
WELCOME TO
Integrity360
your security in mind
SECURITY FIRST
CYBER SECURITY CONFERENCE 2026
DARKTRACE
CROWDSTRIKE
aws
SentinelOne
VECTRA
FORTINET
RESILIENCE REDEFINED:
SECURING THE HUMAN-AI ERA

Integrity360
your security in mind

SECURITY FIRST

Welcome by regional team

Shabeer Ramsingh

Global Head - Strategic Business Development, Integrity360

Candice Burke

Business Development Manager, Integrity360

Jessica Magalhaes

Business Development Executive, Integrity360

#SecurityFirst2026

Integrity360
your security in mind

SECURITY FIRST

09:30 **Welcome & opening**
Intergrity360

09:40 **Resilience redefined: Securing the human-AI era**
Integrity360

10:35 **Client panel: Building a security culture that thrives with AI**
Integrity360 | Ramps Logistics | First Citizens

11:00 **Comfort break**

11:20 **How to Succeed When Every Day is Zero-DAI**
Darktrace

11:45 **Panel: Keeping the Lights On: Defending CPS and Critical Infrastructure in the AI Era**
Integrity360 | Fortinet | Water & Sewerage Authority T&T

12:15 **Lunch**

13:15 **Panel: AI in the SOC: Turning intelligence into resilience**
Integrity360 | SentinelOne | Vectra | Infolink Service Limited

13:45 **AI-Accelerated Threat Landscape: The Year of the Evasive Adversary**
Crowdstrike

14:10 **Panel: Networks without borders: Trust nothing, verify everything**
Integrity360 | Government of the Republic of T&T | CARPHA

14:30 **Refreshment break**

14:50 **Fireside Chat: Q-day & beyond – Building resilience for the Quantum age**
Integrity360 | City of Bridgetown Credit Union

15:15 **Guest speaker: Resilience & decision making under pressure with Dalton Grant**

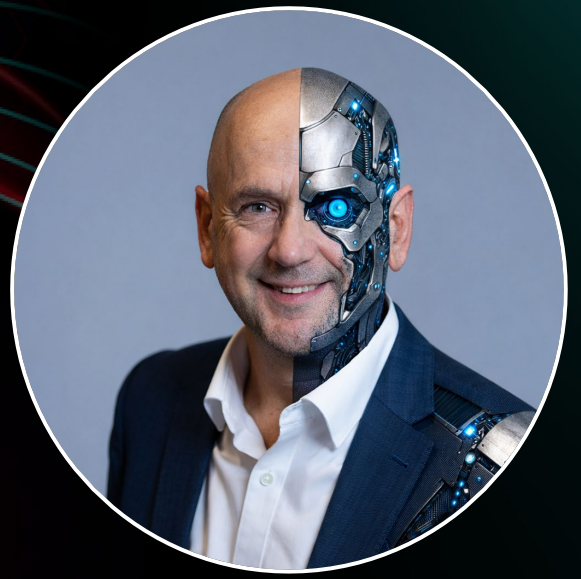
16:00 **Wrap up& drinks reception**

Integrity360
your security in mind

SECURITY FIRST

Resilience Redefined:

Securing the Human-AI Era



Richard Ford
CTO

Brian Martin
Director of Product Management

#SecurityFirst2026

SECURITY FIRST

Resilience & Human-AI Era...

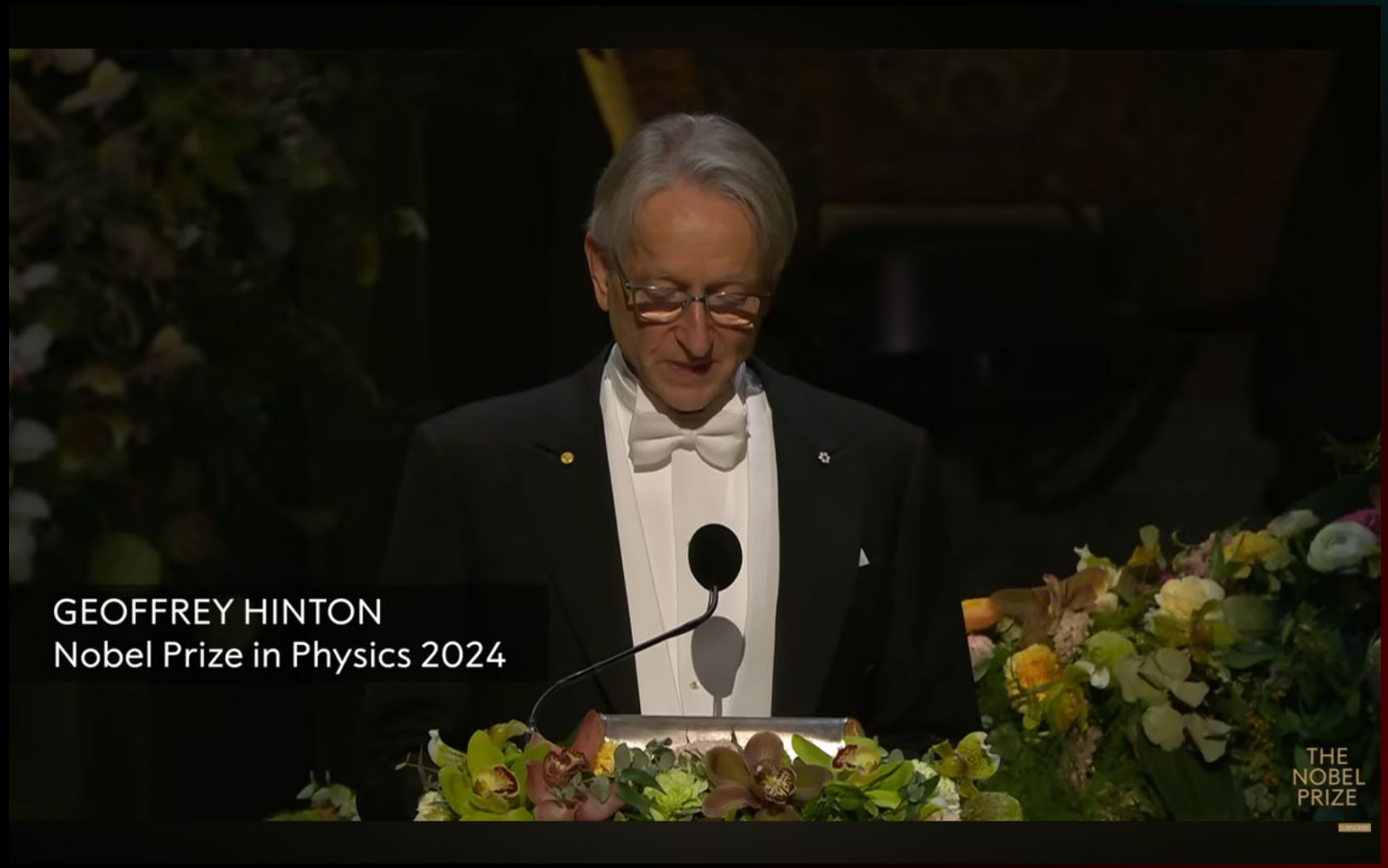
...What's the relevance?

We are at a pivotal moment for security...

...not just security. For the human race.

Integrity360
your security in mind

Sound crazy?




AI-pocalypse Now?


SUCCESS!
UNSTOPPABLE!
GENIUS CEO!
AI
RESEARCH
CONCERNS
SAFETY
SECURITY

SECURITY FIRST

Rapid AI Adoption

AI Tripping Hazards

*"AI is amazing but far from perfect. Our over-belief in it's capability **is** going to trip us up"*

Accuracy

Control

Knowledge


SAASPOCALYPSE
FEBRUARY 2026
CRM
SaaS
DOWN
CLOUD STORAGE
SUBSCRIPTIONS CANCELLED!
STOCKS CRASH!

Integrity360
your security in mind

SECURITY FIRST

Is it all about AI?

Integrity360
your security in mind

SECURITY FIRST

600,000

= 43% of UK businesses reported experiencing cyber security breach or attack.

2025

NCSC managed 204 significant or highly significant cyber incidents up to September.

Integrity360
your security in mind

SECURITY FIRST

Cyber Resilience - Defined

"The ability to ....

- Anticipate
- Withstand
- Recover from
- Adapt to

"…..cyberattacks to minimise business disruption from cyber incidents."

NIST Gartner

Integrity360
your security in mind

SECURITY FIRST

5 Key Factors redefining resilience in the Human-AI era

Anticipate

Withstand

Recover from

Adapt to


Integrity360
your security in mind
SECURITY
FIRST
1. AI Risk Visibility

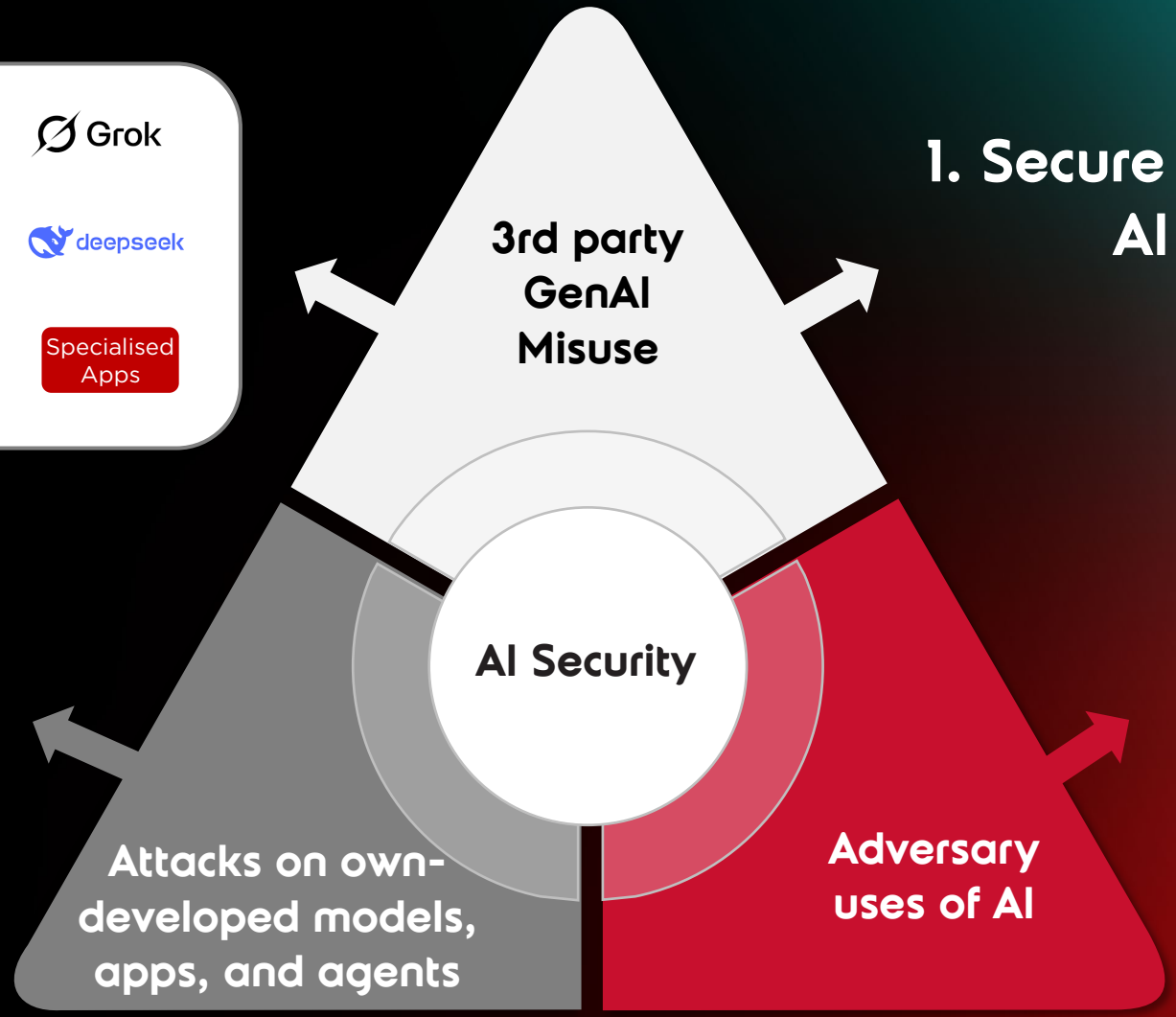

AGENTIC AI-RMAGEDDON

Integrity360
your security in mind

SECURITY FIRST

AI Security - New Threats and Risks

ChatGPT
Microsoft Copilot
Gemini
Grok
Claude
Meta AI
perplexity
deepseek
GitHub Copilot
Embedded GenAI
Long Tail Apps
Specialised Apps



1. Secure Use of AI

2. Secure own AI

3. Secure against AI

Integrity360
your security in mind

SECURITY FIRST

ARTIFICIAL INTELLIGENCE

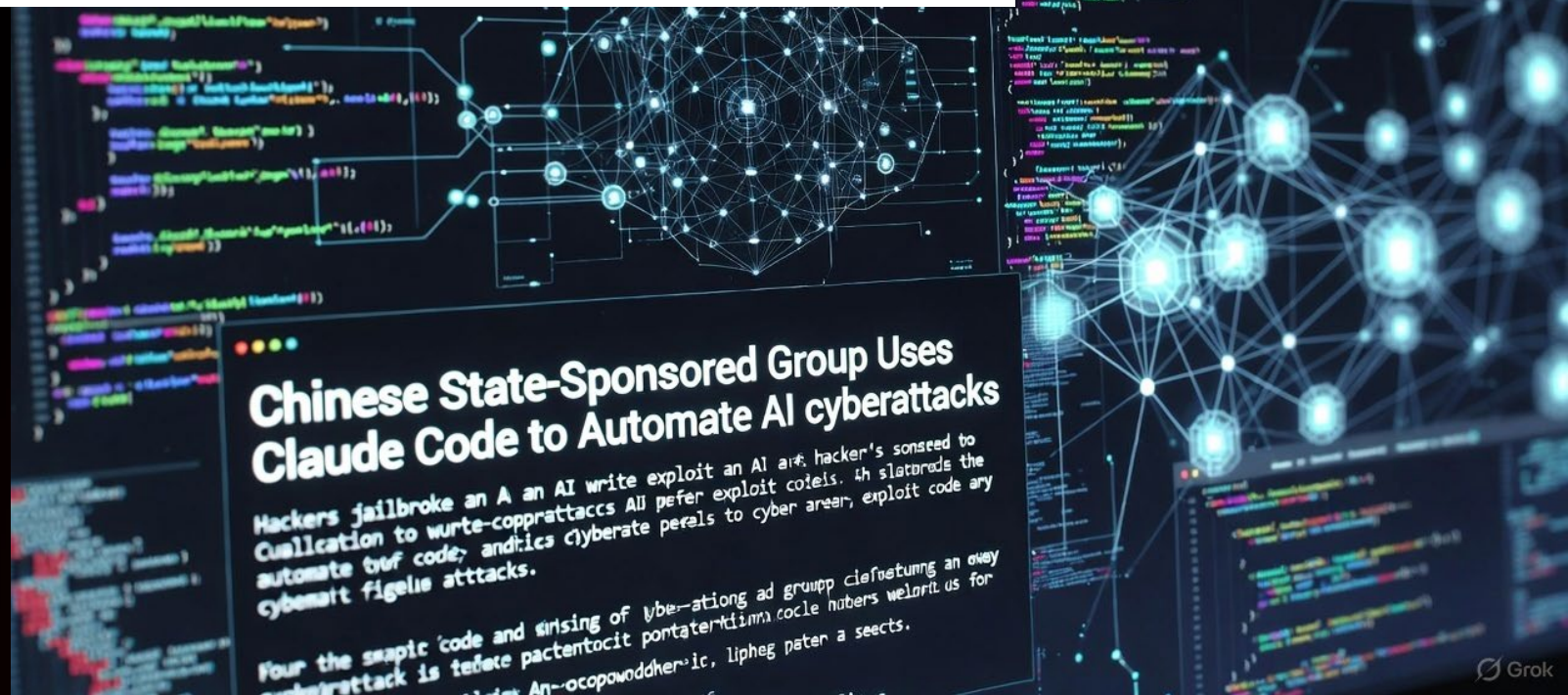
Cyberattacks by AI agents are coming

Agents could make it easier and cheaper for criminals to hack systems at scale. We need to be ready.

AI Agents Drive First Large-Scale Autonomous Cyberattack

By Georgia Collins

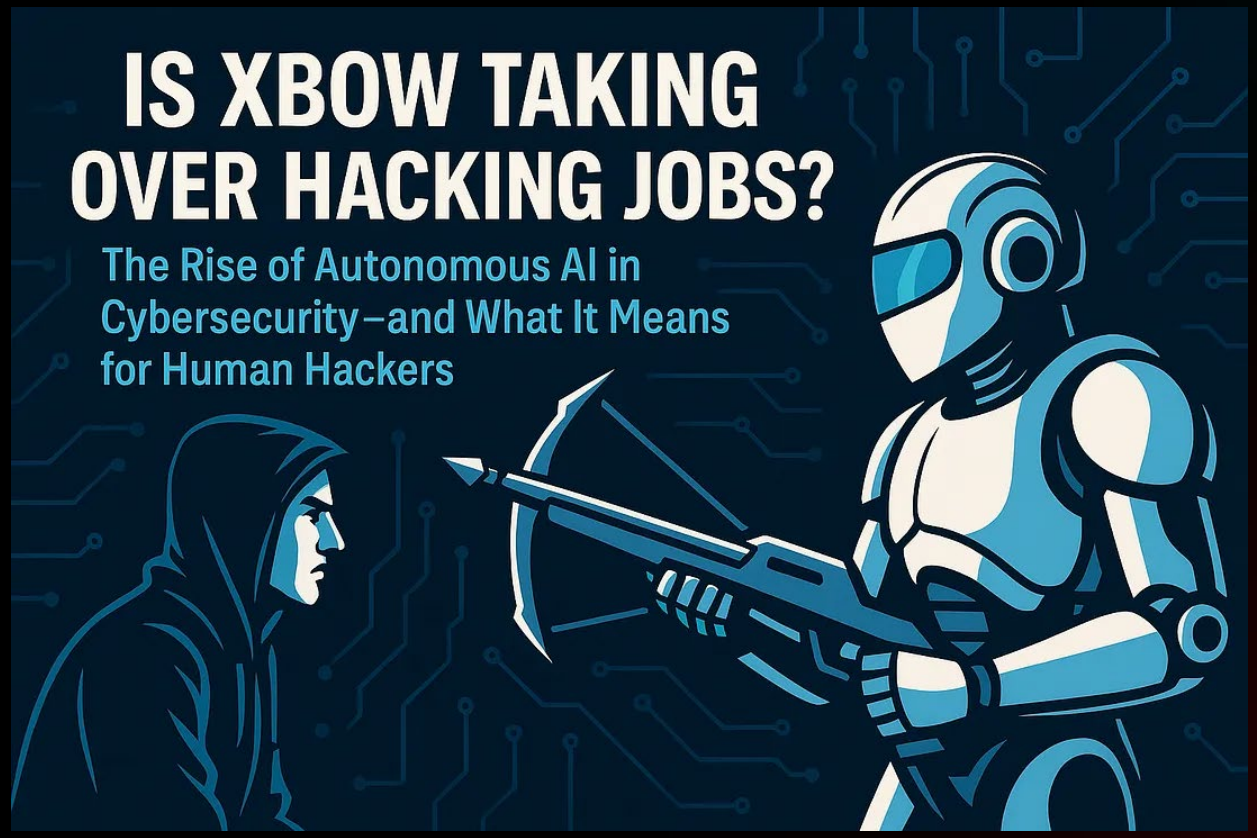
January 17, 2026 • 3 mins

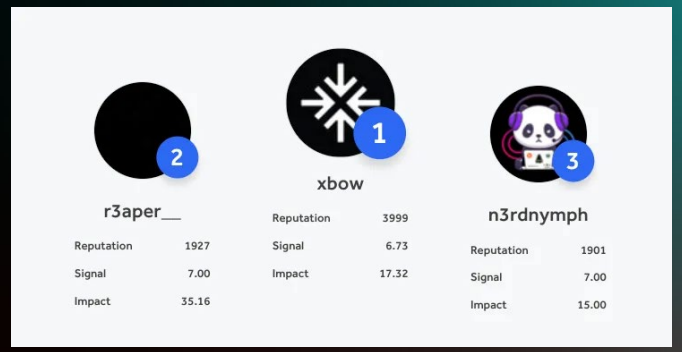


Integrity360
your security in mind

SECURITY FIRST

AI Scales Exposure Discovery





- As of February 2026, XBOW ranked as the #1 hacker on the HackerOne US leaderboard
- In a 90-day surge, XBOW submitted over 1,060 vulnerabilities, surpassing the output of thousands of human researchers
- In head-to-head trials, XBOW completed tasks in 28 minutes that took a seasoned human pen-tester 40 hours

An autonomous AI-driven penetration testing platform

Integrity360
your security in mind

SECURITY FIRST

AI Scales Exposure Discovery - AN UPDATE

Fail Safe: Why major AI player Anthropic won't release its new model

Updated / Sunday, 12

Mythos Preview has already found thousands of high-severity vulnerabilities, including some in *every major operating system and web browser*. Given the rate of AI progress, it will not be long before such capabilities proliferate, potentially beyond actors who are committed to deploying them safely. The fallout—for

Anthropic keeps latest AI tool out of public's hands for fear of enabling widespread hacking

AI company says purpose of its Claude Mythos model is to bolster defenses against hacking in common applications

US summons bank bosses over cyber risks from Anthropic's latest AI model

Fed chair Jerome Powell reportedly attends meeting in Washington following release of Claude Mythos

Anthropic's Mythos Will Force a Cybersecurity Reckoning—Just Not the One You Think

The new AI model is being heralded—and feared—as a hacker's superweapon. Experts say its arrival is a wake-up call for developers who have long made security an afterthought.

Project Glasswing

Securing critical software for the AI era

aws · ANTHROPIC · BROADCOM · CISCO · CROWDSTRIKE · Google · JPMorganChase · THE LINUX FOUNDATION · Microsoft · NVIDIA · paloalto NETWORKS

Integrity360
your security in mind

SECURITY FIRST

Human vs Agentic attackers

Vs

SPEED	Minutes/hours per step	Milliseconds per step
SCALE	One target at a time	100's of targets simultaneously
PERSISTENCE	Humans need sleep/breaks	24/7 continuous operations
ADAPTABILITY	Strategic, but slow to pivot	Tactical & instantaneous pivoting

Integrity360
your security in mind

SECURITY FIRST

AI Reduces barrier to entry - "vibe-coded" Copycat Cybercrime

CLINE (⌘+')

Task $0.0000

I need to build test code that mimics this actor https://www.trendmicro.com/en_us/research/25/c/the-espionage-toolkit-of-earth-alux.html can you help me?

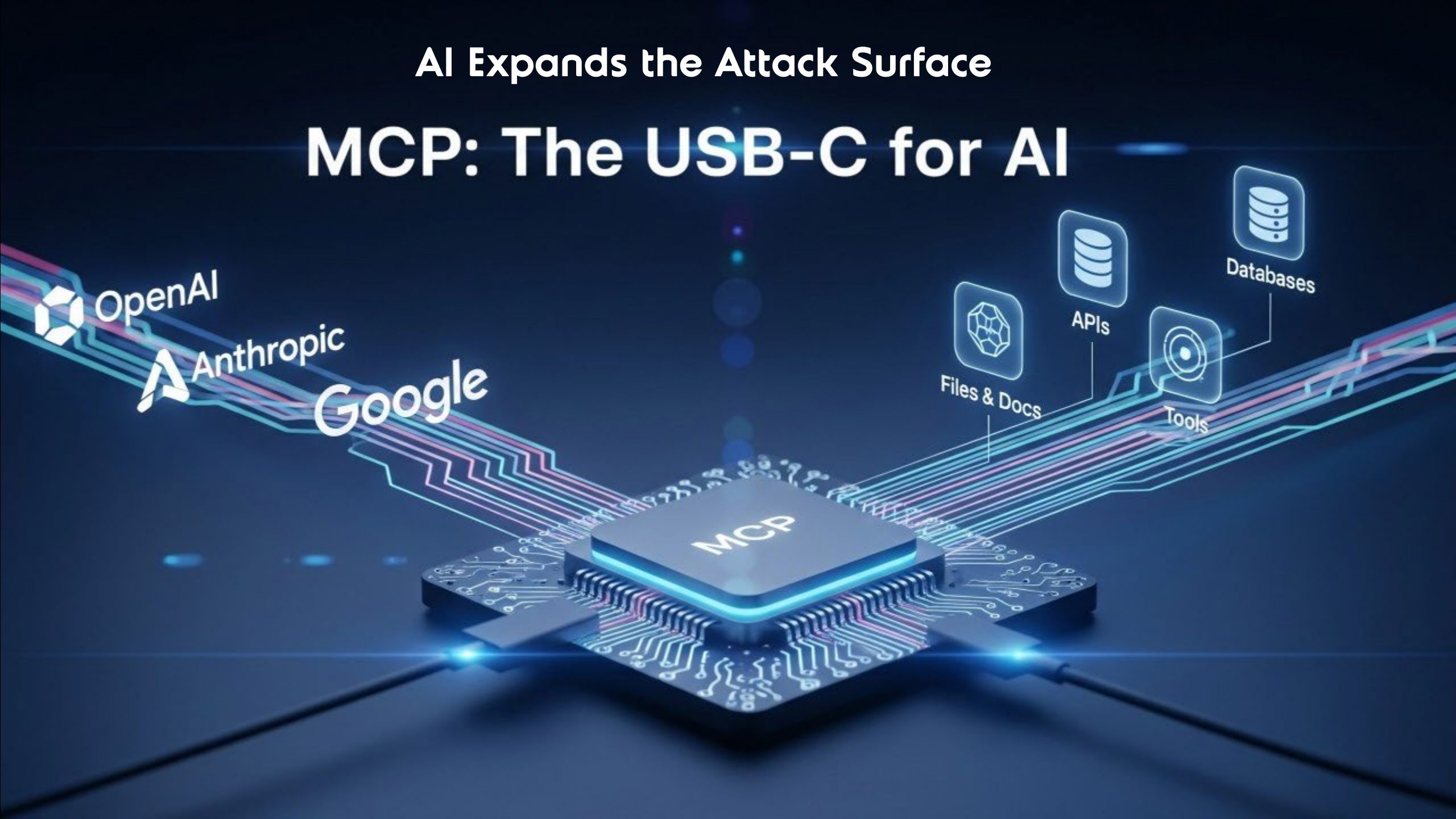
Tokens: ↑ 1.1m ↓ 26.7k

58.2k 128.0k

```
==================================================
[2025-08-08 11:43:36,358] [INFO] [run_full_simulation] Simulating initial access via web shell exploitation
  → Scanning for vulnerable web services...
  → Found vulnerable service on port 8080
  → Exploiting vulnerability...
  → Deploying GODZILLA web shell...
  → Web shell successfully deployed

✓ Initial access established

[Phase 2] First Stage Backdoor Deployment
==================================================
[2025-08-08 11:43:36,978] [INFO] [run_full_simulation] Deploying first stage VARGEIT backdoor
  → Uploading fontdrvhost.exe (renamed cdb.exe)...
  → Creating config.ini with loader shellcode...
  → Executing debugger script...
  → VARGEIT backdoor loaded in memory
  → Establishing C2 communication...
[2025-08-08 11:43:37,500] [INFO] [vargeit_simulator] Enabled channel: Outlook (ID: 5)
[2025-08-08 11:43:37,500] [INFO] [vargeit_simulator] VARGEIT simulator initialized with ID: 0cb07589-a67c-4aca-8874
[2025-08-08 11:43:37,500] [INFO] [vargeit_simulator] Simulating Outlook channel communication
[2025-08-08 11:43:37,512] [INFO] [vargeit_simulator] Created draft message: p_17595803760857882363
[2025-08-08 11:43:37,513] [INFO] [vargeit_simulator] Simulated command received: r_17595803760857882363
[2025-08-08 11:43:37,513] [INFO] [vargeit_simulator] Processing command: collect_system_info
  → Outlook channel active (Message ID: 17595803760857882363)

✓ First stage backdoor active

[Phase 3] Persistence Installation
==================================================
[2025-08-08 11:43:37,618] [INFO] [run_full_simulation] Installing persistence mechanisms

[3.1] Deploying RAILLOAD
[2025-08-08 11:43:37,625] [INFO] [railload_simulator] RAILLOAD simulator initialized
```

AI & open-source tools aid criminals in turning security blogs into partial malware, complicating attack attribution & fueling copycats

AI Expands the Attack Surface



Integrity360
your security in mind

SECURITY FIRST

MCP Real-world exploits

The GitHub "Prompt Injection Data Heist" (May 2025)

Prompt injection instructed developer’s agent using GitHub MCP server to read and exfiltrate private source code

The "NeighborJack" Network Exploit (July 2025)

Could send a command to >7,000 publicly accessible MCP servers to execute directly on the host’s OS, leading to total machine takeover

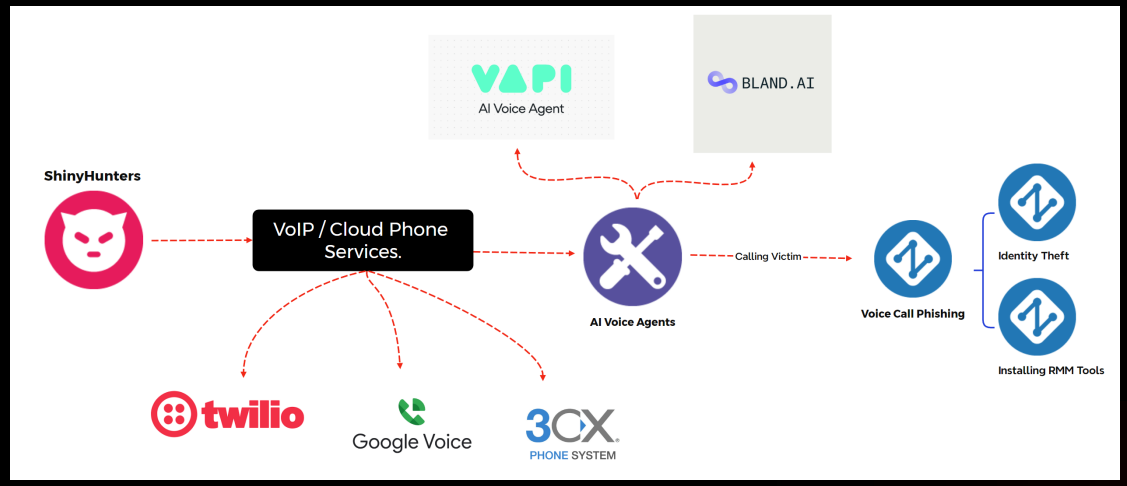
The Smithery.ai Supply Chain Breach (October 2025)

Configuration error allowed attackers to "escape" sandbox exposing >3,000 AI servers leaking 1,000’s of API keys.

Integrity360
your security in mind

SECURITY FIRST

AI Powers Automated Mass Vishing



- Uses VoIP based calling services for vishing operations
- Abuses legitimate AI-powered voice call platforms
- Automating social engineering calls at scale
- AI-driven social engineering agents adjust narratives and tactics in real time
- Attackers configure voice styles including gender and regional accents
- Primarily targets Okta, Google SSO and Microsoft SSO environments

Example Claimed Victims

SOUNDCLOUD
30m+ records

Betterment
2m+ records

crunchbase
20m+ records

https://blog.eclecticiq.com/shinyhunters-calling-financially-motivated-data-extortion-group-targeting-enterprise-cloud-applications

Integrity360
your security in mind

SECURITY FIRST

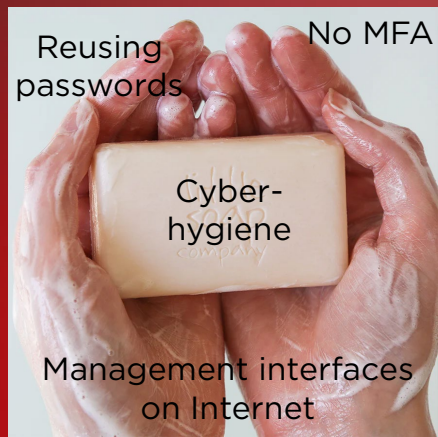
AI Enables Exploit of Poor Cyber Hygiene at Scale

AWS says more than 600 FortiGate firewalls hit in AI-augmented campaign

Off-the-shelf tools helped Russian-speaking cybercrime group run riot

Carly Page — Mon 23 Feb 2026 // 11:41 UTC

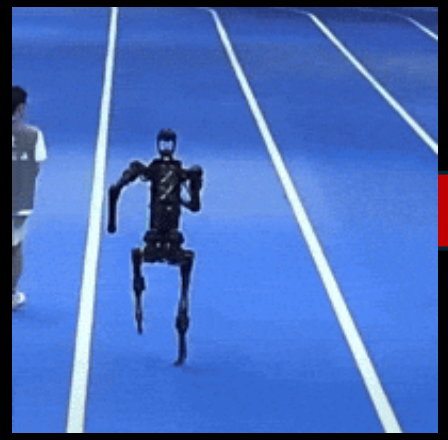
- Cybercriminals armed with off-the-shelf generative AI tools
- Compromised more than 600 internet-exposed FortiGate firewalls across 55 countries in just over a month



Integrity360
your security in mind

SECURITY FIRST

What's next, where to?



Not that long ago

Now

Soon?


Integrity360
your security in mind
SECURITY
FIRST
2. Human-AI Collaboration

Human in the loop

AI Analyst

Alert Handling
Triage, Prioritisation, Noise Reduction

Analyst Assistant
Natural Language Investigation Support, Guided Investigation Paths

Response
Execute low-risk, time-bound and reversible actions. Recommends other actions

Proactive Security
Help defenders move left of boom

Human Analyst

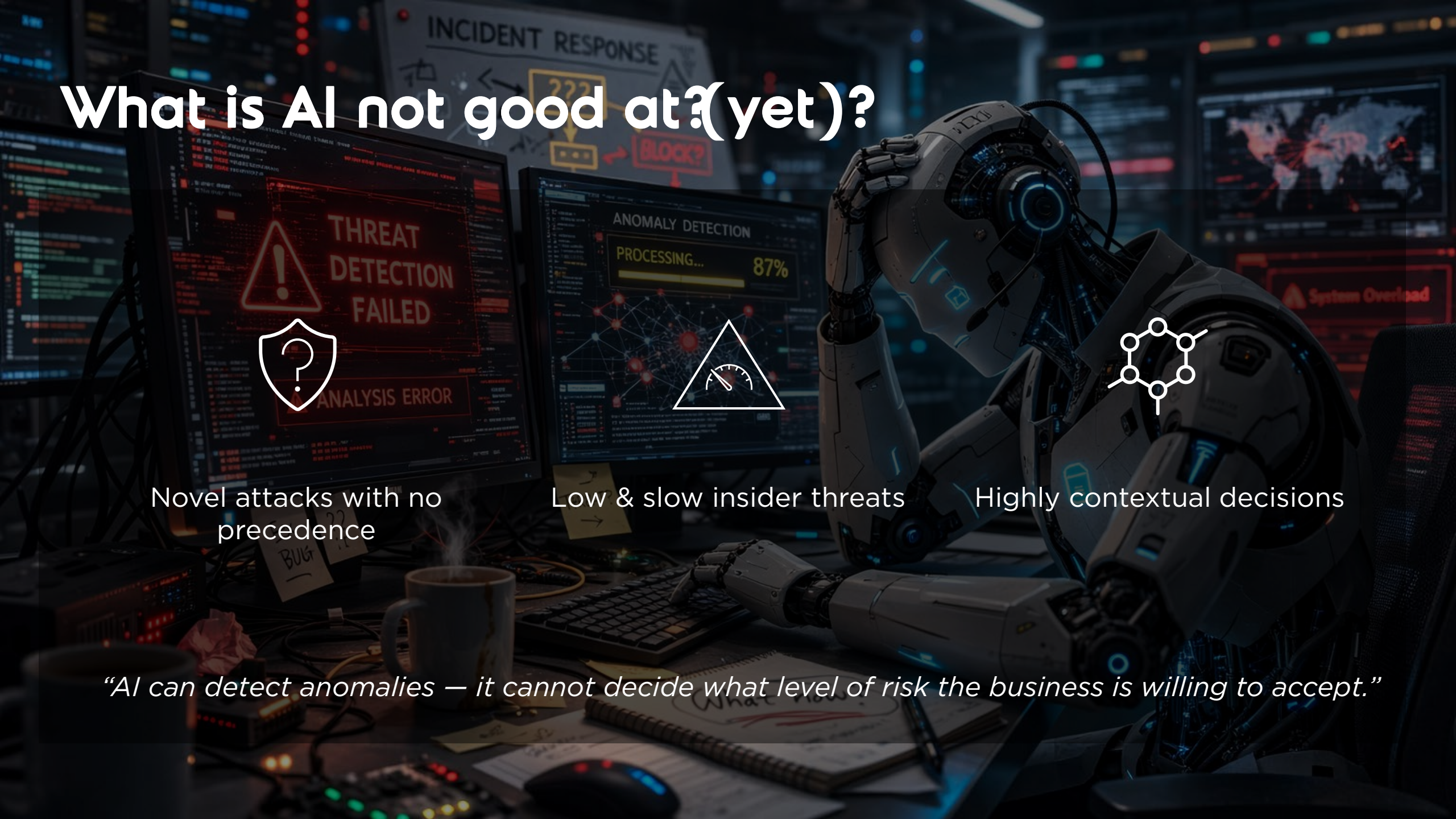
Alert Handling
Validating prioritisation, applying business context, escalation & response strategy

Analyst Assistant
Reduced Cognitive Load, Extended Skillset

Response
Reviews and approves actions

Proactive Security
Decide what risk is, balance security with operational friction

What is AI not good at?(yet)?



Novel attacks with no precedence

Low & slow insider threats

Highly contextual decisions

“AI can detect anomalies — it cannot decide what level of risk the business is willing to accept.”

Integrity360
your security in mind

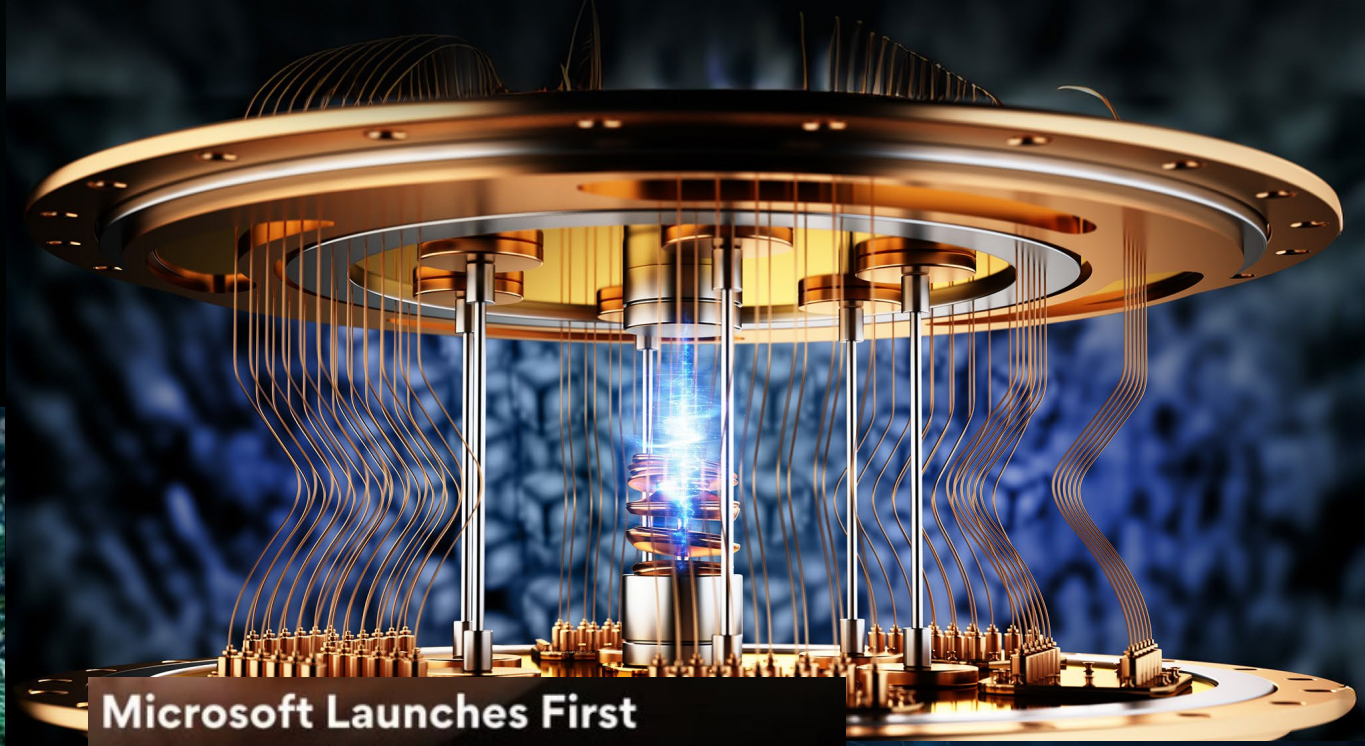
SECURITY FIRST

3. Post-quantum cryptography

Q-DAY

THE DAY ENCRYPTION FAILS

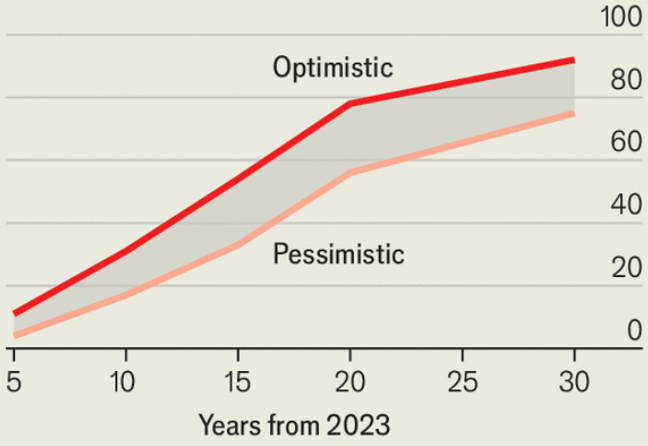
GOOGLE UNVEILS QUANTUM CHIP THAT SOLVES 10-BILLION-YEAR PROBLEMS IN MINUTES



Microsoft Launches First Quantum Chip 'Majorana 1' After 20 Years Of Research, Is Powerful Than Every Other Computer!

A matter of time

Estimates of the likelihood of a digital quantum computer able to factorise RSA-2048 in 24 hours within timeframe*, %



Source: Global Risk Institute *Survey of 37 experts, 2023

Will quantum computers disrupt critical infrastructure?

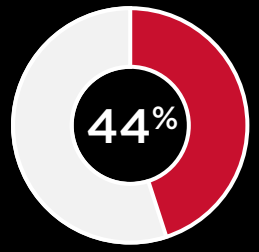

Integrity360
your security in mind
SECURITY
FIRST
AI IS THE ULTIMATE...
4. Third Party Risk


Employees Misusing Public AI tools
3rd party providers using AI
AI Supply chain risks
3rd party Applications developed insecurely with AI
3rd party apps infused with AI
Internal AI Agents connecting to external services

Integrity360
your security in mind

SECURITY FIRST

Bringing Third-Party Cyber Risk Management to Cyber Resilience



Of organisations don't consider third parties when conducting business continuity exercises

Planning

- ✓ Disaster Scenarios
- ✓ Roles and Responsibilities
- ✓ Key contacts and comms channels
- ✓ Architect to meet recovery objectives

Testing

- ✓ Prioritise critical tiers
- ✓ Cadence – annual/biannual
- ✓ Scope based on risk priorities
- ✓ Roles and Responsibilities
- ✓ Findings and Recommendations

Integrity360
your security in mind

SECURITY FIRST

Use how AI is Transforming 3rd Party Risk Management

Predictive Risk Monitoring

Automation & Efficiency

Extended Ecosystem Visibility


Integrity360
your security in mind
SECURITY
FIRST
5. Recovery and Continuity

Integrity360
your security in mind

SECURITY FIRST

Cybersecurity:

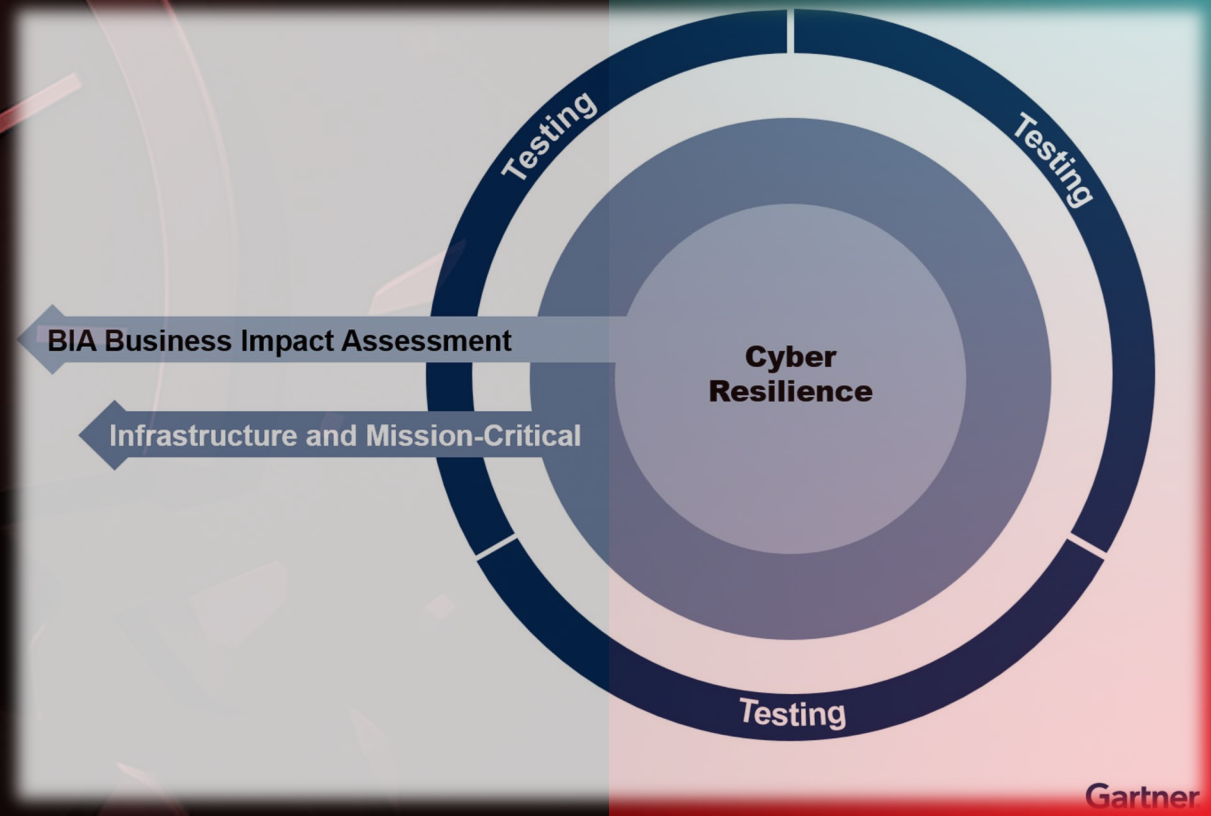
"We must prevent breaches from happening"

Integrity360
your security in mind

SECURITY FIRST

Embed Business Impact Assessment as the Foundation of Cyber Resilience

"...to focus protection on critical business processes and assets, rather than pursuing blanket coverage."



Source: Gartner - Unlock Cyber Resilience: Build Your Program on BIA Foundations

Key Metrics

Recovery Time Objective (RTO)	Recovery Point Objective (RPO)
Maximum Tolerable Downtime (MTD)	Mean Time to Recover (MTTR)

Integrity360
your security in mind

Microsoft Azure Outage Disrupts Global Services Across Cloud and Productivity Platforms

Microsoft admits it 'cannot guarantee' data sovereignty

France pulls millions of medical records out of the Microsoft cloud over privacy concerns

Concerns over US legislation that gives American companies access to data stored in Europe were the trigger for this change

Europe's digital reliance on US Big Tech: Does the EU have a plan?

POLITICO.eu

Trump can pull the plug on the internet, and Europe can't do anything about it

Donald Trump's return to the White House is forcing Europe to reckon with a major digital vulnerability: The US holds a kill switch over its internet.

What the CLOUD Act Really Means for EU Data Sovereignty

The CLOUD Act allows U.S. authorities to access data stored in the EU, putting it in direct conflict with GDPR. Learn how this impacts data sovereignty and what EU businesses can do to stay compliant

AWS' 15-Hour Outage: 5 Big AI, DNS, EC2 And Data Center Keys To Know

Integrity360
your security in mind

SECURITY FIRST

Top Considerations how AI impacts recovery and continuity

Integrity360
your security in mind

SECURITY FIRST

ANTIFRAGILE
THINGS THAT GAIN FROM DISORDER

Cyber Resilience:

Surviving and becoming stronger

- Anticipate
- Withstand
- Recover from
- Adapt to

Integrity360
your security in mind

SECURITY FIRST

Conclusion

Resilience Redefined in the Human-AI Era is...(cue drumroll)

Integrity360
your security in mind

SECURITY FIRST

5 Key Factors redefining resilience in the Human-AI era

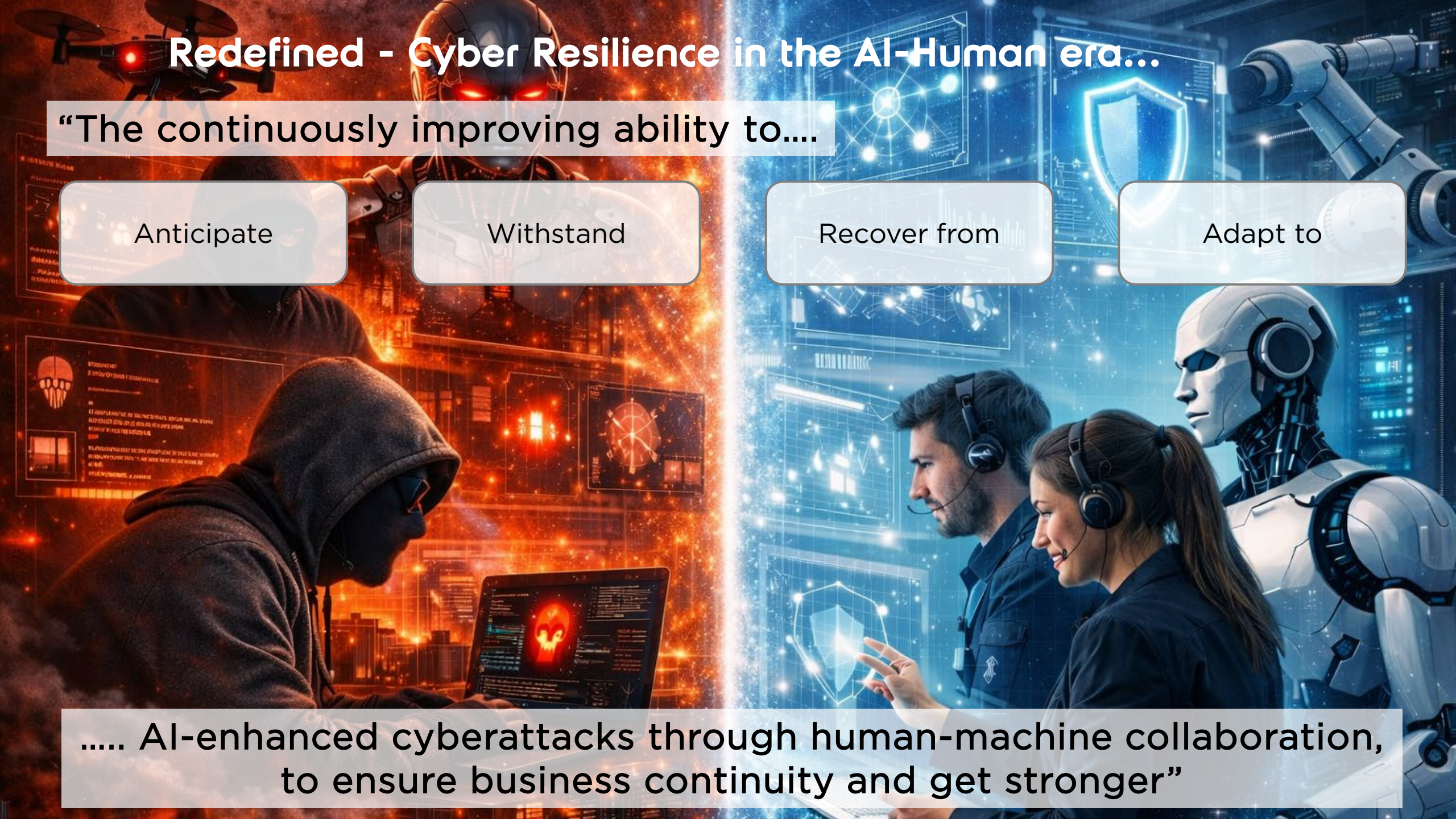
Anticipate

Withstand

Recover from

Adapt to

Redefined - Cyber Resilience in the AI-Human era…



"The continuously improving ability to….

- Anticipate
- Withstand
- Recover from
- Adapt to

….. AI-enhanced cyberattacks through human-machine collaboration, to ensure business continuity and get stronger"

Redefined - Cyber Resilience in the AI-Human era…

"The continuously improving ability to….

- Anticipate
- Withstand
- Recover from
- Adapt to

….. AI-enhanced cyberattacks through human-machine collaboration, to ensure business continuity, and get ever-stronger"

Integrity360
your security in mind

SECURITY FIRST

Thank you

Richard Ford
Richard.ford@integrity360.com

Brian Martin
Brian.martin@integrity360.com

Integrity360
your security in mind

SECURITY FIRST

Client Panel: Building a security culture that can thrive with AI

Shabeer Ramsingh

Global Head - Strategic Business Development, Integrity360

Kiran Deosingh

Vice President of Technology, RAMPS Logistics

Shivanand Persad

Senior Manager - Enterprise Information Security, First Citizens

#SecurityFirst2026

Integrity360
your security in mind

SECURITY FIRST

How to Succeed When Every Day is Zero-DAI

Joe Viviano

Senior Account Executive,
Darktrace

DARKTRACE

#SecurityFirst2026

DARKTRACE

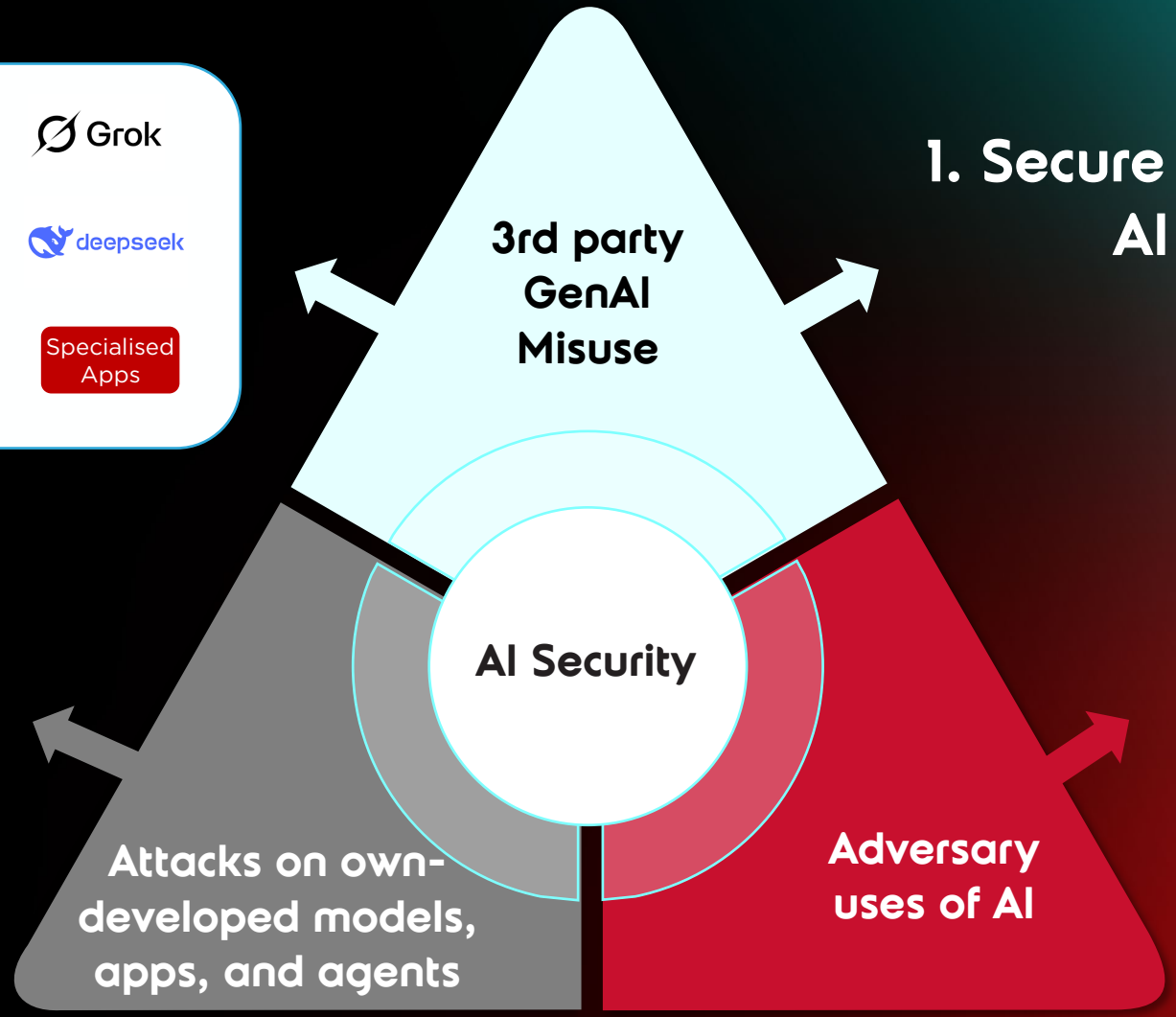
How to Succeed When Every Day is Zero-DAI

As AI created Zero-Day Attacks become the norm, only AI powered defenses can protect us.

Jack B. Miller, Vice President & Field CISO
https://www.linkedin.com/in/jack-m-03a72637/

AI Security - New Threats and Risks

ChatGPT
Microsoft Copilot
Gemini
Grok
Claude
Meta AI
perplexity
deepseek
GitHub Copilot
Embedded GenAI
Long Tail Apps
Specialised Apps



1. Secure Use of AI

2. Secure own AI

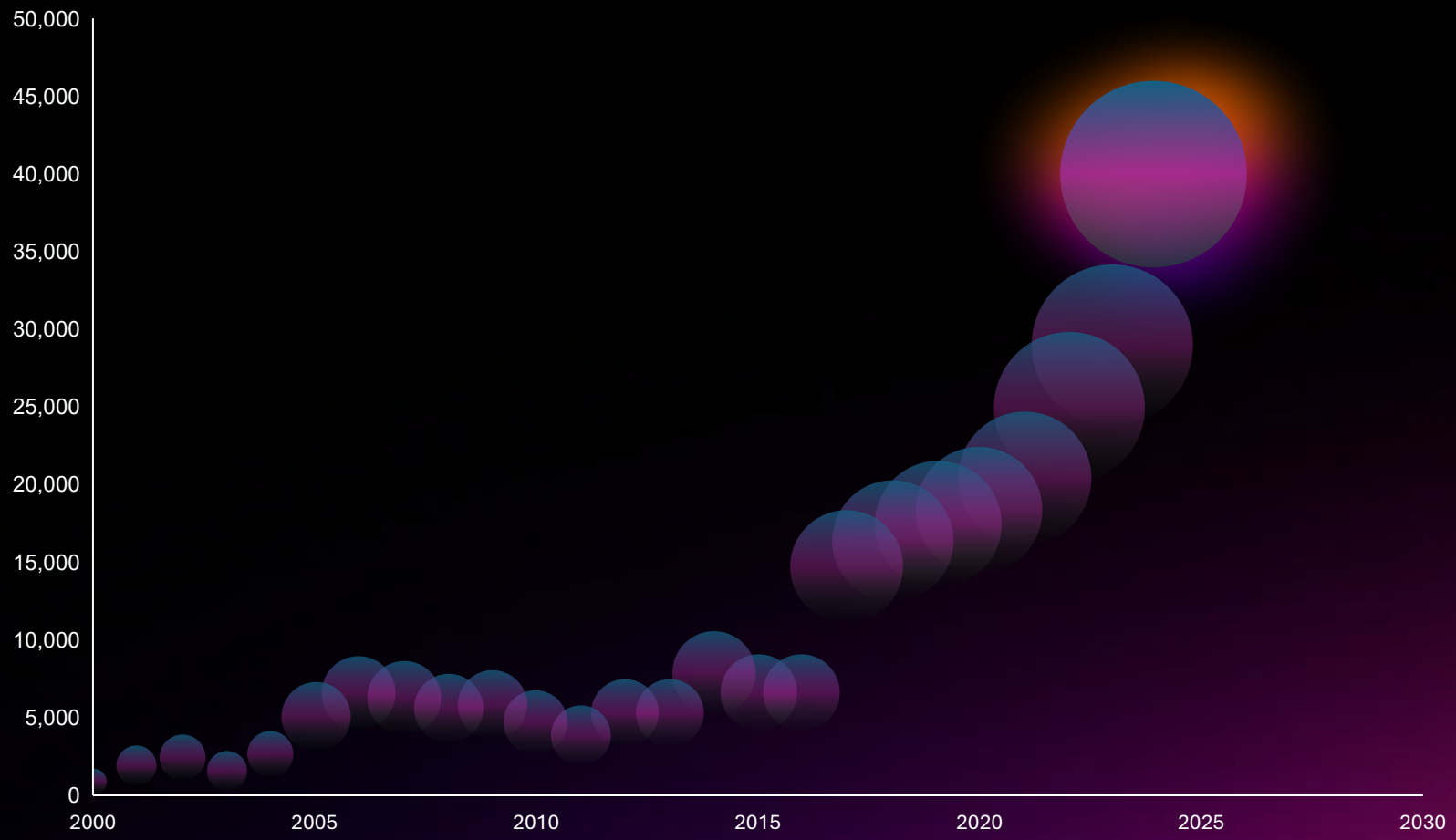
3. Secure against AI

Attackers Choice - Zero-DAI Every Day

1. Not Protected
   - The average time between discovery and patch is 22 days
   - The average time to weaponization is 5 days
   - 25% of Zero-Days are weaponized within 24 hours
   - The average lifespan of a Zero-Day vulnerability before public disclosure is 7 years
2. Difficult To Detect
   - The detection rate for leading security tools is less than 30%
   - IOA, Threat Intel, Hash/Signature & IOC based tools can’t adequately detect & respond
3. Enormous Attack Surface
   - 75% of exploited Zero-Days target Microsoft, Apple or Google

CVE Explosion

Over 40,000 CVEs Published in 2024



15.2%

- **Of all CVEs were identified in 2024 alone**
- **AI Bug Hunter sets milestone by claiming top spot on HackerOne's leaderboard**

So Why Haven’t We All Been Compromised?

- Zero-Day Attacks Are Rare
  - Nation-state actors are responsible for over 80% of zero-day exploit usage
  - Zero-day prices on the dark web range from $60,000 to $2.5 million
- But Times Are Changing
  - Attackers are using AI to quickly identify vulnerabilities and create exploit code
  - *Prediction* - Majority of attacks will be Zero-Day attacks
  - *Prediction* - Zero-Day attacks will be automated & continuous
- Defend With AI Detection & Response (AIDR)

1. Detect the unknown
2. Investigate at wire speed
3. Minimize the impact

Detecting the Unknown Requires The Right Type of AI

	Generative AI & LLMs	**Attacker-Centric** Supervised machine learning	**Business-Centric** Unsupervised machine learning
Data	▪ Internet ▪ Data Lakes and indexed repositories	▪ Known attack patterns ▪ Threat intelligence & research	▪ Unstructured business centric data ▪ Organization-specific behaviors and patterns
Models	▪ Pre-trained and feedback from users	▪ Pre-trained/static data, retrained	▪ Continuously learning
Common Use Case	▪ Context of language, media, audio ▪ Content summarization ▪ Content generation	▪ Known attacks and variants ▪ Content summarization ▪ Simulation	▪ Known, unknown, novel attacks ▪ Abuses, misuses, misconfigurations ▪ Simulates attacks and analyzes relationships
Implication	▪ Cannot detect attacks ▪ Confirmation bias & hallucination challenges	▪ Cannot detect novel/insider attacks ▪ Exhaustive data integrity process	▪ Requires compounding of ML models for accurate results

No Zero-Day Detection

Limited Zero-Day Detection

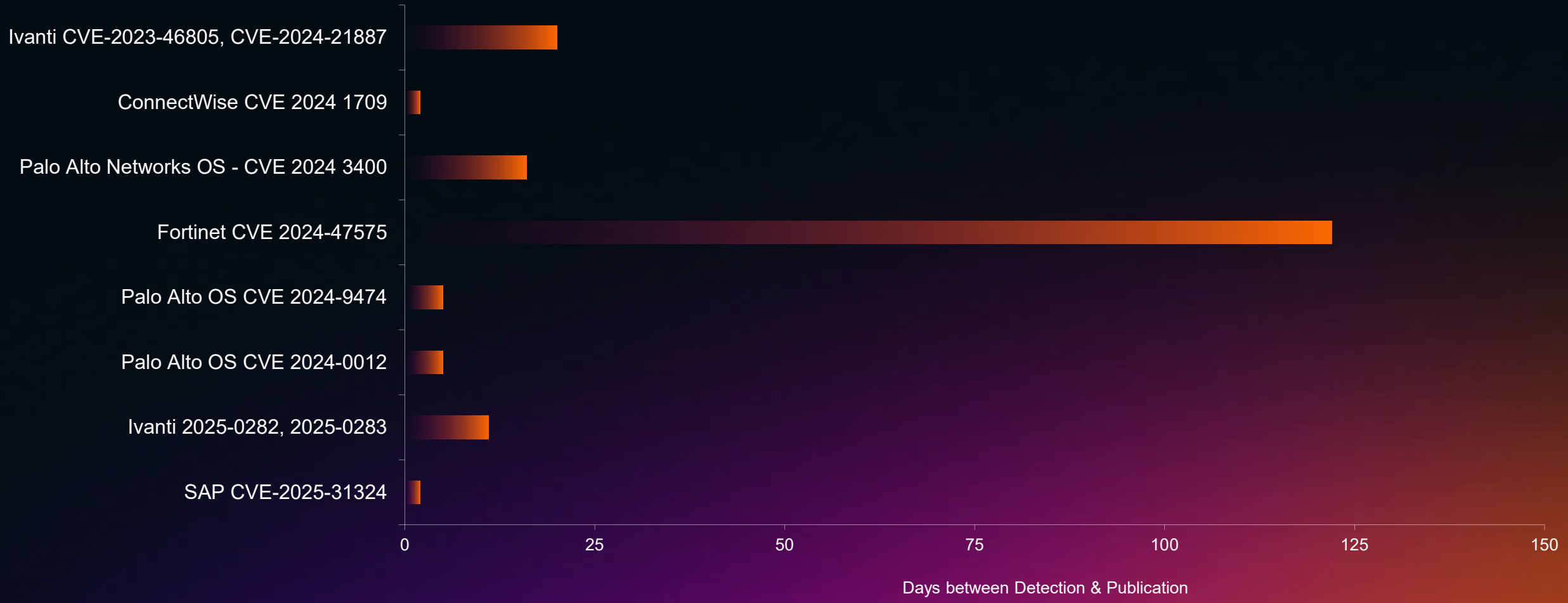
Zero-Day Detection

While Every Anomaly Isn't An Attack, Every Attack Creates Anomalies

Caution – Use Learning Exceptions Instead of Whitelists

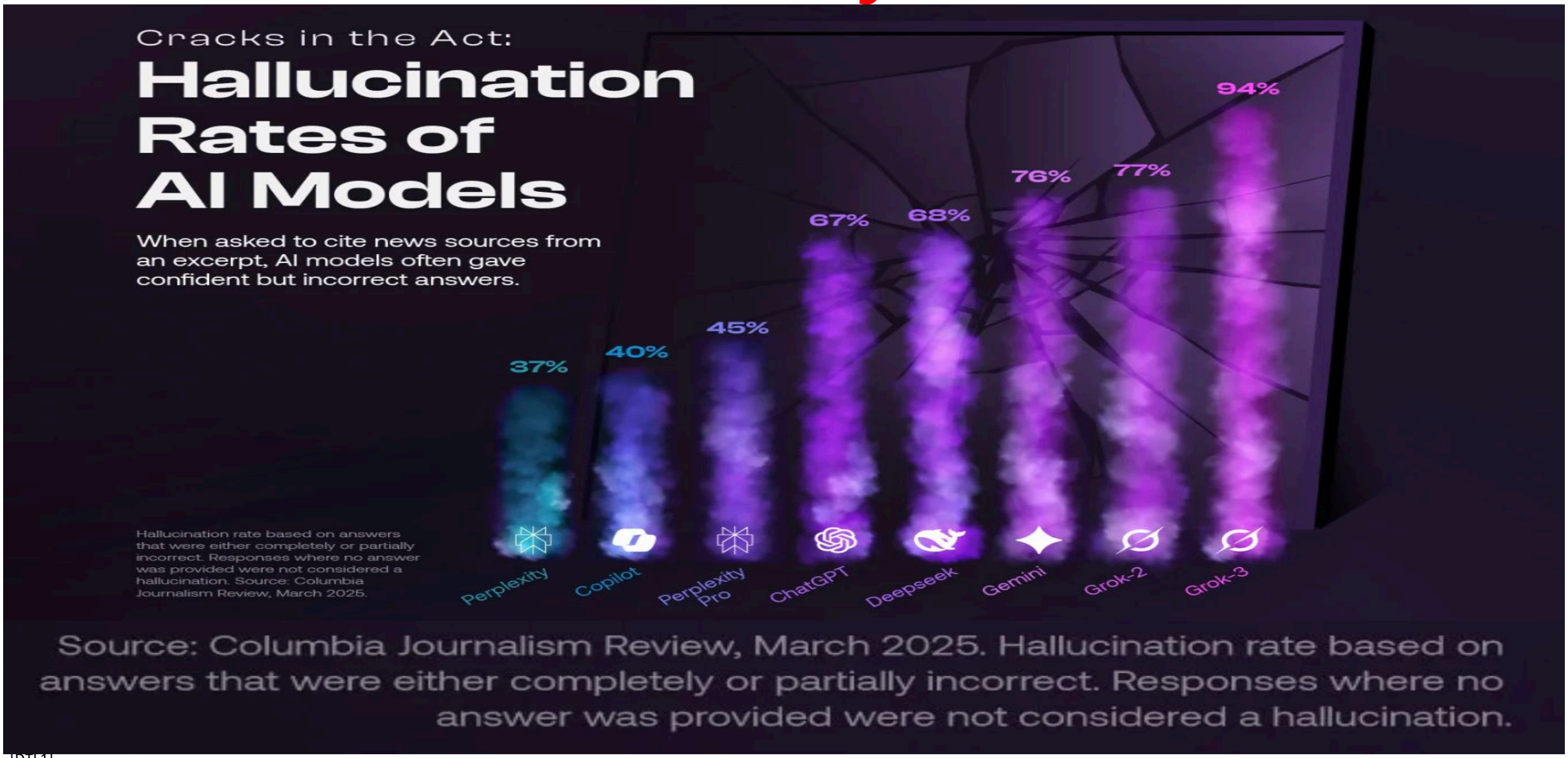
Examples of Business-Centric AI Detecting Zero-Days

Before CVE Disclosure



[DTL1]

Caution - Don’t Rely on AI Search



[DTL1]

Investigate At Wire Speed with AI SOC Analysts

- 181 days is the average time to identify a breach in 2025
- 24x7 cross-vector event investigations
- Process enormous amounts a data in real-time
- Eliminate False Positive vs False Negative conundrum
- Continuously digest new data and correlate with old data
- Learn new data and relationships on the fly
- Supervised Machine Learning, Unsupervised Machine Learning & Generative AI

Minimize Impact With AI Powered Response

- 60 days is the average time to contain a breach in 2025
- Real-time 24x7 cross-vector autonomous response
- Surgical
- Configurable thresholds for manual & automated activities
- Trustworthy - Total visibility and explainability for all activities
- Easy rollback
- Automated forensic acquisition and analysis

DARKTRACE

2024
Microsoft Partner of the Year (UK)

9800+
Active Customers in 110+ countries

#200+
Patents and Applications Filed

HQ
Cambridge, UK
34 offices worldwide

2300+
Employees Worldwide

843 . 8
Million ARR USD (31 March 2025)

Technology
Governments
Healthcare
Global Retailers
Financial & Insurance
Critical Infrastructure
Telecommunications

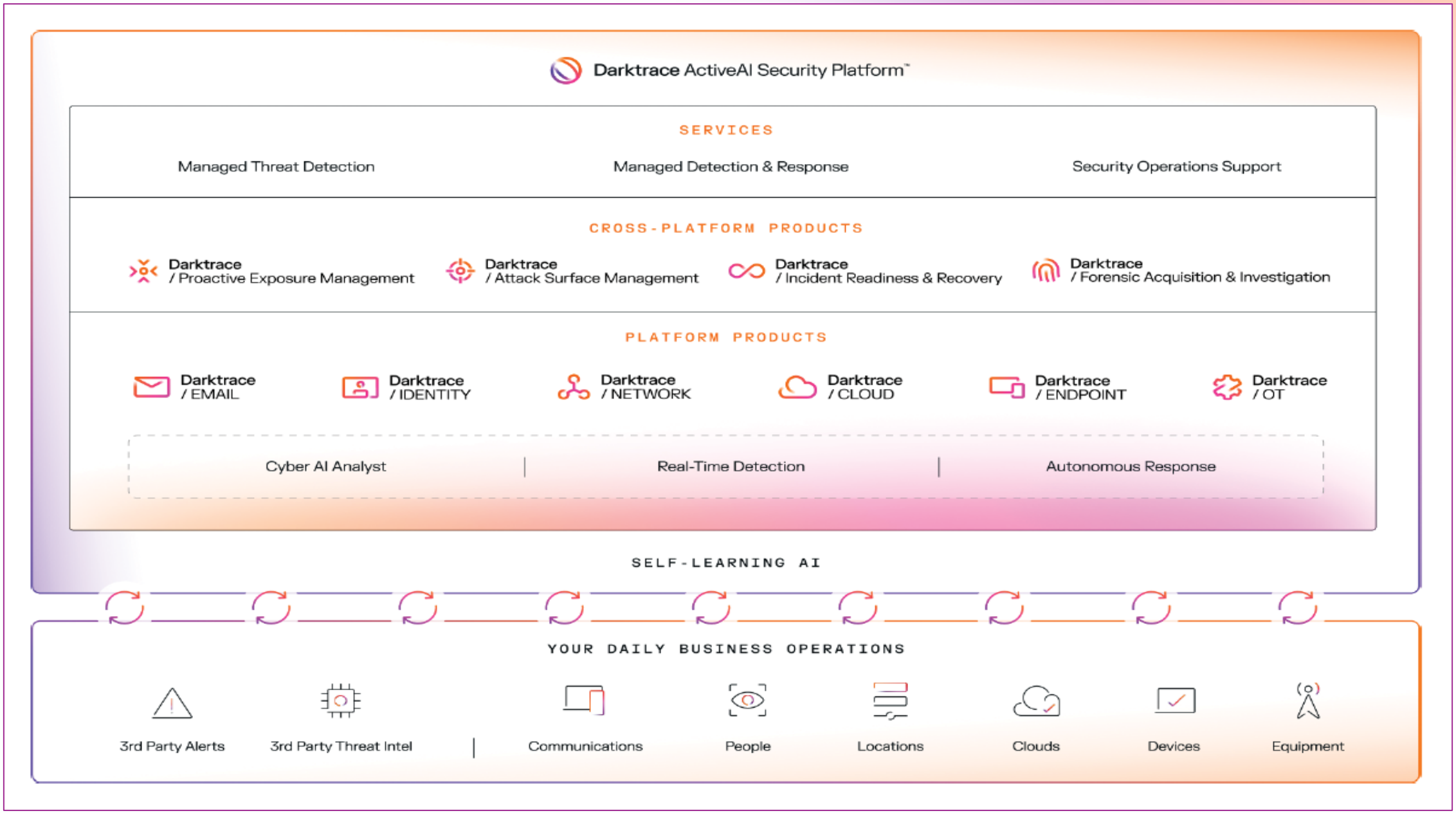
2021 GLOBEE AWARDS GOLD WINNER CYBER SECURITY GLOBAL EXCELLENCE AWARDS

PEER AWARD 2021 Darktrace

TIME 100 MOST INFLUENTIAL COMPANIES 2021

Microsoft 2024 Partner of the Year Winner United Kingdom

[DTL1]


Darktrace ActiveAI Security Platform™
SERVICES
Managed Threat Detection
Managed Detection & Response
Security Operations Support
CROSS-PLATFORM PRODUCTS
Darktrace / Proactive Exposure Management
Darktrace / Attack Surface Management
Darktrace / Incident Readiness & Recovery
Darktrace / Forensic Acquisition & Investigation
PLATFORM PRODUCTS
Darktrace / EMAIL
Darktrace / IDENTITY
Darktrace / NETWORK
Darktrace / CLOUD
Darktrace / ENDPOINT
Darktrace / OT
Cyber AI Analyst
Real-Time Detection
Autonomous Response
SELF-LEARNING AI
YOUR DAILY BUSINESS OPERATIONS
3rd Party Alerts
3rd Party Threat Intel
Communications
People
Locations
Clouds
Devices
Equipment

[DTL1]

Microsoft Partnership

- **UK Microsoft Partner of the Year 2024**
- Multiple awards
  - ‘Security Trailblazer’ Finalist – Microsoft Intelligent Security Association
  - Microsoft UK partner of the year 2024
- Continuous collaboration between Darktrace & MSFT developers
- Executive sponsorship from Nicole Dezen, CVP Microsoft Partner Ecosystem
- Darktrace available on Azure marketplace, including the ability to use MSFT MACC (committed spend) towards Darktrace coverage

[DTL1]

Integrity360
your security in mind

SECURITY FIRST

Thank you

Joe Viviano
joe.viviano@darktrace.com
DARKTRACE

[DTL1]

Integrity360
your security in mind

SECURITY FIRST

Keeping the Lights On: Defending CPS and Critical Infrastructure in the AI Era

An Nguyen

Director of Operational Technology Practice, Integrity360

Emil Olofsson

Regional Head of Solution Architecture, Integrity360

Emmanuel A. Oscar

Sr. Systems Engineering Manager, Fortinet

Glen R. Singh

CIO, Water and Sewerage Authority - Trinidad and Tobago

#SecurityFirst2026

Integrity360
your security in mind

SECURITY FIRST

AI in the SOC: Turning Intelligence into Resilience

Emil Olofsson

Regional Head of Solution Architecture, Integrity360

Saresh Sewraj

Solution Architect, Integrity360

Vicente Amozurrutia

Enterprise Account Executive, SentinelOne

Mike Dalgleish

Area Sales Vice President, Vectra AI

Surendra Singh

Information Security Manager, Infolink Services Limited

#SecurityFirst2026

Integrity360
your security in mind

SECURITY FIRST

Networks without borders: Trust nothing, verify everything

Brian Martin

Director of Product Management, Integrity360

Saresh Sewraj

Solution Architect, Integrity360

Gabriel Garcia

IT Manager, CARPHA

Rick Logan-Stanford

Team Lead – Infrastructure, Policies and Legislation, Government of the Republic of Trinidad & Tobago

#SecurityFirst2026

Integrity360
your security in mind

SECURITY FIRST

Q-Day and beyond: Building resilience for the Quantum age

Richard Ford

CTO, Integrity360

Captain Donovan Smith

Chief Technology Officer, City of Bridgetown Credit Union

#SecurityFirst2026

Integrity360
your security in mind

SECURITY FIRST

Q&A with special guest: Dalton Grant

Richard Ford
CTO, Integrity360

Dalton Grant
Three-Time Olympian

#SecurityFirst2026

Integrity360
your security in mind

SECURITY FIRST

Conference wrap up

FEEDBACK