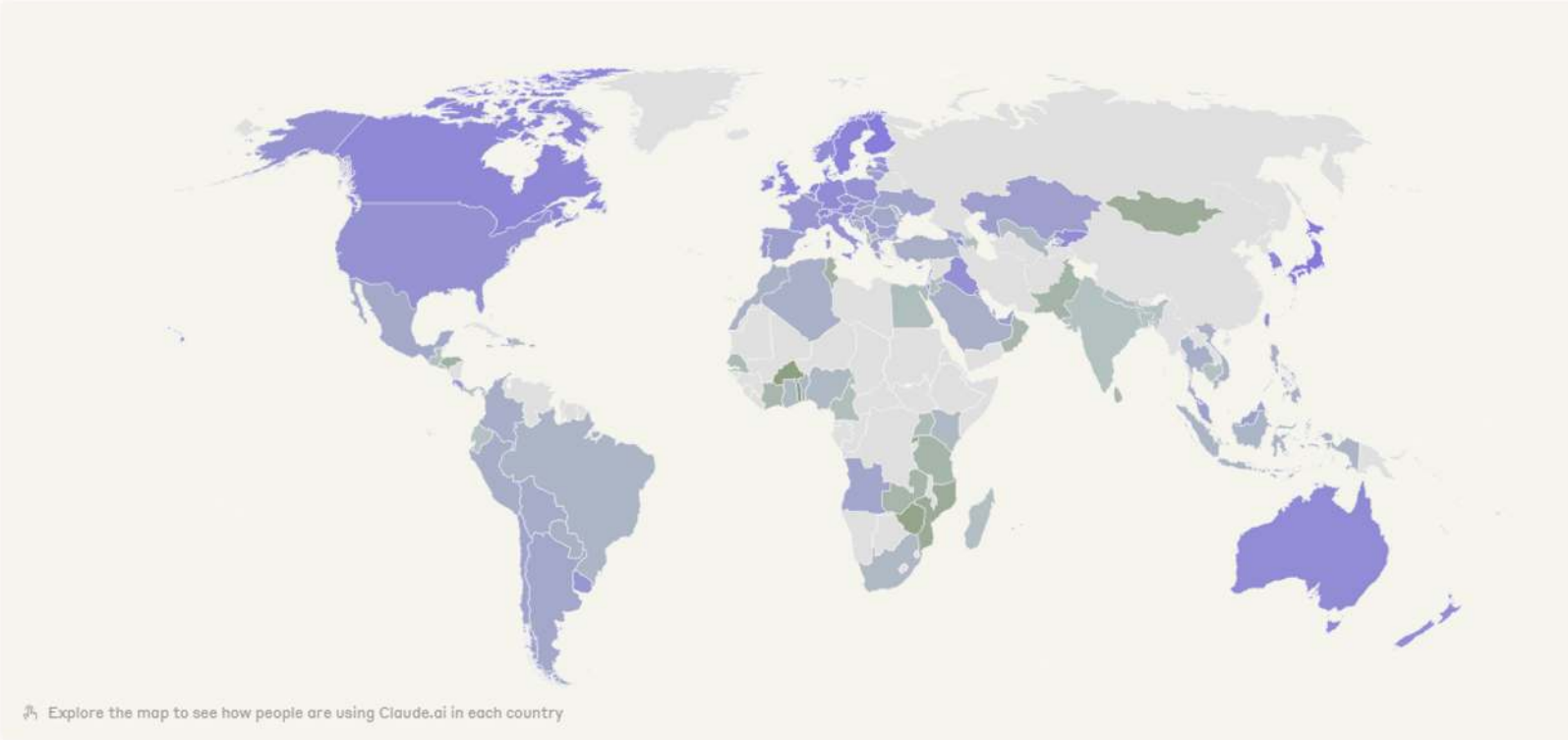


Top Industries

Explore Claude usage by industry across countries.

Use cases

Explore Claude usage by work, personal, and coursework contexts.



The world map shows data on Claude.ai conversations. The world map is based on Natural Earth's world map with the ISO standard point of view for disputed territories, which means that the map may not contain some disputed territories. We note that in addition to the countries shown in gray ('Claude not available'), we do not operate in the Ukrainian regions Crimea, Donetsk, Kherson, Luhansk, and Zaporizhzhia. In accordance with international sanctions and our commitment to supporting Ukraine's territorial integrity, our services are not available in areas under Russian occupation.

Countries in view

Japan	63%		37%	United Kingdom	60%		40%
Finland	62%		38%	Canada	60%		40%
The Netherlands	61%		39%	Ireland	60%		40%
Sweden	61%		39%	Singapore	60%		40%
Denmark	61%		39%	Switzerland	60%		40%

🚨 New milestone in cybersecurity: when AI strikes 🚨

The company Anthropic detects the first cyber-espionage campaign executed by an AI agent.

- The attack in mid-September 2025 has a high probability of being a Chinese state group.
- The target actor included approximately 30 global organizations: large technology companies, financial institutions, chemical manufacturing companies, and government agencies
- AI was involved in 80-90% of the campaign work, and humans were involved in only about 4-6 critical decisions per operation.

"For cybersecurity teams, the message is clear: our defense must evolve at the same pace as attacks. If malicious actors can delegate **80-90% of the operation to AI, our response must also be reimagined with AI, automation, and real-time visibility."**

Policy

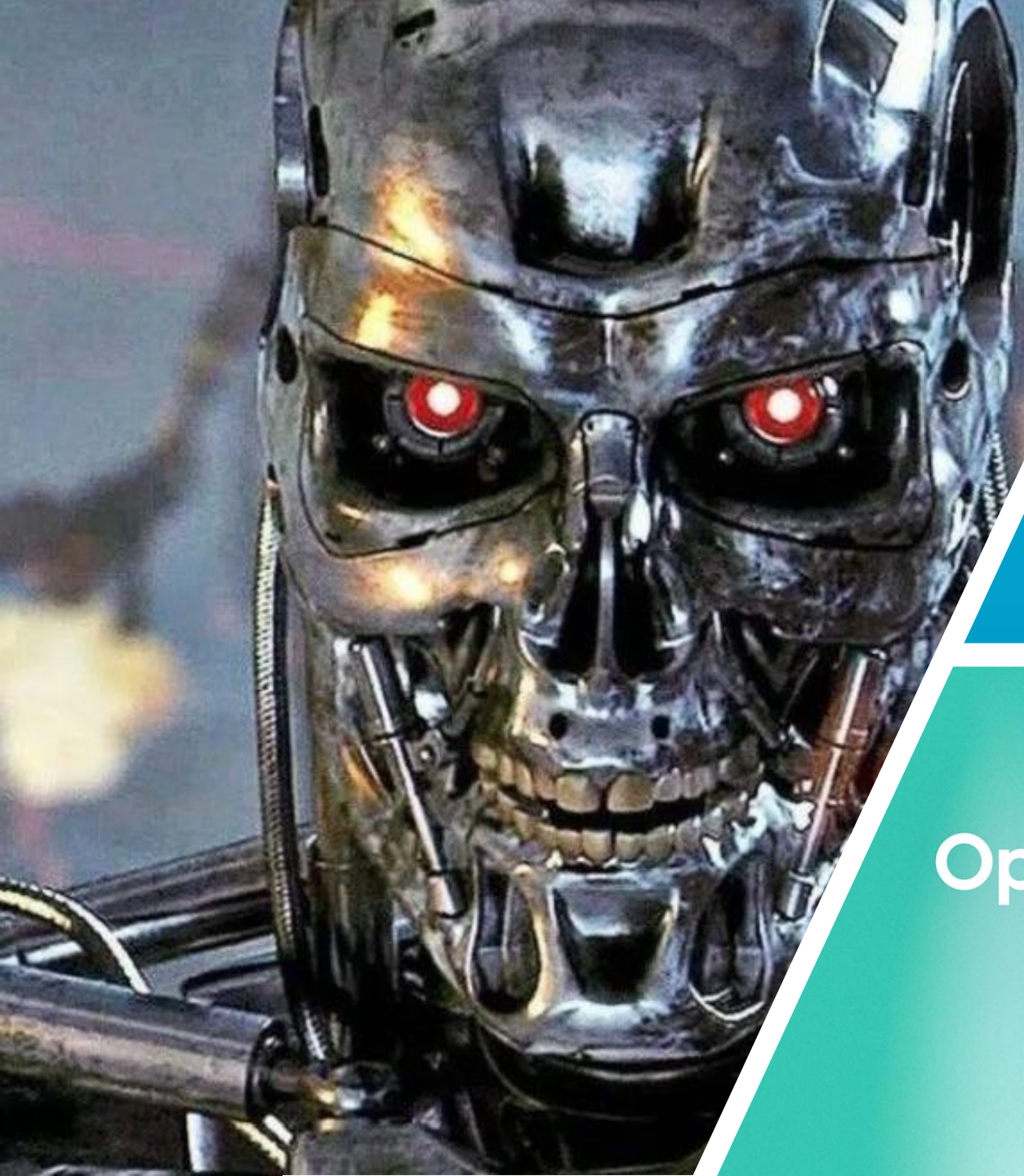
Disrupting the first reported AI-orchestrated cyber espionage campaign

Nov 13, 2025 • 7 min read

[Read the report](#)

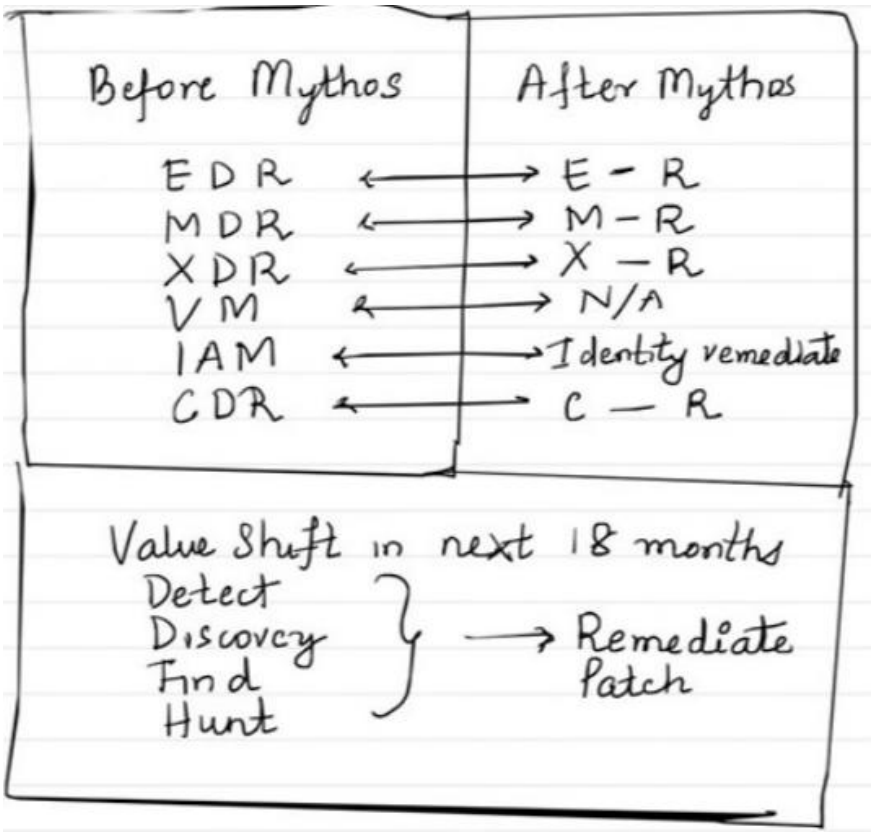
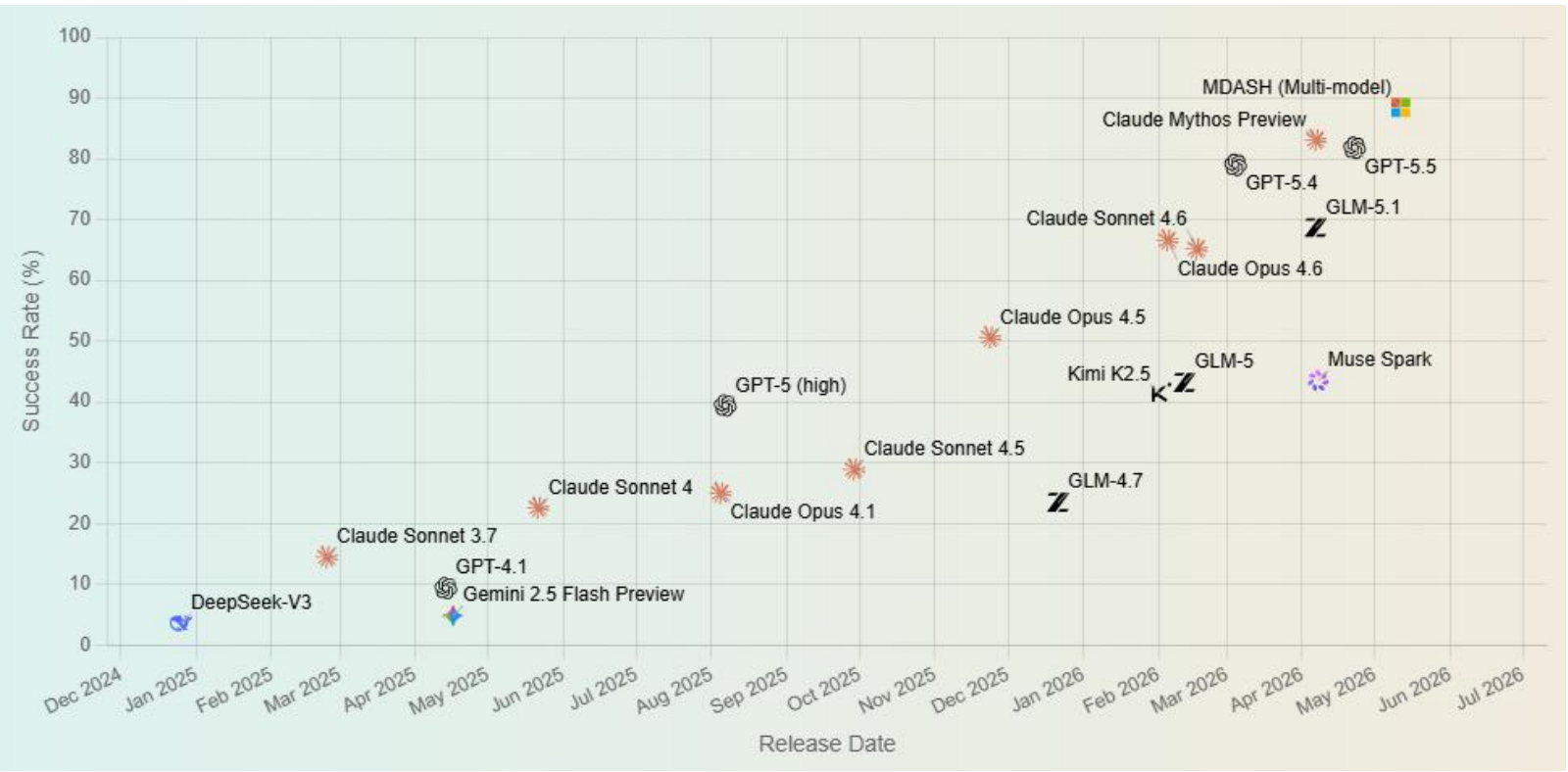


We recently argued that an [inflection point](#) had been reached in cybersecurity: a point at which AI models had become genuinely useful for cybersecurity operations, both for good and for ill. This was based on systematic evaluations showing cyber capabilities doubling in six months; we'd also been tracking real-world cyberattacks, observing how malicious actors were using AI capabilities. While we predicted these capabilities would continue to evolve, what has stood out to us is how quickly they have done so at

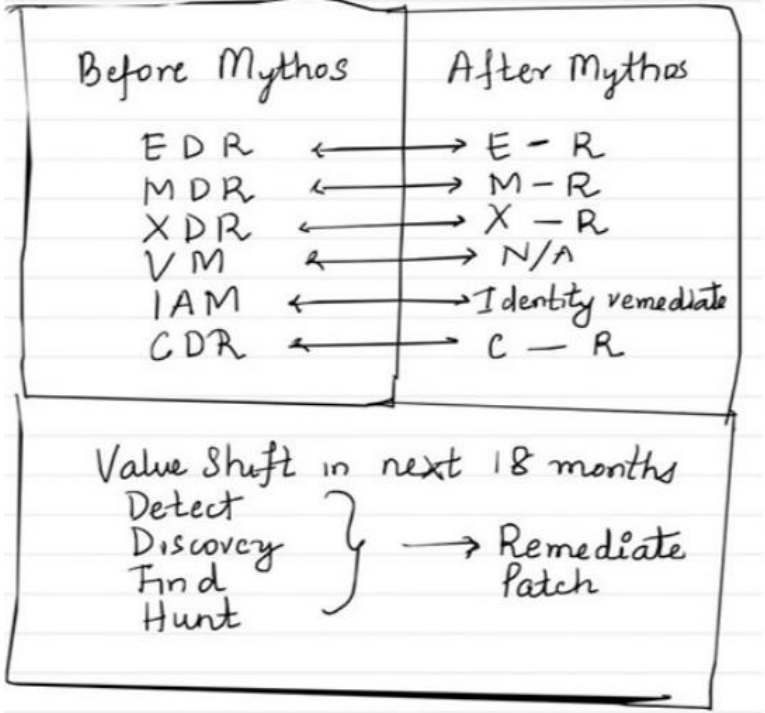
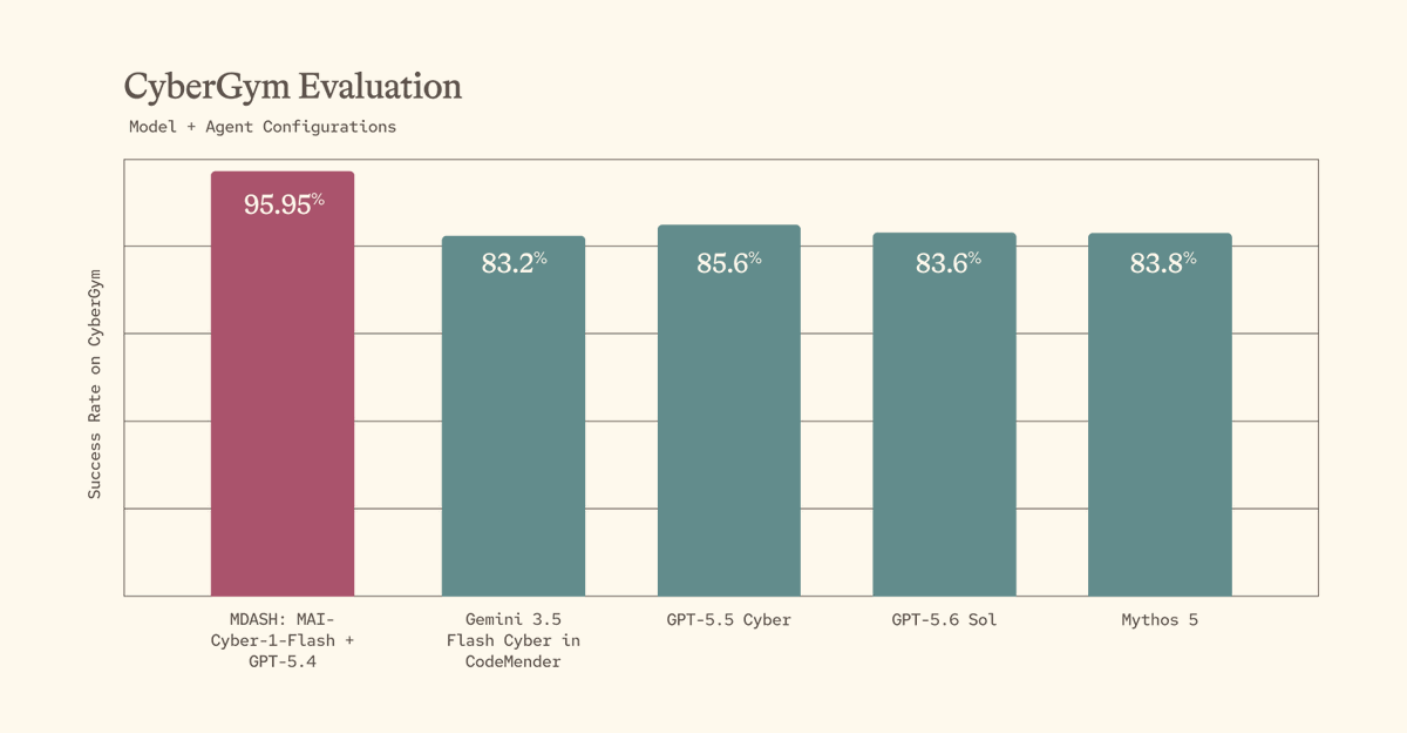


OpenAI and Hugging Face
partner to address
security incident

The New Risk Surface



The New Risk Surface



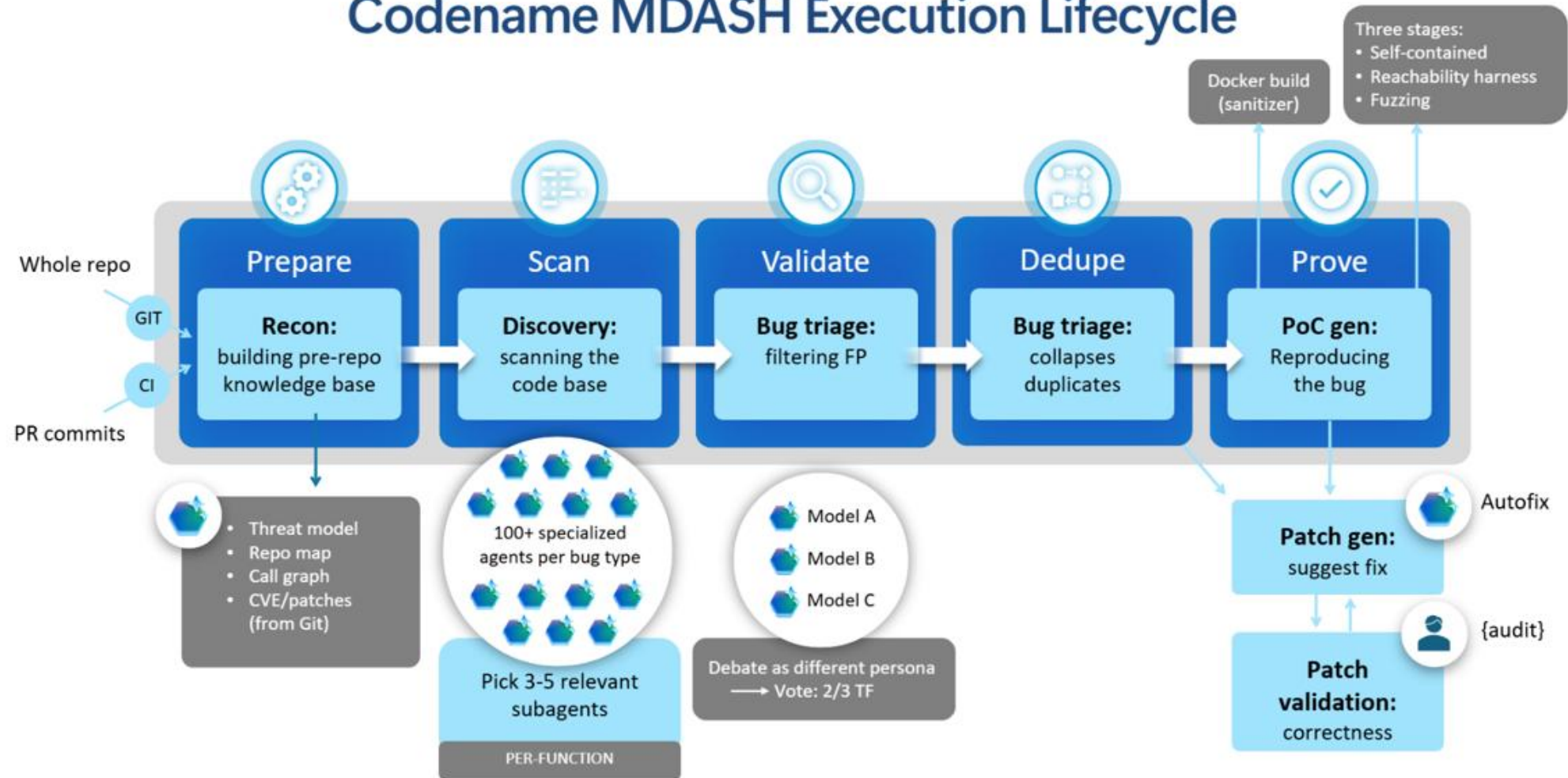
The New Risk Surface



Before Mythos		After Mythos	
EDR	←→	E - R	
MDR	←→	M - R	
XDR	←→	X - R	
VM	←→	N/A	
IAM	←→	Identity remediate	
CDR	←→	C - R	

Value Shift in next 18 months			
Detect	}	→ Remediate Patch	
Discovery			
Find			
Hunt			

Codename MDASH Execution Lifecycle



**How do you resolve this
challenge?**

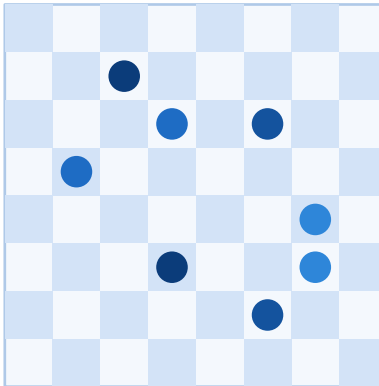
Security needs to be

RETHINKING

New Mindset

Strategize
and think proactively

Anticipate
opponent's next move



Adapt
to constant change

New Principles

Assistive AI



Autonomous AI

Reactive



Proactive

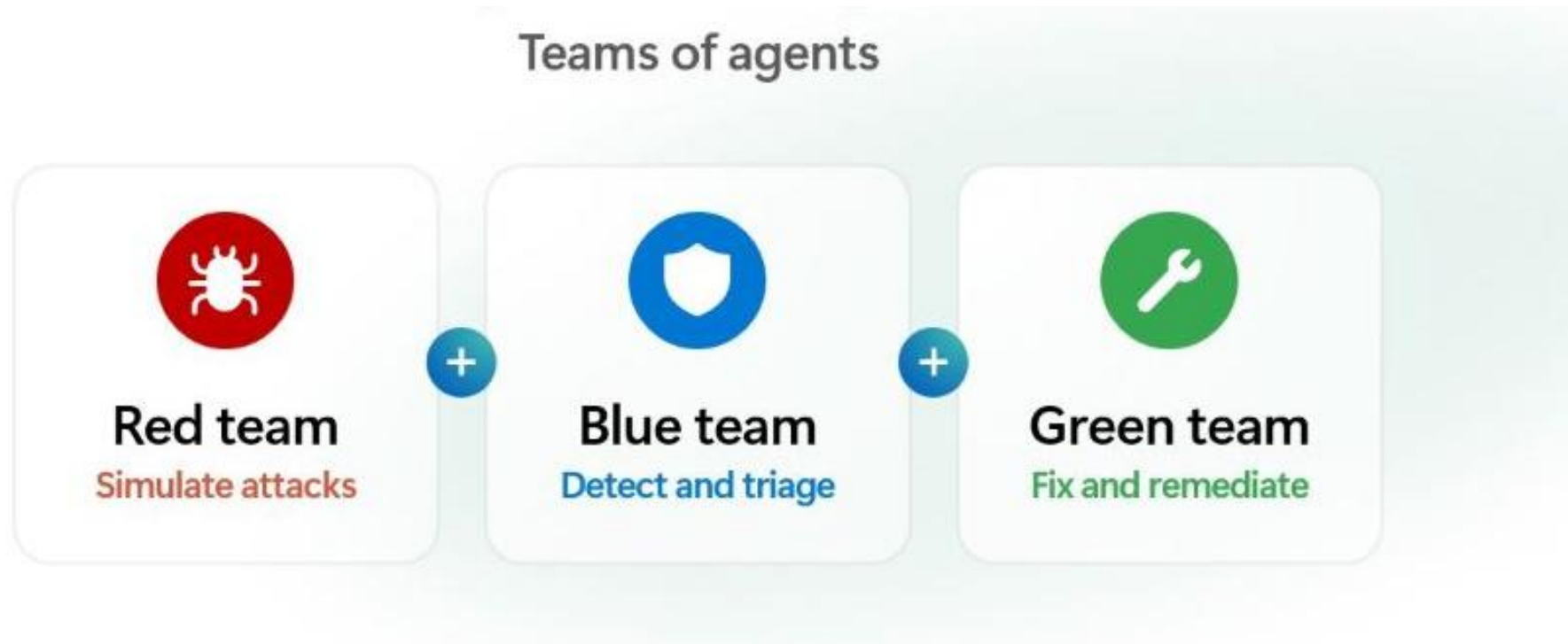
Knowledge-based



Action-based

The New Risk Surface need a new reshape of our cybersecurity capabilities

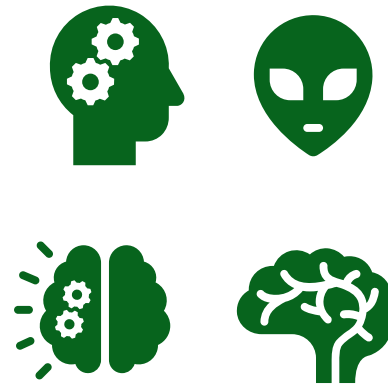
Security needs a new Cyber Stack. A new Cyber Stack must continuously perceive risk across the entire digital estate, reason across vast amounts of context and take action at machine speed. It must learn and adapt as environments evolve, helping organizations stay ahead of threats. And because security is ultimately a human mission, it must amplify defenders with better insights and more powerful ways to act. The defining characteristic of the next generation of security systems will not be their ability to generate more alerts. It will be their ability to continuously perceive, reason and act.



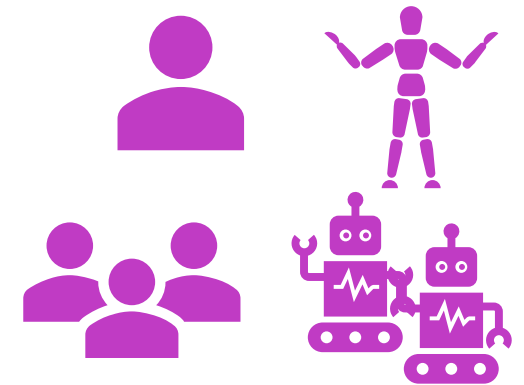
Simplifying security with AI



Data



Model



Experience

Data



The New Risk Surface need a new reshape of our cybersecurity capabilities

Milestone 1

Unify the platform foundation

LAYER • DATA

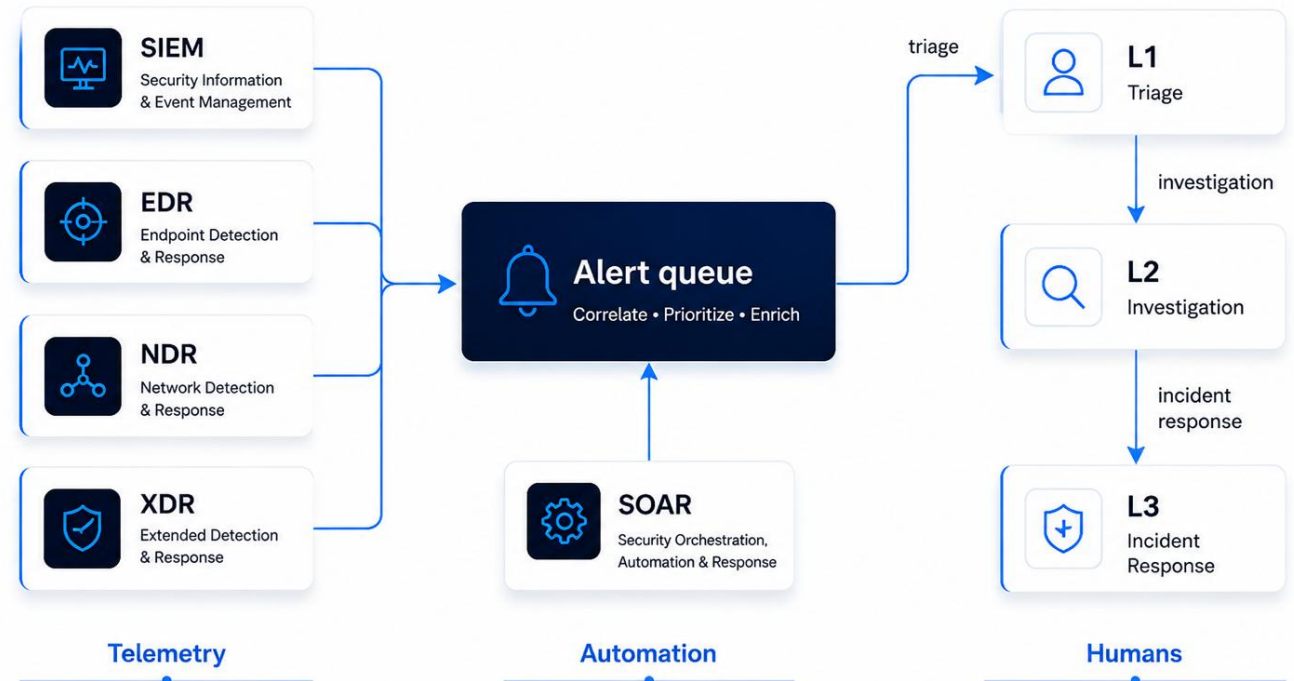
- Unified platform: endpoint, identity, apps and cloud
- Resolves data divergence: one shared view, not hand-stitched evidence
- Data Convergence (Unified | Mix)
- Deterministic autonomous disruption (policy-bound)

RESULT

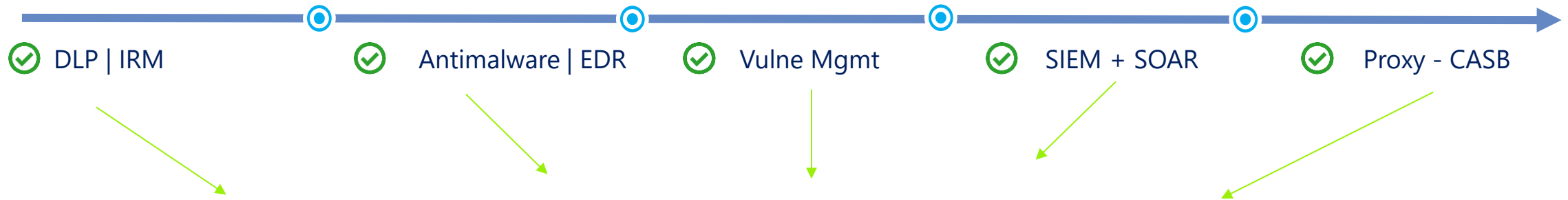
Ransomware contained in ~3 min • 99.99% confidence

Unified Security Platform

Intelligent detection. Automated response. Human oversight.



Data | Components to platform

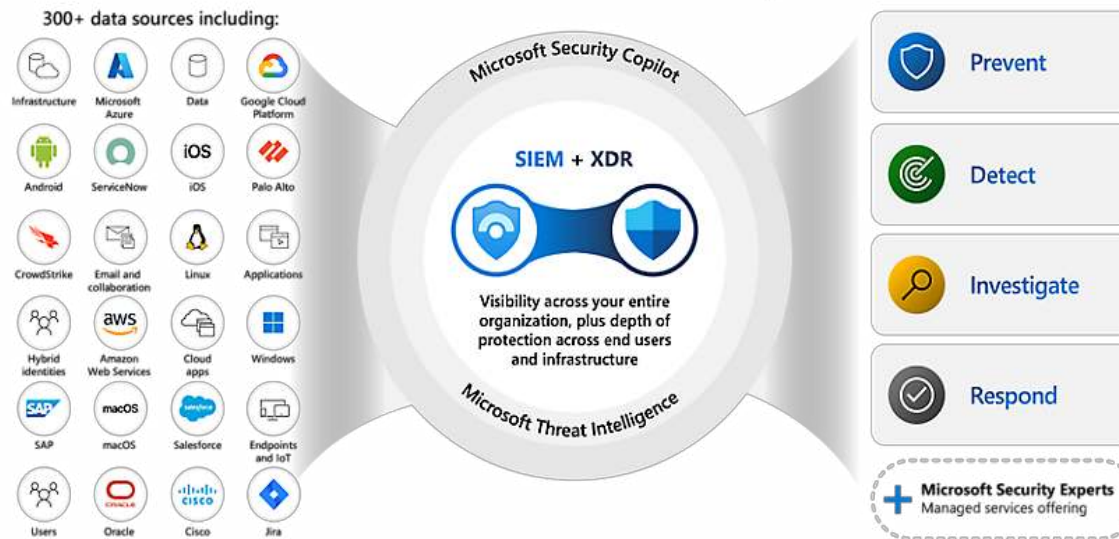


Simplifying is key to strengthening business agility.

75% of security leaders adopt a consolidation strategy since 2022.

A unified security operations platform

Microsoft Sentinel and Defender XDR together



- ~24% reduction of architectural tools simplifying and reducing operating cost of operation.
- Savings of 10% - 20% on licensing costs and support of cybersecurity tools, while occasionally savings of up to 35% per year are realized
- Increased automation capabilities and enabling Generative AI and Agent capabilities for CyberSOC operation (~80% reduction in D&R time)
- Reduction of administrative burden and management of daily operations and in the investigation and response to cyberattacks.

Model



The New Risk Surface need a new reshape of our cybersecurity capabilities

Milestone 2

Accelerate with GenAI + task agents

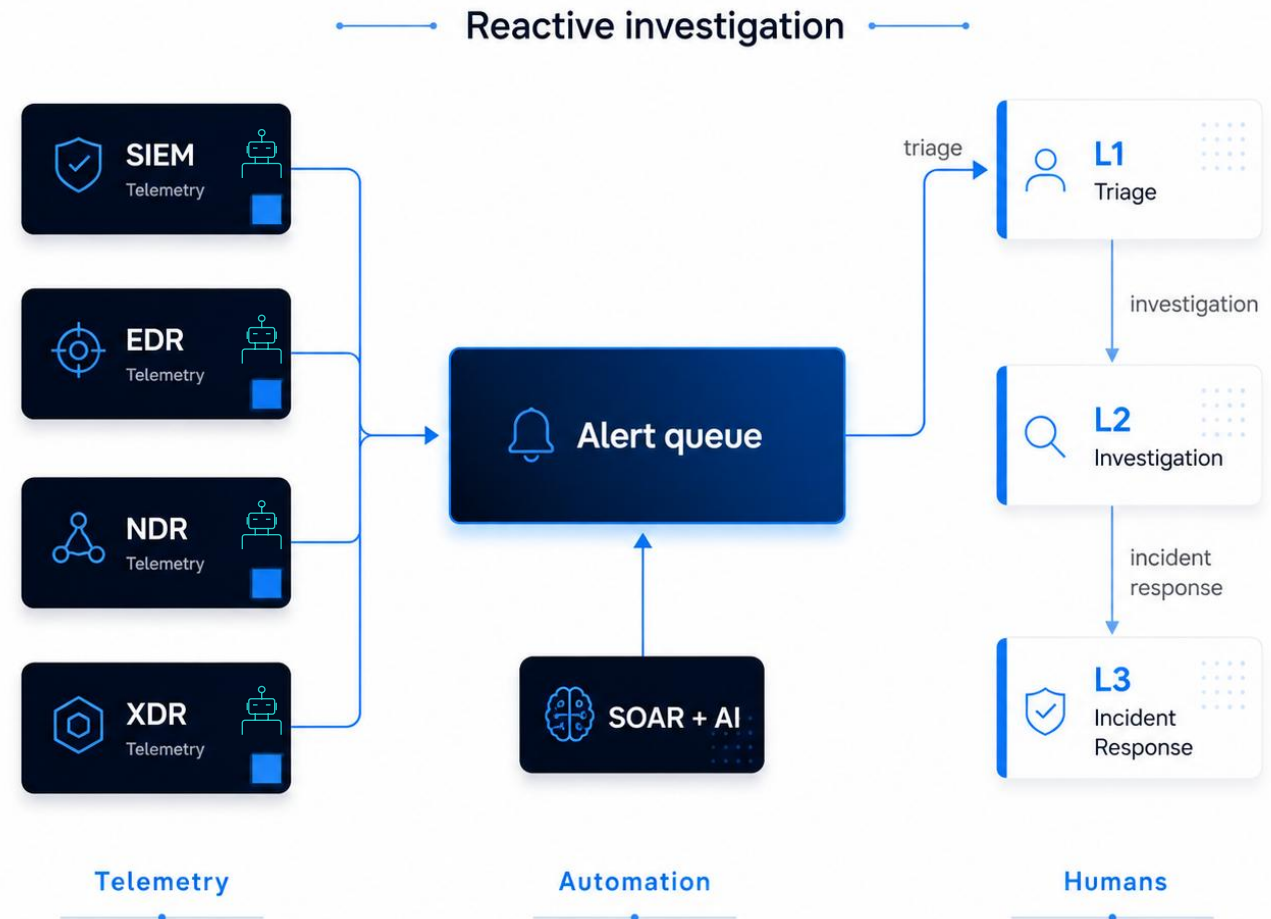
LAYER · MODEL — Cybersecurity Brain

- Security Copilot assembles context and synthesizes signals
- Task agents under human supervision
- Coherent investigations; alert noise drops
- The analyst shifts from executing to deciding

RESULT

~75% of phishing/malware investigations automated

AI-augmented SOC operating model

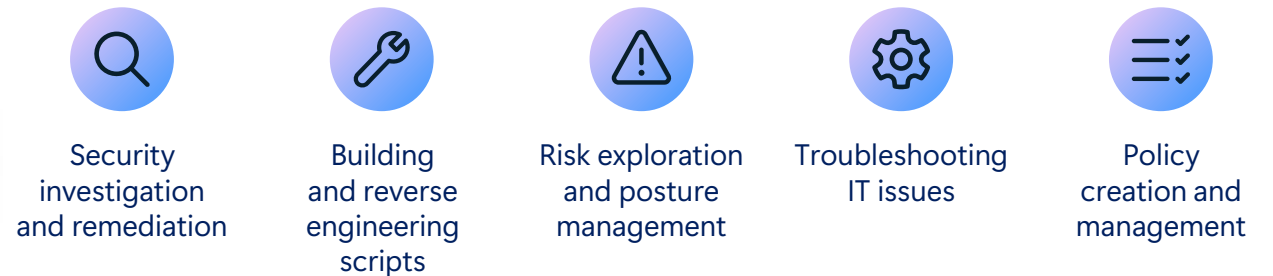


Model | Brain

A generative AI-powered assistant for daily operations in security and IT that empowers teams to protect at the speed and scale of AI



Always-ready Gen AI assistant for use cases like:



30% reduction in mean time to resolution¹

The New Risk Surface need a new reshape of our cybersecurity capabilities

Milestone 3

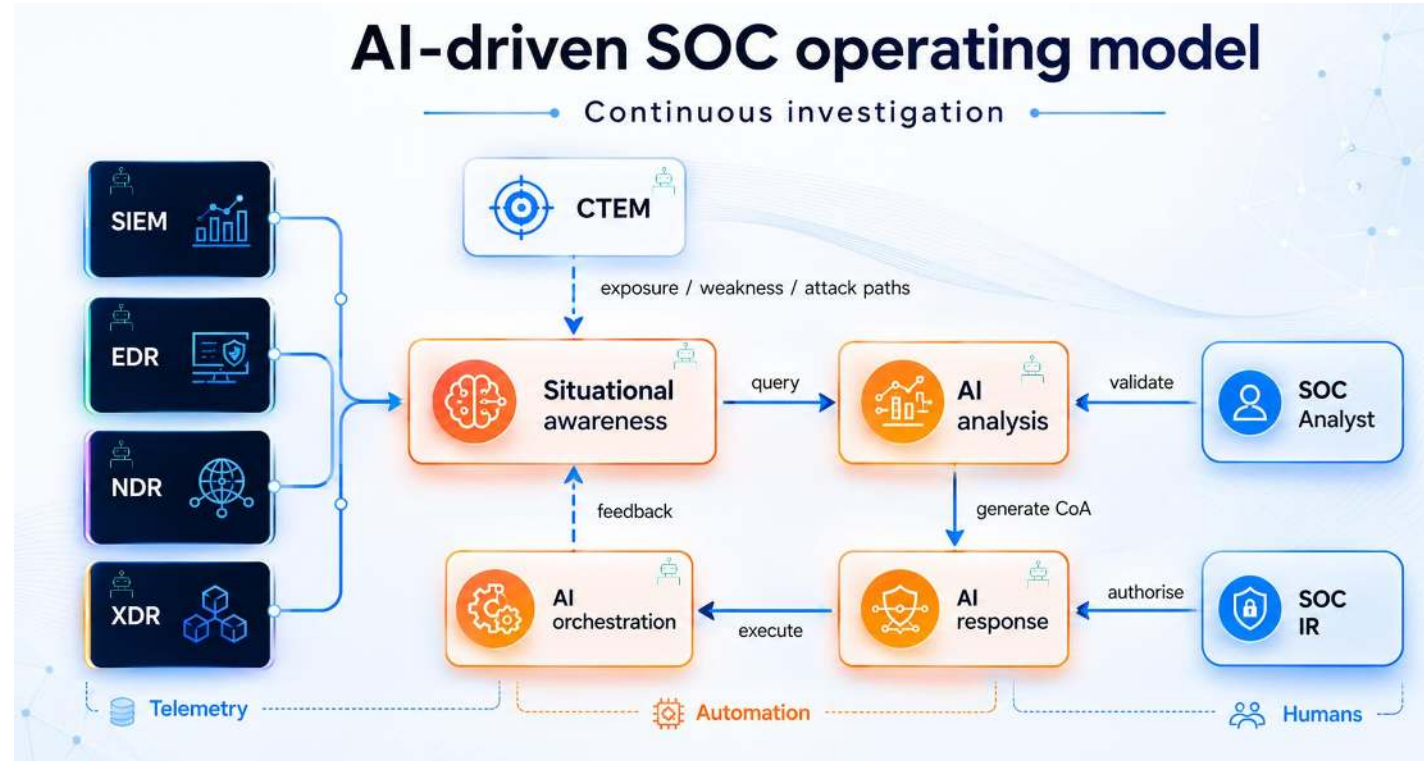
Deploy agentic automation

LAYER • EXPERIENCE – Autonomous defense

- Agents orchestrate cross-domain response
- Anticipate attack paths and optimize posture (CTEM)
- The human defines intent; AI executes at machine speed
- The team shapes posture and risk, not queues

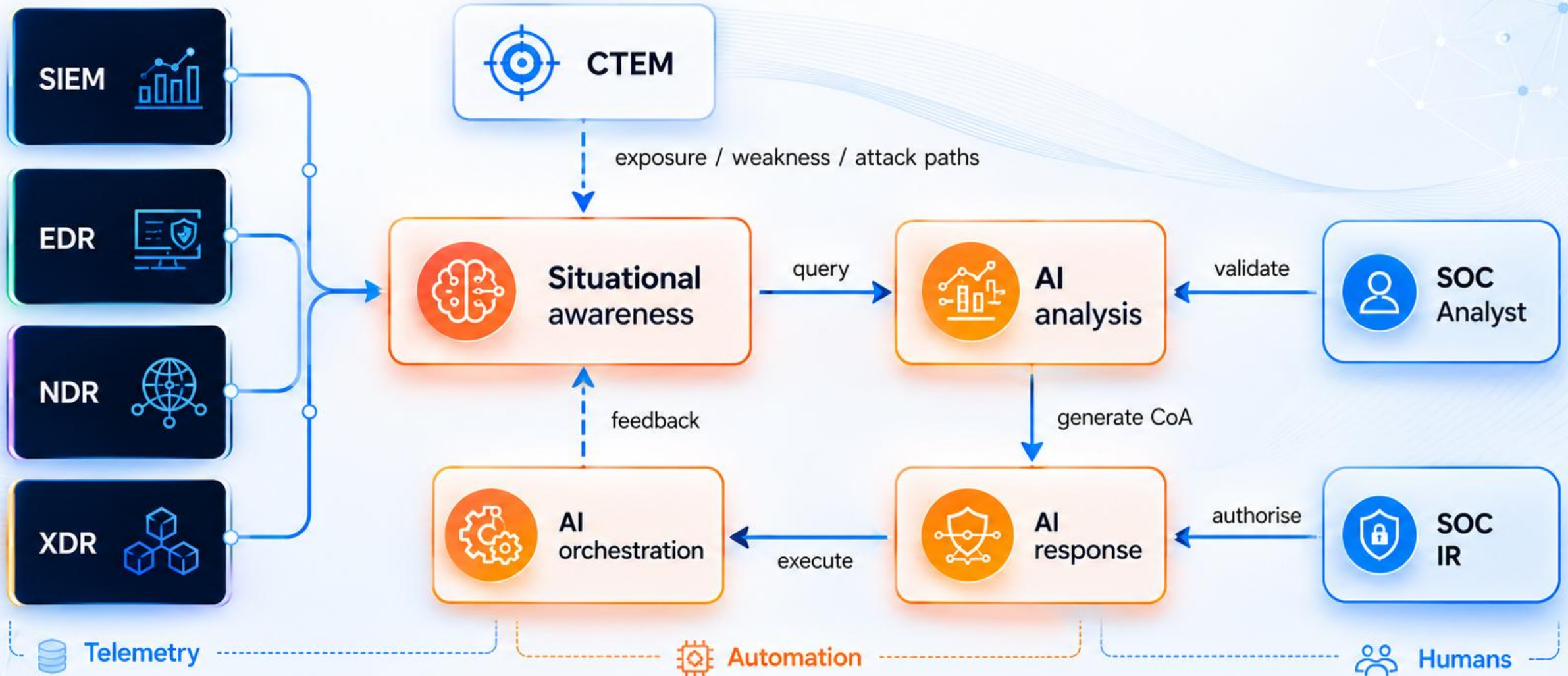
RESULT

Adaptive, autonomous defense at scale



AI-driven SOC operating model

Continuous investigation



Experience





New Era CyberSOC



Remember

- AI is changing everything, and cybersecurity is at the center of this new era.
- Simplifying and transforming is the key to protecting ourselves in this new era.

CONGRESO · INTELIGENCIA ARTIFICIAL · 2026

Congreso AI LATAM

El encuentro de la comunidad de Inteligencia Artificial de
Latinoamérica.



31JUL



Toronto | Canada



ialatam.com



IA LATAM · Comunidad

Congreso AI LATAM