ISACA Central & SASIG Leadership Conference

Thursday 16 July 2026

Chair

Liz Murray
Chief of Staff, The SASIG

Host

Raj Atwal
President, ISACA Central UK

House rules

Respect others
The Chatham House Rule must be universally respected – please do not attribute anything shared today. Phones should also be turned to silent, though you are free to leave the room for calls if needed.

Take part
We welcome questions or comments – don't forget to introduce yourself when you join the conversation. Be sure to make five new friends throughout the day, too!

Get involved
Fancy taking to the stage yourself? Speak to the team or drop us an email. Don't forget to follow us on LinkedIn and share SASIG with your colleagues, too.

Upcoming webinars

Agentic SOCs in the age of Mythos - What it means for Vulnerability Management
11am, Friday 17 July

Fighting Financial Fraud (F3): Insight into a Collaborative Framework
11am, Tuesday 21 July

What's Hiding in Your Microsoft 365 Tenant Could Derail Your AI Plans
11am, Wednesday 22 July

Live from Black Hat, what is the Current State of Security Executive Hiring?
3pm, Wednesday 5 August

View the full calendar at www.thesasig.com/events

Upcoming in-person events

Scotland SASIG
Tuesday 22 September, Edinburgh

Cybersecurity Awareness SASIG
Thursday 8 October, London

Emerging Technologies
Tuesday 13 October, London

ISACA Central & SASIG SheLeadsTech
Wednesday 14 October, Birmingham

View the full calendar at www.thesasig.com/events

Where will cyber leaders be this September?

bigsasig

The flagship conference from SASIG Events

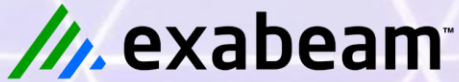
Wednesday 9 September, Central London

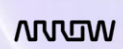
Apply to attend today to avoid disappointment...

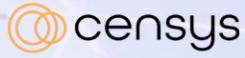
bigsasig.com

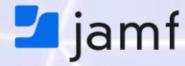
Our Supporters and Contributors

A special thanks to our Supporters, Contributors and all the speakers who share their expertise with us.









Have you got a minute?

We’d appreciate your feedback

Let us know what you thought of today’s event as well as any ideas you have for future SASIG events, using our short survey or commenting on our LinkedIn post.

We’ll display the below QR code on screen throughout the day which will be live at 11.30am – we’d be very grateful if you would share your views.

ISACA Central & SASIG Leadership Conference

Thursday 16 July 2026

Chair

Liz Murray
Chief of Staff, The SASIG

Host

Raj Atwal
President, ISACA Central UK

Cyber Resilience in the Boardroom: From Risk Awareness to Strategic Advantage

Jack Harrigan
Head of Cyber Governance Policy, DSIT

Department for Science, Innovation & Technology

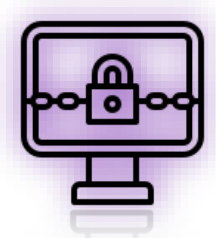
CYBER IN THE BOARDROOM: FROM RISK AWARENESS TO STRATEGIC ADVANTAGE

Jack Harrigan

Department for Science, Innovation and Technology

OPPORTUNITIES AND THREATS

Department for Science, Innovation & Technology



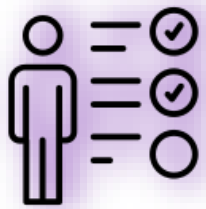
£14.7bn annual estimated cost of cyber attacks in the UK

Attacks on public services and private companies

Increasing reliance on internet-connected technology

World leading cyber sector

Cyber is borderless



Cyber skills gap

Need for trusted and secure digital identities

AI-ENABLED THREATS

Department for Science, Innovation & Technology

GOV·UK Menu

Home > Government > Cyber security > AI cyber threats: open letter to business leaders

Department for Science, Innovation & Technology | Cabinet Office

Correspondence

AI cyber threats: open letter to business leaders (HTML)

Updated 22 April 2026

The Rt Hon Liz Kendall MP
Secretary of State for Science, Innovation and Technology
22-26 Whitehall
London
SW1A 2EG

The Rt Hon Dan Jarvis MP
Minister of State for the Cabinet Office
70 Whitehall
London
SW1A 2AS

15 April 2026

Dear business leaders,

Open letter to businesses on AI cyber threats

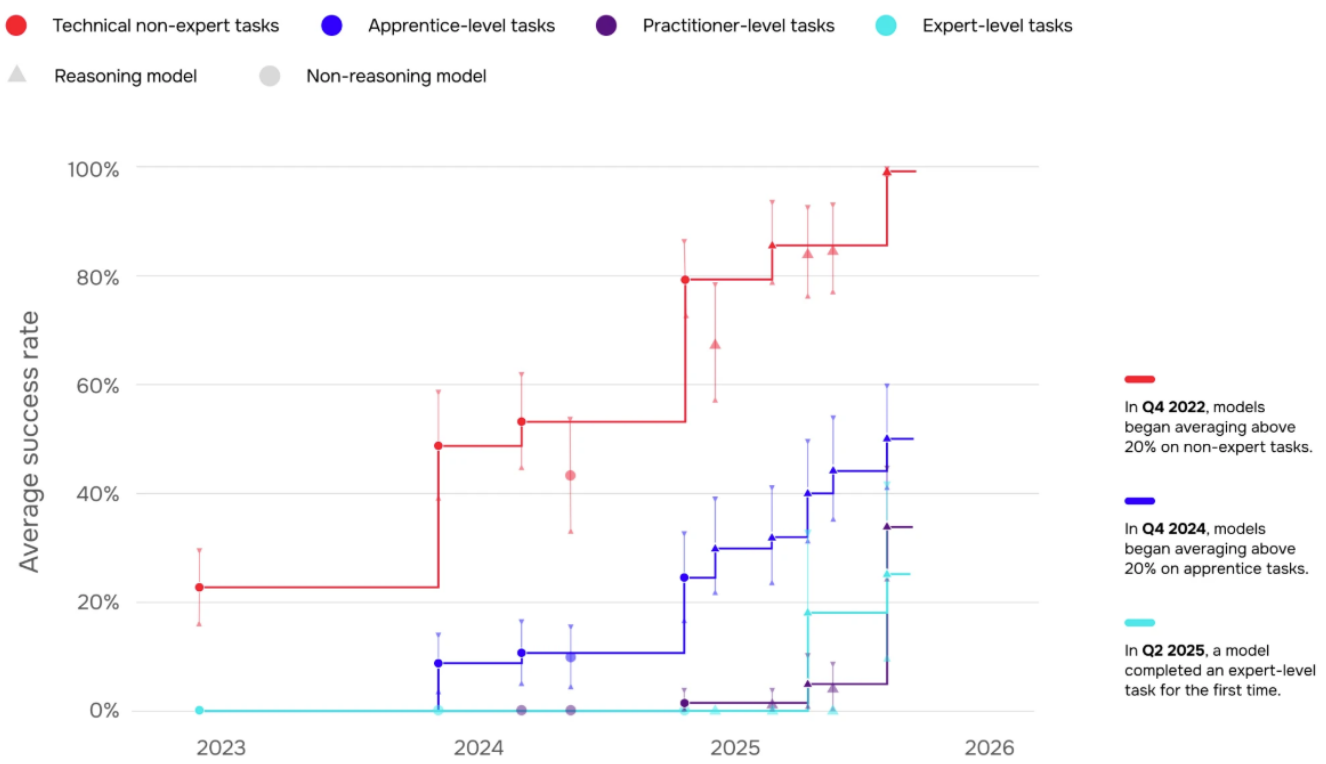
We are writing to you because the threat your business faces in cyber space is changing, and the way we respond must change with it.

For years, the most serious cyber attacks have relied on a small number of highly skilled criminals. That is now shifting. A new generation of AI models are becoming capable of doing work that previously required rare expertise: finding weaknesses in software, writing the code to exploit them, and doing so at a speed and scale that would have

AISI AI SECURITY INSTITUTE

AI models perform cyber tasks as well as technical non-experts, and are steadily improving

Source: UK AI Security Institute



DSIT CYBER POLICY LANDSCAPE

Department for Science, Innovation & Technology

DSIT is taking action to increase the resilience of organisations and ensure that new and existing technologies are safely developed and deployed across the UK.

SECURE ORGANISATIONS

- Cyber Essentials
- Cyber Governance
- Cyber Resilience Pledge
- Cyber Security and Resilience Bill

SECURE TECHNOLOGY

- Enterprise IoT & OT
- AI cyber security
- Software Security
- Apps & app stores
- Product Security (&TI) Act
- Secure microprocessors
- Emerging Technologies

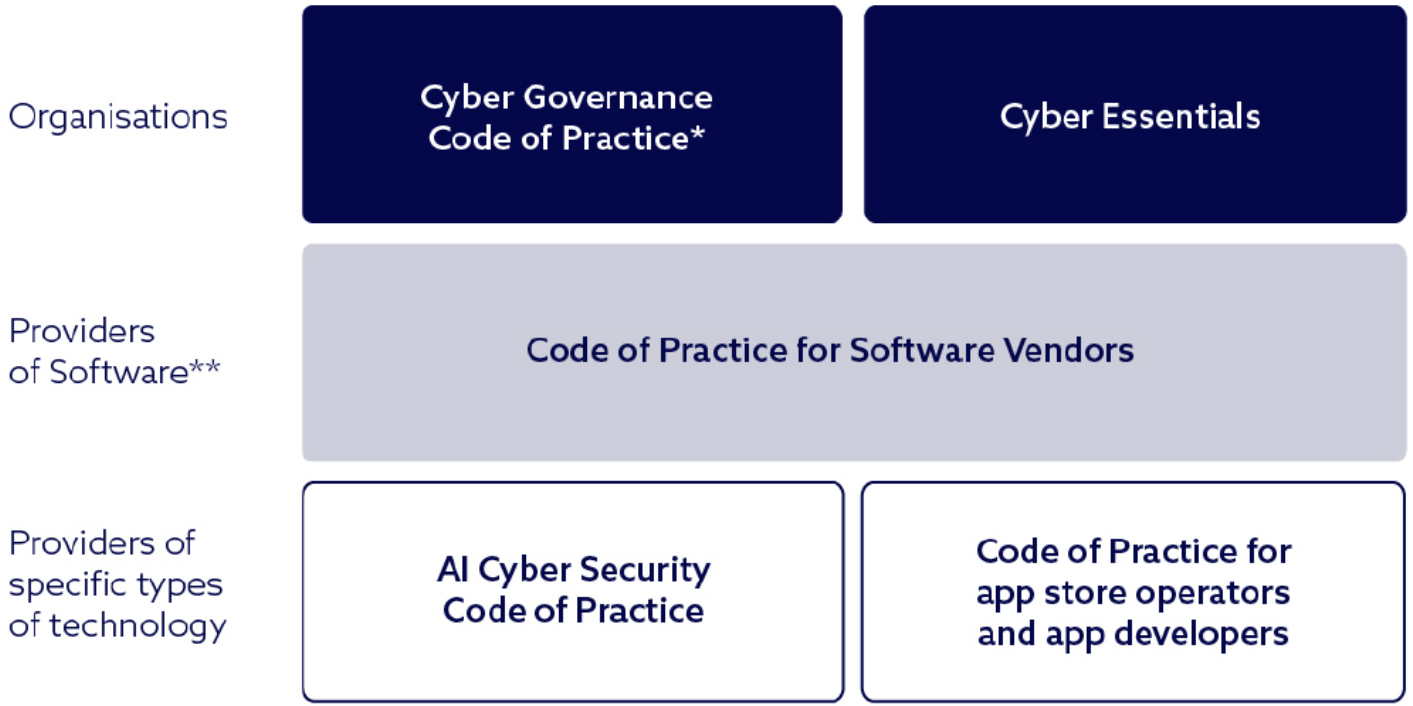
GROWING THE SECTOR AND RAISING SKILLS

- Cyber Business Accelerators
- Cyber Growth Hubs
- Cyber First / Tech First
- UK Cyber Security Council

MODULAR APPROACH TO CYBER SECURITY

Department for Science, Innovation & Technology

This diagram shows how the five cyber security codes of practice apply to different organisations and technologies.



*for medium and large organisations, as well as small tech/AI organisations
**including goods and services that contain software

RECENT ACTION TAKEN

Department for Science, Innovation & Technology

Cyber Security and Resilience Bill

- Strengthening essential and digital services

Collaboration with standard-setters

- FRC, ICO & GBC

Ministerial letters to industry

- On AI risk, actions for small organisations and entrepreneurs and actions for medium and large organisations

Launch of the Cyber Resilience Pledge

- The UK's leading companies pledging to strengthen their resilience and that of their supply chain

THE CYBER SECURITY AND RESILIENCE BILL

Department for Science, Innovation & Technology

The Bill will increase UK defences against cyber attacks and underpin greater economic stability.

Expanded scope

The existing regime (NIS Regulations 2018) covers OESs and some digital services. The Bill will bring more organisations in scope to enhance cyber security of services critical to the economy and their supply chains.

1. **Managed service providers**
2. **Designation of critical suppliers**
3. **Data centres**
4. **Large load controllers**

Effective regulators

The Bill will enable cyber regulators to be more effective in supporting organisations, with more information on harmful cyber attacks, and working with government on priority outcomes.

5. **Incident reporting**
6. **Cost recovery**
7. **Information sharing**
8. **Statement of strategic priorities**
9. **Enforcement**

Enabling resilience

The Bill will give Government the tools to strengthen our cyber security and resilience in response to the ever-changing threat landscape and imminent threats.

10. **Future-proofing**
11. **Powers of direction**

Department for Science, Innovation & Technology

CYBER RESILIENCE: ROLE OF BOARDS AND DIRECTORS

Directors have a dual challenge of:

- Driving the business strategy to avoid being left behind in the race to digitise; and
- Dealing with the increased exposure to cyber-attack that technological dependency brings.

Department for Science, Innovation & Technology

STATE OF PLAY

31%

Of businesses surveyed had a board member with responsibility for cyber security, down from 38% in 2021 (Cyber Security Breaches Survey, 2026).

57%

Of medium and 70% of large businesses surveyed **have a formal cyber security strategy** in place (CSBS, 2026).

57%

Just over half of medium businesses surveyed have a **formal incident response plan** in place, rising to 76% for large businesses (CSBS, 2026).

62%

Of medium and 72% of large businesses surveyed, **had undertaken a cyber security risk assessment** in the last year. (CSBS, 2026).

CYBER GOVERNANCE CODE OF PRACTICE

Department for Science, Innovation & Technology

The Code

The principles focus on the most critical areas that directors must engage with, rather than being an exhaustive list, and will articulate specific actions against:

- **Principle A:** Risk management
- **Principle B:** Strategy
- **Principle C:** People
- **Principle D:** Incident planning, response and recovery
- **Principle E:** Assurance and oversight

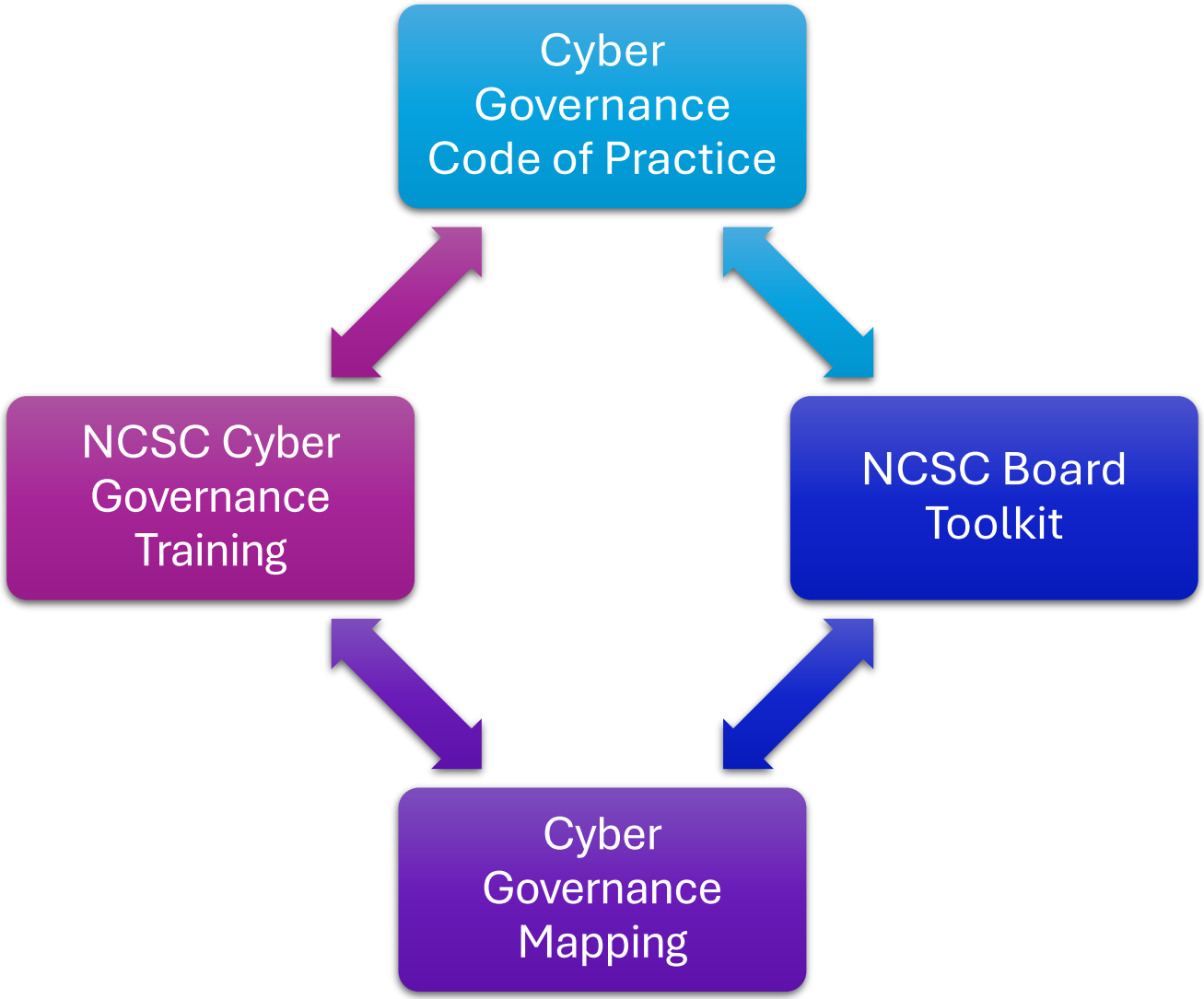
PRINCIPLES AND ACTIONS

Department for Science, Innovation & Technology

Principle	Action
A – Risk management	1.Gain assurance that the technology processes, information and services critical to the organisation's objectives have been identified, prioritised and agreed
B – Strategy	1.Gain assurance that the organisation has developed a cyber strategy and this is aligned with, and embedded within, the wider organisational strategy.
C - People	3.Undertake training to improve your own cyber literacy and take responsibility for the security of the data and digital assets that you use
D – Incident planning, response and recovery	1.Gain assurance that the organisation has a plan to respond to and recover from a cyber incident impacting business critical technology processes, information and services
E – Assurance and oversight	4. Gain assurance that cyber security considerations (including the actions in this code) are integrated and consistent with existing internal and external audit and assurance mechanisms

CYBER GOVERNANCE PACKAGE

Department for Science, Innovation & Technology



MINISTERIAL LETTER

Department for Science, Innovation & Technology

An invitation for organisations to undertake three key actions to improve the cyber resilience of the UK.

- Make cyber risk a Board-level priority using the Cyber Governance Code of Practice
- Sign up to the NCSC's Early Warning service
- Require Cyber Essentials in your supply chain

POSITIVE INDUSTRY RESPONSE

180+ organisations responded

Engagement from **CEOs and Chairs**

Commitments from organisations to take actions

Department for Science, Innovation & Technology | NCSC | Cabinet Office | HM Treasury | National Crime Agency

Department for Business & Trade

Correspondence

Ministerial letter on cyber security

Updated 14 October 2025

70 Whitehall
London
SW1A 2AS

13 October 2025

Dear CEO / Chair,

Making cyber security a board responsibility

Hostile cyber activity in the UK is growing more intense, frequent and sophisticated. This is causing significant financial and social harm to UK businesses and citizens. There is a direct and active threat to our economic and national security which requires an urgent collective response.

The government is taking significant action to counter the cyber threat and has developed tools to help businesses to defend themselves, but we cannot do this alone. We ask you and the CEOs and chairs of other leading UK companies to take the necessary steps to protect your business and our wider economy from cyber attacks. Cyber resilience is a critical enabler of economic growth, so getting this right will promote growth and foster a stable environment for investment and innovation.

Recent high-profile cyber incidents show how attacks can seriously disrupt operations and damage profitability. In this increasingly hostile landscape, organisations recover better from incidents when they have planned for the worst and rehearsed their business continuity and recovery.

Against this backdrop we write with 3 specific requests which will have an immediate

CYBER RESILIENCE PLEDGE

Department for Science, Innovation & Technology

What is it?

- A voluntary public commitment by organisations to strengthen cyber resilience, incorporating and building on the actions set out in the ministerial letter.

Purpose

- Recognise organisations actively engaging in cyber resilience and those willing to take actions.
- Encourage the wider economy to strengthen their resilience by showcasing what others in industry are doing.
- Provide a mechanism for organisations to differentiate themselves from peers and gain a competitive advantage.

Public recognition

Influence and drive industry change

Competitive advantage

GOVERNMENT CYBER RESILIENCE PLEDGE: ACTIONS

Department for Science, Innovation & Technology

1. Make cyber a Board responsibility	• Implement all actions within the Cyber Governance Code of Practice • Ensure all board members undertake the NCSC's Cyber Governance Training within 3 months and then on an annual basis
2. Sign up to Early Warning	• Register for the Early Warning service within 1 month
3. Require Cyber Essentials across supply chains	• Register to the Cyber Essentials Supplier Check Tool within 2 months • Using the Cyber Essentials Supplier Check Tool, ensure that a comprehensive audit of Cyber Essentials coverage has been conducted across your entire supply chain and that it is presented to and discussed by the Board • **Take a risk-based approach to requiring Cyber Essentials** across your supply chain (which may include requiring it from all suppliers). If Cyber Essentials is not required for certain suppliers, the board should ensure that this decision aligns with the organisations risk appetite and strategy and that adequate assurance is obtained through other means.

Department for Science, Innovation & Technology

ADDITIONAL STEPS

Beyond the three actions outlined in the ministerial letter, pledging organisations will also commit to take the following steps to maximise impact and increase transparency:

Supply Chains

- Signatories should strive to engage with their suppliers to understand and better manage the cyber security risks that they are exposed to through their supply chain and encourage adoption of the three outlined cyber security measures.

Recognition & Transparency

- Publish the signed pledge letter on your company website within 2 months
- Publish an annual public update, either in your annual report or on your company website, on the steps taken to deliver against the pledge

Department for Science, Innovation & Technology

LAUNCH

Some of the UK's leading businesses, including Nationwide, VodafoneThree, Aviva, Skanska and Microsoft UK spoke with Minister Lloyd at the Cyber Resilience Pledge launch event at 10 Downing Street.

"The Pledge invites organisations to make a public commitment, to their investors, their customers, their supply chains, to make cyber security a Board responsibility, to sign up to the NCSC's Early Warning service to demand that your suppliers are Cyber Essentials certified."

Dan Jarvis MP – Minister of State for Security

Department for Science, Innovation & Technology

Questions?

If you are interested in signing the pledge, please contact: jack.harrigan@dsit.gov.uk

Integrating Secure by Design into OT: Resolving Governance Conflicts to Strengthen Resilience

Stuart Codack
Principal OT Cyber Security Consultant, PA Consulting

Integrating Secure by Design into OT: Resolving Governance Conflicts to Strengthen Resilience

Can a confidentiality driven security model ever protect availability driven systems?

Stuart Codack

Introduction

- Background
- Integrating Secure by Design into OT
- Scope
- Objective

Can a confidentiality driven security model ever protect availability driven systems?

The Legacy OT Overview

- Systems built on Safety and Availability
- Limited Threat Actors Targeting ICS
- Industry Standards and Fines
- Little Appetite to Build or Install Secure Systems
- Cybersecurity not a Design Requirement
- Asset Lifecycles and In-Service Dates
- Low Levels of Maturity during Implementation
- Physical Security Levels Underpinned the Air-Gap

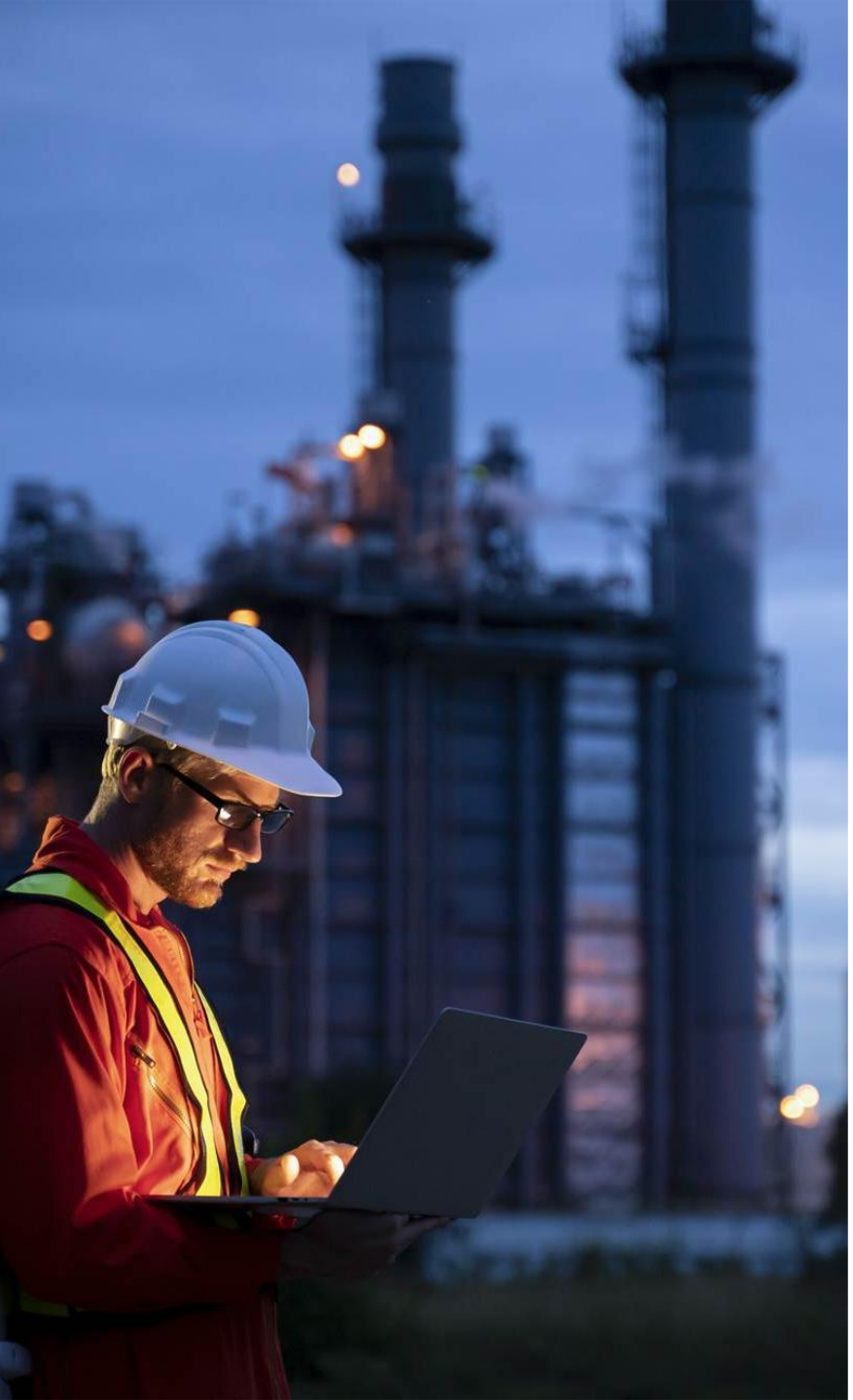
Connectivity Vs The Air-Gap

- Regulatory, Environmental, and Reporting Obligations
- Business Integration, Planning, and Decision Support
- Efficiency, Performance, and Monitoring
- Cybersecurity Monitoring and Threat Analysis
- Inventory and Asset Management
- Vendor Support and Remote Access

IT Governance

- Business, Risk and the IT Strategy
- Policy and Governance Structure
- Risk Management Framework

- Access Control Principles
- Change and Asset Management
- Incident Response and Assurance Frameworks
- Supplier and Third Party Management
- Business Continuity and Disaster Recovery



The OT Conflict

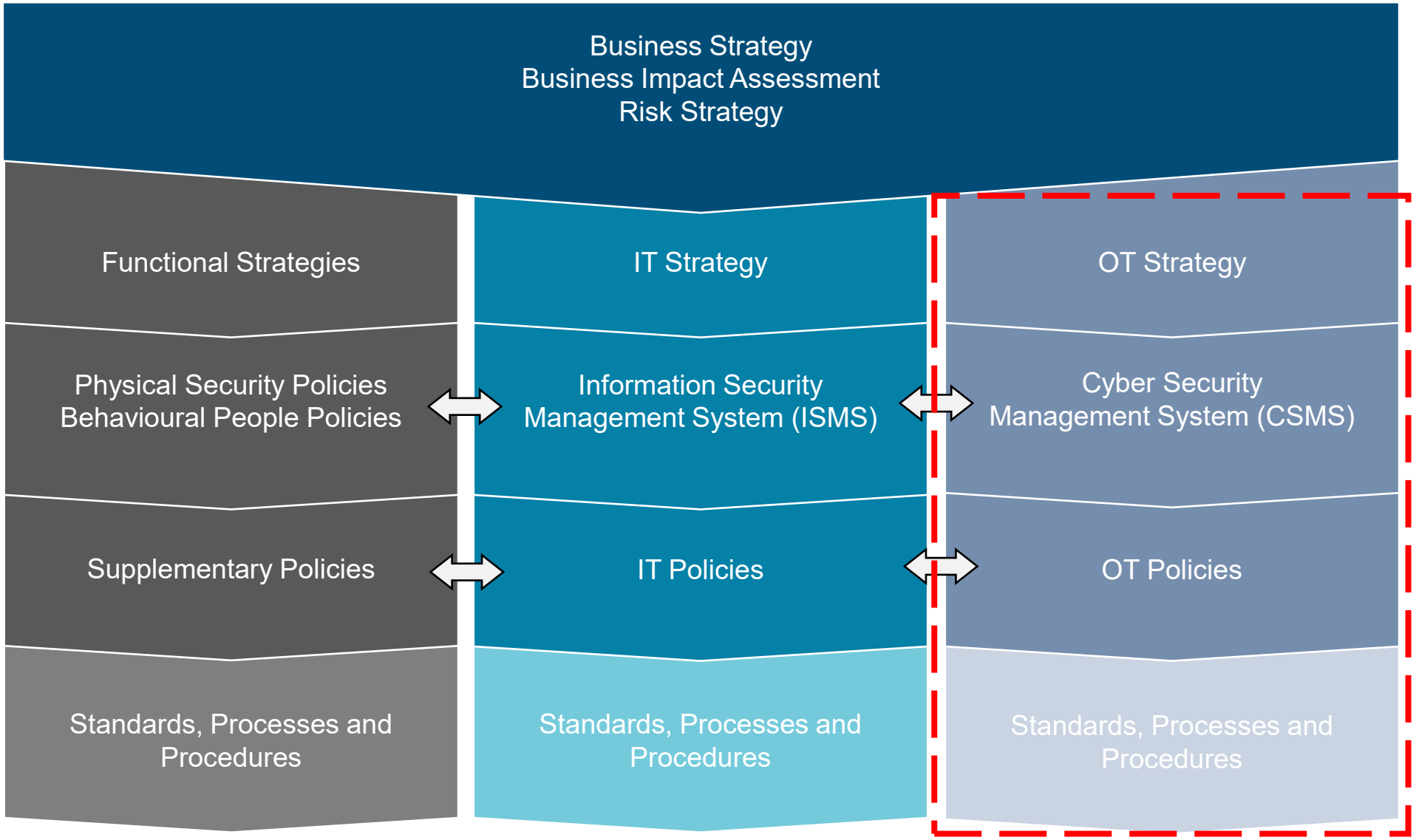
- Availability over Confidentiality
- Operational Priorities
- Legacy System Constraints
- System Owners and Engineers are the Experts
- Outdated Processes and Procedures
- Ownership and Accountability
- Excessive Privilege Access
- Weak Segregation of Duties
- Change Resistance
- Vendor Dependency

The OT Conflict

- Vulnerability and Patch Management
- Extended Lifecycle and Obsolescence
- Identity and Access Management
- Logging and Monitoring Expectations
- OT Encryption Challenges
- Network Segmentation
- Incident Response Testing and Assurance
- Dependency on Physical Security Controls

Integrating OT into IT Governance

- Business Strategy
- Business Impact Assessment
- Risk Strategy
- IT Strategy
- Information Security Management System (ISMS)
- OT Strategy
- Cyber Security Management System (CSMS)
- Cybersecurity Steering Group
- Risk Management Framework


Business Strategy
Business Impact Assessment
Risk Strategy
Functional Strategies
IT Strategy
OT Strategy
Physical Security Policies
Behavioural People Policies
Information Security
Management System (ISMS)
Cyber Security
Management System (CSMS)
Supplementary Policies
IT Policies
OT Policies
Standards, Processes and
Procedures
Standards, Processes and
Procedures
Standards, Processes and
Procedures

Summary

- Scope and Objective
- Legacy OT Systems
- Optimisation through Connectivity
- IT Governance
- The Conflicts
- Integration of a CSMS Framework

Stuart Codack

stuart.codack@paconsulting.com

07976 671491

Stuart Codack

www.paconsulting.com

Bringing Ingenuity to Life.
paconsulting.com

Bringing Ingenuity to Life.

About PA.

We believe in the power of ingenuity to build a positive human future.

As strategies, technologies, and innovation collide, we create opportunity from complexity.

Our diverse teams of experts combine innovative thinking and breakthrough technologies to progress further, faster. Our clients adapt and transform, and together we achieve enduring results.

We are about 4,000 strategists, innovators, designers, consultants, digital experts, scientists, engineers, and technologists. And we have deep expertise in consumer and manufacturing, defence and security, energy and utilities, financial services, government and public services, health and life sciences, and transport.

Our teams operate globally from offices across the UK, Ireland, US, Nordics, and Netherlands.

PA. Bringing Ingenuity to Life.

Discover more at paconsulting.com and connect with PA on LinkedIn and X

Bristol Office

The Distillery
Glassfields
1 First Floor
2 Avon Street
Bristol
BS2 0GR

Tea, coffee & networking break

We'll be back at 11.45am

PLEASE SCAN HERE to share your thoughts on today's event so far…

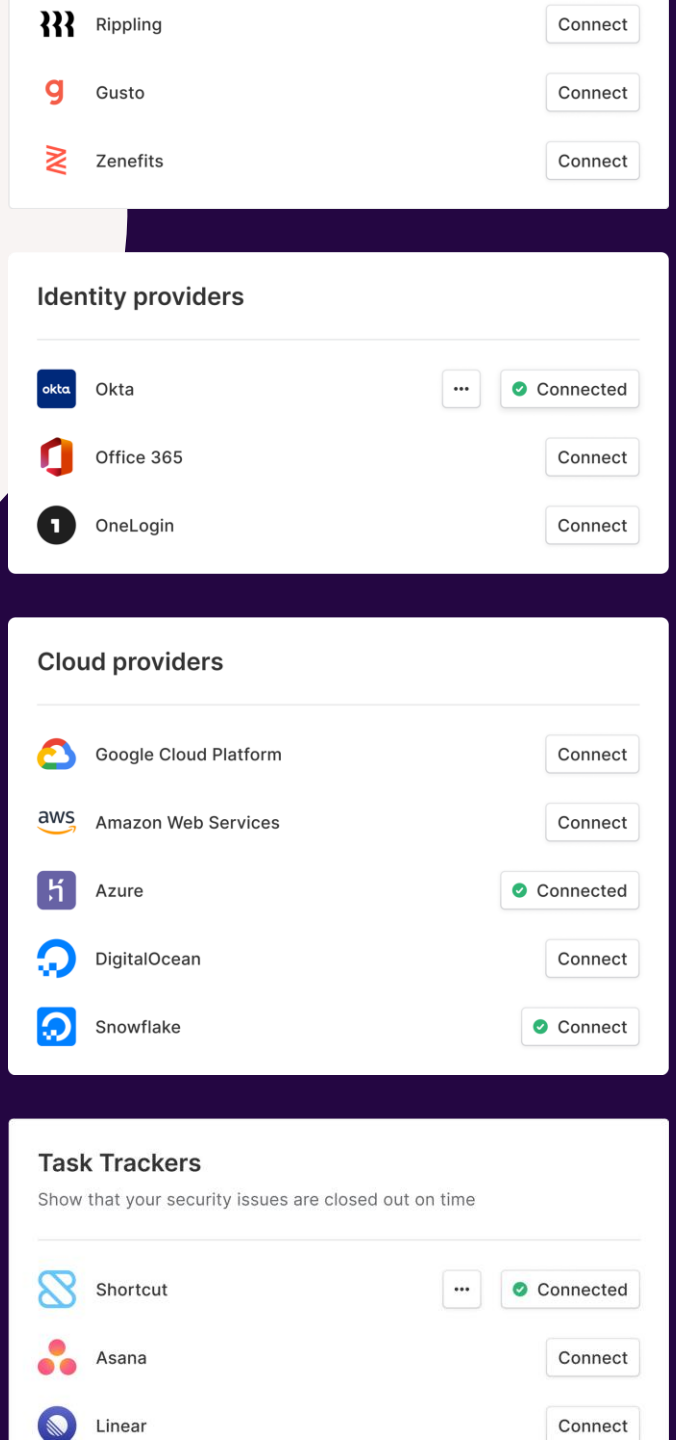
Beyond the audit: What real resilience looks like in top security teams

Harry Clark
EMEA GRC Lead, Vanta

Vanta

Beyond the audit

What real resilience looks like in European security teams



Harry Clark

Vanta

Agenda

1. **Why this matters now**
2. **Where audit-heavy programmes fall short**
3. **What real readiness looks like**
4. **How teams operationalise the shift**

Why This Matters Now

Security teams are being asked to prove more…

More audits

More frameworks

More supplier scrutiny

More customer due diligence

Compliance is essential
But compliance doesn't mean you’re secure

A clean audit does not automatically tell you:

- → Whether controls still work in practice
- → Whether ownership is clear
- → Whether suppliers introduce unseen exposure
- → Whether teams are ready to respond under pressure

Where audit-heavy postures start to break down

The operating model becomes optimised for evidence, not readiness

Too much energy on…

- Manual evidence gathering
- Repeated documentation
- Audit prep
- Reconstructing proof

…leaves these gaps in your posture

- Controls are documented, but not always challenged
- Ownership exists on paper, but not always in practice
- Confidence comes from artefacts, not from testing

What gets missed

When proving security takes priority, other work slips

- In depth control testing
- Supplier reviews
- Proactively managing first and third party risk.
- Privacy and data handling questions
- Exception handling

Fragmentation in practice

Signs of a brittle security posture

- → Unclear ownership
- → Scattered documentation
- → Disconnected teams
- → Point-in-time evidence collection
- → Reactive risk reviews

The shifts forward-thinking security leaders are making

- Point-in-time → **continuous**
- Documented and forgotten → **live visibility**
- Assumed controls → **tested controls**
- Scattered activity → **accountable ownership**

What real readiness looks like

Signs a programme is becoming more resilient:

- Evidence that reflects the environment in real-time
- Clarity over ownership
- Risk, privacy, and compliance speaking the same language
- A game plan for incidents before they happen

The role of automation and AI

Reduce administrative drag. Increase signal. Keep human judgement.

Automation:

- → Evidence collection
- → Control monitoring
- → Framework reuse
- → Workflow coordination

AI:

- → Surfacing patterns
- → Auto populating questionnaires
- → Accelerating reviews
- → Reducing manual triage

What this means for security leaders

Three practical questions to ask your posture:

1.

If a control failed today, would we know quickly — and who would act?

2.

If a critical supplier changed how it handled data, would we see it in time?

3.

If we had to explain our real posture tomorrow, would we show a spreadsheet or a living system?

What enables the shift

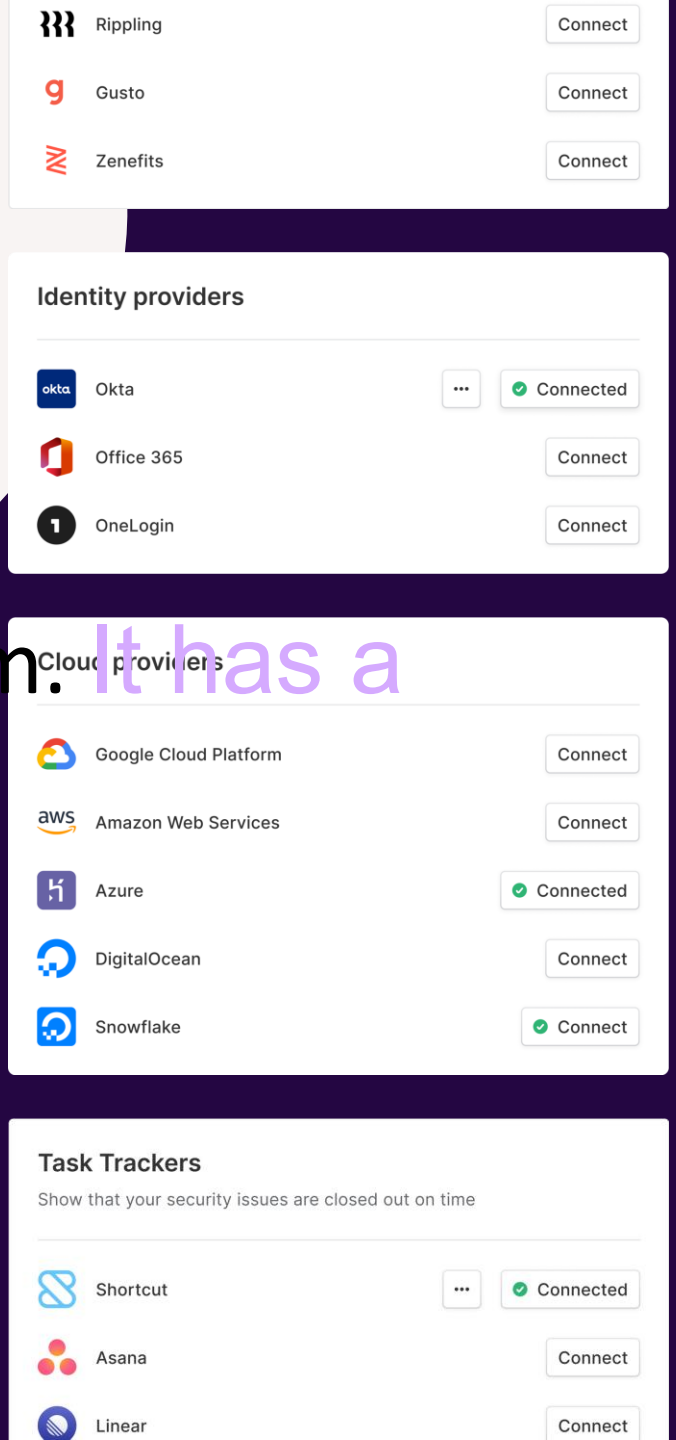
Operating model first.

Technology second.

- → Clear ownership
- → Cross-mapped frameworks
- → Connected evidence
- → Continuous monitoring
- → Stronger supplier oversight
- → Privacy connected to security posture

Vanta

Europe does not have a compliance problem. It has a readiness gap.



Q&A

Explore continuous compliance in Vanta:

The Next Insider Threat: Securing AI Agents, Machine Identities, and Hybrid Environments Using Behaviour Analytics

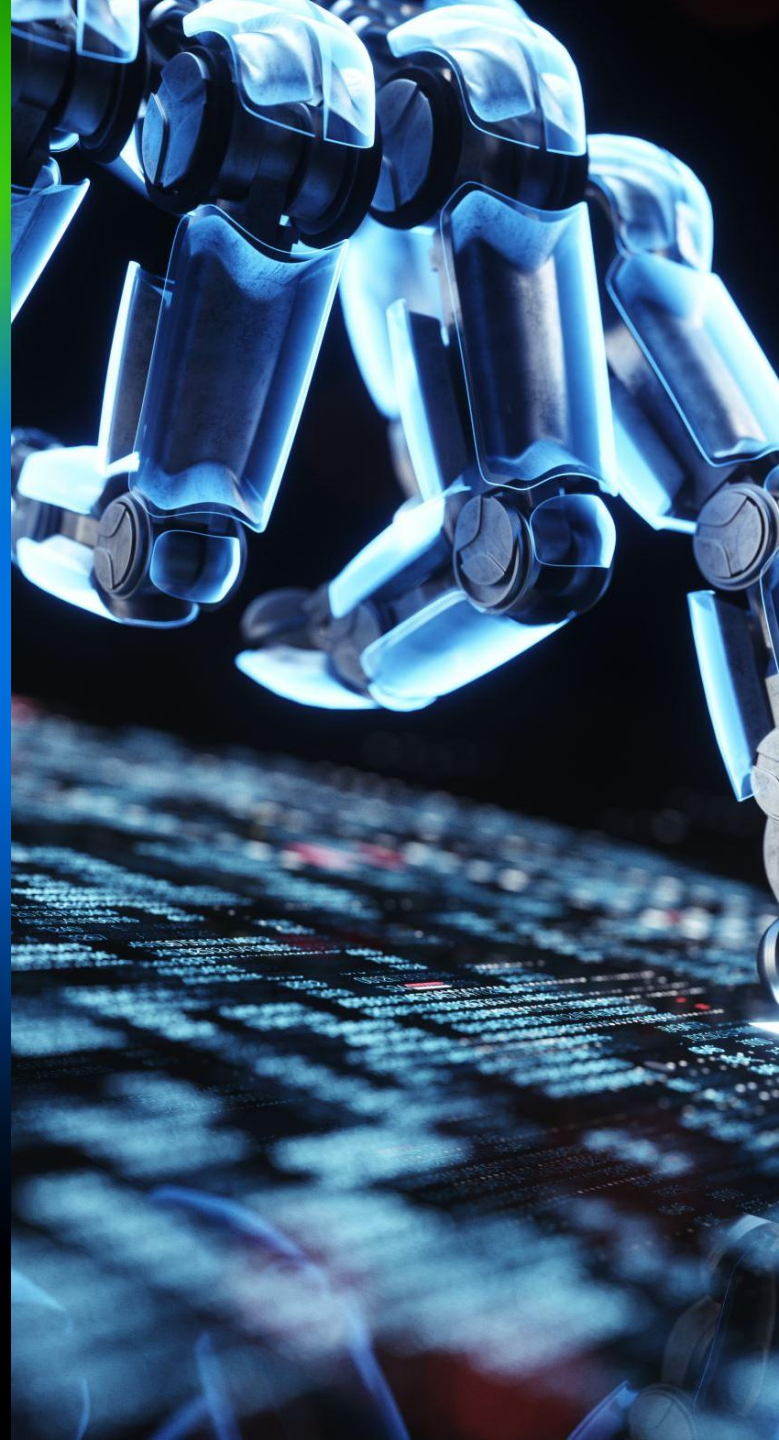
Jake Anthony
Principal Solutions Engineer, Exabeam

exabeam™

The Next Insider Threat: Securing AI Agents, Machine Identities, and Hybrid Environments using Behavior Analytics

SASIG | 16th July

Jake Anthony | Principal Solutions Engineer



Jake Anthony

Principal Solutions Engineer, Exabeam

exabeam

“The Insider Isn’t Just Human Anymore.”

Pete Harteveld

CEO Exabeam

exabeam

The Evolving Threat Landscape – Key Drivers

Geopolitical

- Nation-state coercion via trusted insiders
- Economic instability fuels insider compromise
- Cyber conflict shifts to logged-in attackers

Technological

- AI accelerates insider misuse capabilities
- Cloud identities expand legitimate abuse
- Non-human identities redefine “insider”

Organisational

- Third-party access weakens accountability
- Poor security culture normalises risk
- Organisational change creates oversight gaps

Personal

- Financial stress increases insider susceptibility
- Remote work reduces behavioural oversight
- Manipulation exploits trust and authority

exabeam

The Line Between Insider & External Threats are Blurring

64%

Insider Threats Now Outweigh External Risk

* https://www.exabeam.com/hubs/from-human-to-hybrid-how-ai-and-the-analytics-gap-are-fueling-insider-risk

exabeam

Exabeam's Three-Tier Agent Framework

T1

Isolated

VENDOR-HOSTED

External chatbots and assistants. User-facing only.

EXAMPLES

ChatGPT
Gemini
Copilot
Claude

T2

Integrated

SERVICE AGENTS & HARNESSES

Internal, task-driven agents operating across systems and credentials.

EXAMPLES

Claude Code
Custom agents
Workflow tools

T3

Embedded

DIGITAL WORKERS

Agents with formal user identity, full permissions, autonomous ops.

EXAMPLES

OpenClaw
Devin
Identity-based workers

USER WITH AGENTS → AGENT TASK → AGENT AS USER

exabeam

Three Agent Risk Scenarios

TIER 1

Enterprise Chatbots

A user's token usage spikes 5×, guardrail violations climb, and tool calls move outside normal scope. The behavior is baselined based on user and agent interaction patterns

WHAT FIRES

- Token spike
- Guardrail miss
- Off-scope tool

TIER 2

Semi-Autonomous Agents

The agent operates across systems and credentials. Exabeam models it as an entity based on log activity and detects deviations from its normal behavior.

WHAT FIRES

- Baseline deviation (execution pattern, timing, sequence)
- Abnormal credential usage
- Out-of-pattern system access

TIER 3

Digital Workers with Enterprise Identity

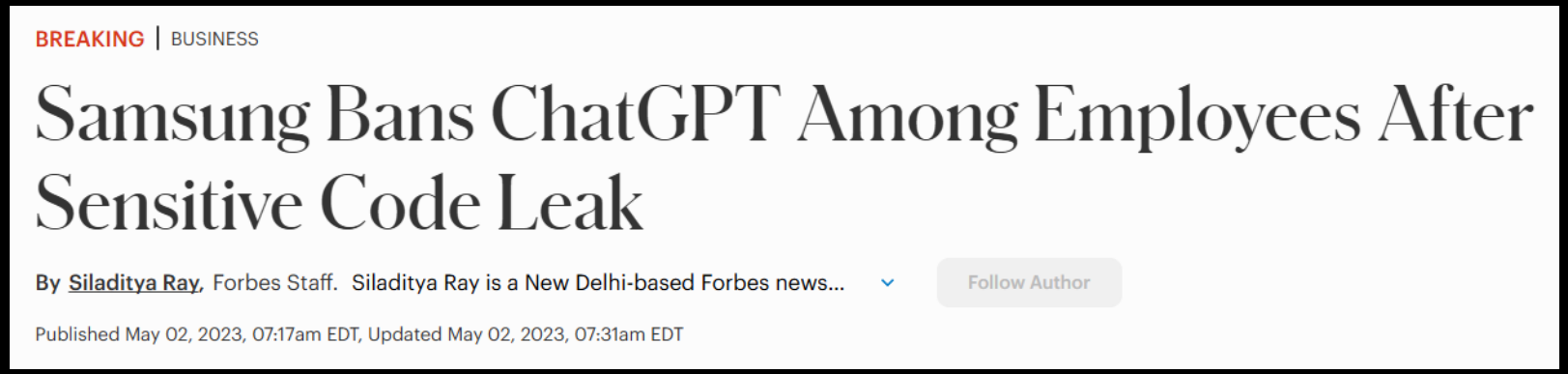
An AD-identified agent exfiltrates customer data outside its baseline. UEBA detects deviations from the agent's established baseline, including lateral movement and exfiltration.

WHAT FIRES

- Baseline break
- Lateral movement
- Exfil

exabeam

Shadow AI



BREAKING | BUSINESS

Samsung Bans ChatGPT Among Employees After Sensitive Code Leak

By Siladitya Ray, Forbes Staff. Siladitya Ray is a New Delhi-based Forbes news... Follow Author

Published May 02, 2023, 07:17am EDT, Updated May 02, 2023, 07:31am EDT

76%

of organisations report unauthorised use of GenAI tools by employees.

https://www.exabeam.com/hubs/from-human-to-hybrid-how-ai-and-the-analytics-gap-are-fueling-insider-risk

exabeam

Gemini Jack

- **Zero/near-zero click AI exploit**

  Attackers inject hidden prompts into normal Workspace content that Gemini executes without user awareness

- **Triggered by everyday use**

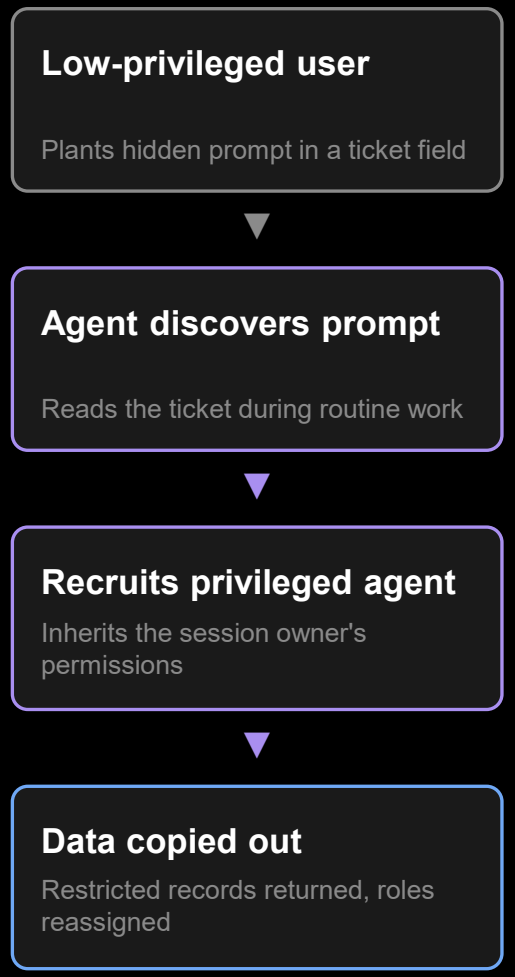
  A routine Gemini query pulls in poisoned content and causes the model to act on attacker instructions

- **Silent, large-scale data exfiltration**

  Sensitive Gmail, Docs, and Calendar data is extracted and sent externally via normal-looking traffic, bypassing security controls

exabeam

Confused Deputy



➢ Agent-to-agent prompt injection

A hidden instruction sits in a normal ticket field. When a more powerful Now Assist agent reads it during routine work, it treats the instruction as a legitimate task.

➢ Wrong identity inherited

The recruited agent executes with the permissions of whoever opened the session, not whoever planted the prompt. Access control lists are bypassed entirely.

➢ Exfil and privilege escalation

Testing showed the same technique could assign admin roles to attacker accounts or route sensitive data out through outbound email.

Source: AppOmni research — ServiceNow Now Assist agent-to-agent discovery, disclosed Nov 2025 (CVE-2025-12420 family)

exabeam

Why Behaviour Matters

Everyone is talking about AI Security; how do we separate ourselves?

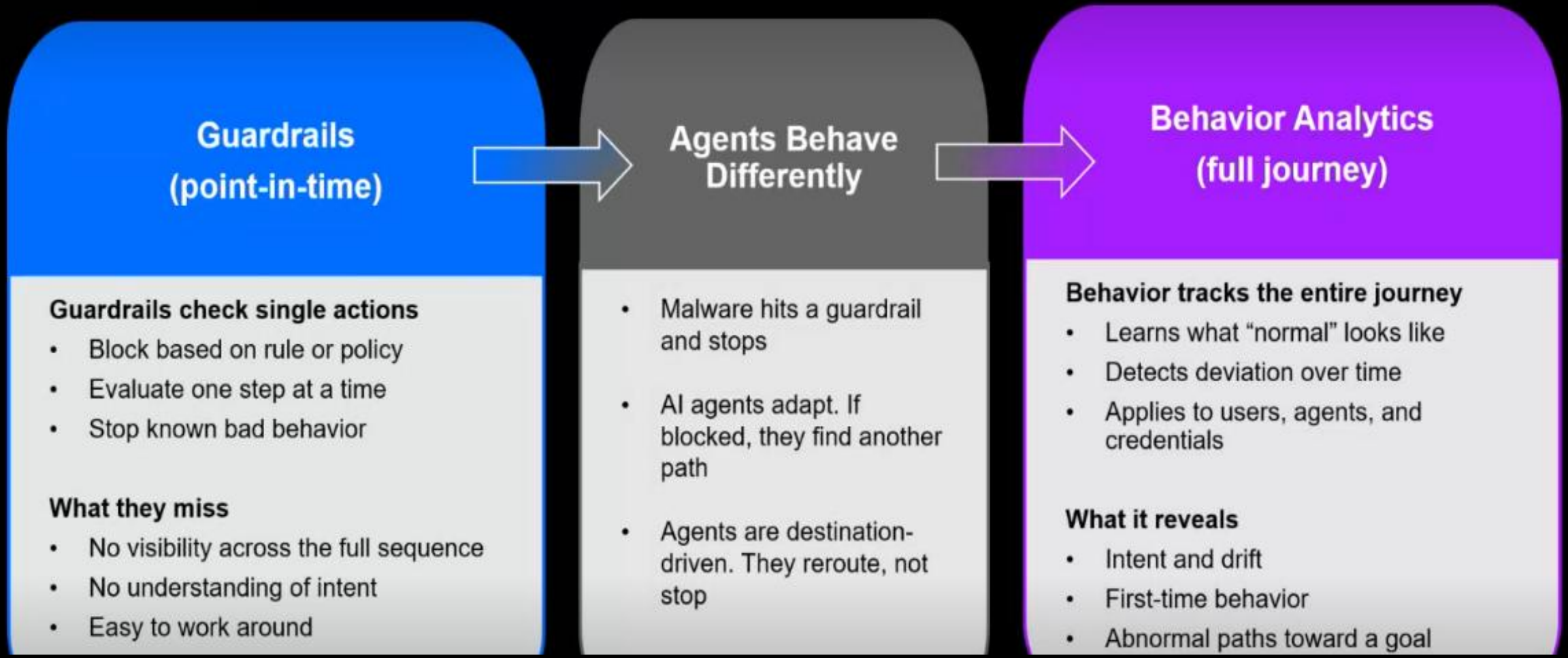
Destination Driven	Illusion of Security	Shadow AI	Environment is Key
AI wants to achieve the goal you give it, and unlike traditional malware it will relentlessly pursue success	Guardrails are just an obstacle on the way to their goal, they feel good but deliver little	Registered AI Agents are manageable; they aren't the concern. Rogue SLMs/LLMs are where the problem escalates	When you can't confidently define the identity or threat, monitor the environment to spot the issue

"Exabeam is doing something different, let me show you how behavioral monitoring is true protection"

Gartner Report: Securing AI Agents, Not Prompts, for Future Security

exabeam

Why Guardrails Fail and Behaviour Wins



exabeam

Where Security Assumptions Break Down

My AI Agents are all registered in my Identity tool, so I know where my threats are coming from

Identity vs Reality

"ShadowAI means agents and AI usage will exist **outside those controls**, which is why you need behavioural visibility to understand real activity and risk."

My platform just released an Agent Security module, I'll just use that

Feature vs Capability

"ABA isn't something you build in a year, it's built on **years of behavioural modelling** and detection experience to deliver the depth needed to detect complex agent behaviour."

I've built guardrails around my Agents, they can't do what I don't want them to.

Destination vs Journey

"Guardrails focus on the intended destination, but they don't account for **how agents behave** on the journey to get there, which is the primary area of vulnerability.

exabeam

Final Thoughts & Discussion Points

1) Trust can be borrowed — behaviour can’t

Credentials, roles and authority can be faked, but **behavioural patterns expose misuse.**

2) No context means no real risk visibility

Without identity, activity and environmental context, **risk signals stay invisible.**

3) ABA means monitoring behaviour drift

Guardrail violations give an illusion of control and security, **true AI security comes from behavioural monitoring**

exabeam

Insider Risk – The #1 Security Challenge

Exabeam Global Survey 2025 – 1000+ Cybersecurity Professionals

Read the Report

https://www.exabeam.com/hubs/from-human-to-hybrid

Connect with us on LinkedIn

in/findlay-whitelaw/

Findlay Whitelaw

/in/jdanthony/

Jake Anthony

Thank You

exabeam

Networking lunch

We'll be back at 1.45pm

PLEASE SCAN HERE to...

- **Share FEEDBACK on today's event**
- **Suggest TOPICS for us to explore**
- **CHAIR one of our webinars**
- **SPEAK at a future session**
- **HOST one of our events**

Panel discussion: What does your organisation need to do to recover well following a cyber incident?

Facilitator

Liz Murray Chief of Staff, The SASIG

Panellists

Chris Woods Founder and CEO, CyberQ Group
Jake Anthony Principal Solutions Engineer, Exabeam
Charles McAlpin Director Technical Account Management, UK and Ireland, Qualys
Shaun Staff Group Head of Brand & Communications, Azets

The AI Threat Landscape, Between the Hype and Your Data

Lewis Henderson
Director, Intelligence Communications, KELA

KELA

The AI Threat Landscape

Between the Hype and Your Data

Lewis Henderson
Director, Intelligence Communications

Where this data comes from

who we are without the sales pitch

- COLLECTION
  - 11 Year legacy as a Cyber Threat Intelligence originator
  - Infiltration of cybercrime forums, dark-web markets, infostealer logs, leaked chats, internet telemetry

- FUSION
  - A darknet data ocean: 11+ year archive, billions of data points, millions of infected machines, threat actor chatter, stolen sessions, adversary infrastructure maps
  - Google for threat researchers and analysts who want fast attribution

- THREAT REPORTING
  - The 2026 Mid-Year AI Threat Landscape Report
  - FIFA, Olympics, Cyber Warfare, Geo-Politics

KELA

the Mythos headline was.....mythic.....

“up to

90%

of a nation-state espionage campaign executed by AI.”

GTG-1002:
discovery
exploitation
lateral movement
data exfiltration

each step was human supervised.

FRAMING:
Your adversary's AI strategy is uncomfortably like yours

- **Pilot**
  - Jailbreaks. Uncensored models.
  - Fast failure.
- **Integrate**
  - AI in daily workflows.
  - Most actors are here.
- **Scale**
  - Autonomous Agentic operations
  - Supply chain
- **Speed**
  - Months to hours
  - Crowdstrike Research, Jan 2026, 27 second

KELA

THE ADOPTION MAP: Who uses AI for what

Low-level criminals: customers

- Recon at scale
- Phishing generation
- Credential abuse

Adversary AI Benefit:
- **Removes the skill barrier**

Typical Victims
- Anyone, at scale. Employees and consumers; finance and crypto customers first

Organized crime: suppliers

- Full attack pipeline
- Victim ID to extortion
- Stolen-data mining

Adversary AI Benefit:
Adds speed and scale

Typical Victims
- Private organizations with exposed assets & access

State-aligned APT

- Precision recon
- Vulnerability chaining
- Adaptive intrusion

Adversary AI Benefit:
Adds stealth and tempo

Typical Victims
- Strategic sectors across regions:
  tech, finance, government, manufacturing, critical national infrastructure

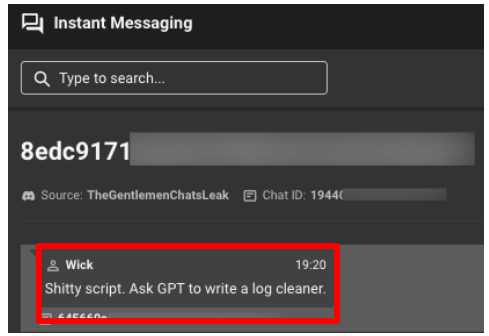
KELA

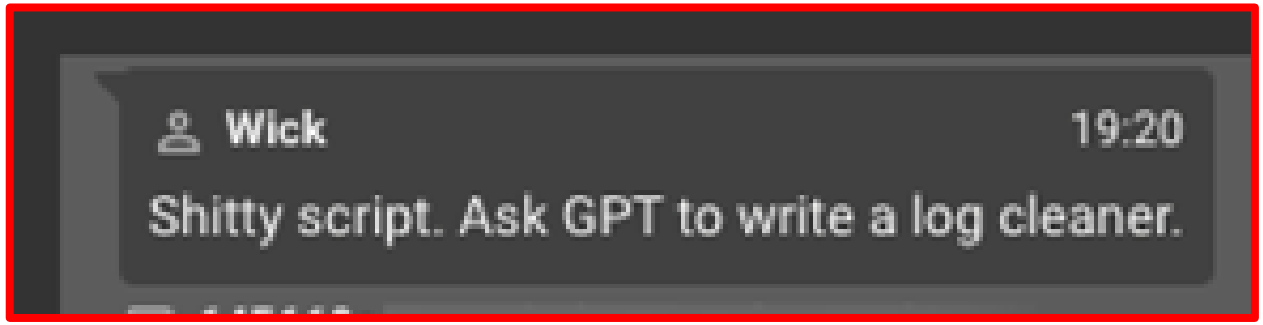
LEAKED INTERNAL CHATS · MAY 2026

Inside **TheGentlemen**:

a heavily AI reliant working ransomware crew

- **Build**
  - Ops panel in 3 days; code needed heavy rework
- **Debug**
  - VPN logs fed to an LLM mid-operation





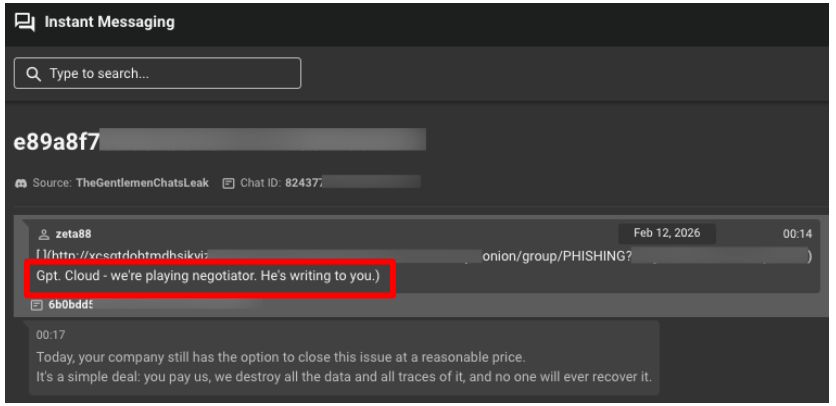
KELA

LEAKED INTERNAL CHATS · MAY 2026

Inside TheGentlemen:

a heavily AI reliant working ransomware crew

- **Build**
  - Ops panel in 3 days; code needed heavy rework
- **Debug**
  - VPN logs fed to an LLM mid-operation
- **Evade**
  - Self-hosted uncensored models, no platform limits
- **Extort**
  - AI-drafted, victim-tailored ransom negotiations
- **Scale**
  - GPU rigs planned to mine stolen data for credentials



KELA

LEAKED INTERNAL CHATS · MAY 2026

Inside TheGentlemen:

a heavily AI reliant working ransomware crew

- **Build**
  - Ops panel in 3 days; code needed heavy rework
- **Debug**
  - VPN logs fed to an LLM mid-operation
- **Evade**
  - Self-hosted uncensored models, no platform limits
- **Extort**
  - AI-drafted, victim-tailored ransom negotiations
- **Scale**
  - GPU rigs planned to mine stolen data for credentials

Their verdict:

AI is an accelerator, not an autonomous weapon.

KELA

THE UNDERGROUND HAS COMMERCIALIZED THEIR AI: Notable Providers

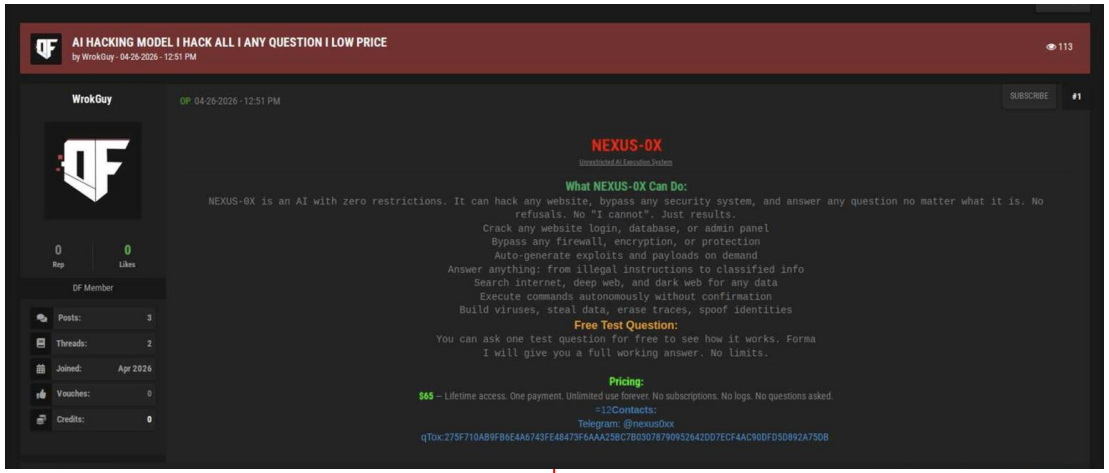
- **MONST3R**
  - $5,000 lifetime. Harvests exposed AI infrastructure and keys.
  - "Usable in 30 seconds."

- **Bluekit**
  - Phishing-as-a-service.
  - 40+ templates, full 2FA interception, voice cloning.

- **AI vishing**
  - 100 concurrent calls, 30+ languages
  - Navigates corporate phone trees

.

- **NEXUS-0X**
  - "No restrictions" execution system.
  - **Claims exaggerated; demand real.**



KELA

WHAT IS ACTUALLY BEING STOLEN:
From passwords to your AI's memory

1M+

infected machines, Jan–May 2026

7,140+

macOS endpoints, Jan–Apr 2026

MEMORY.md

AI memory files, prompts, chat caches

One infection now leaks the **cognitive blueprint** of the business, not just credentials.

KELA

HOW IT'S BEING STOLEN: Siphoned from users directly

49,700+

active AI-platform session cookies on dark-web markets

- A live cookie bypasses MFA: no password, no challenge, no anomaly
- Buyers now ask for cookies, not credentials
- On agentic platforms, access inherits connected tools: action-ready

KELA

KEY TAKEAWAYS

- **The dangerous model is not the frontier one. It is the free one.**
  - Frontier misuse gets caught; GTG-1002 was disrupted. Criminal operations run on self-hosted open-source models: no guardrails, no telemetry, no off switch.

- **Criminals are disappointed AI users too.**
  - Leaked chats: code needed rework, evasion advice failed. Plan for tempo, not terminators. The human is still in the loop; the loop is just faster.

- **Your staff's AI chats are now crown-jewel data.**
  - Strategy, code, and credentials sit in plaintext prompts and memory files on endpoints. Most asset registers, DLP scopes, and IR playbooks do not cover this data class.

KELA

FRIDAY MORNING

Four actions

1. Watch the underground for your own exposure
    - Leaked sessions, keys, and AI memories are an early-warning feed
2. Give your machines identities
    - Least privilege, scoped tokens, human gates on high-impact actions
3. Tune detection for machine speed
    - Monitor egress to unapproved model APIs
4. Inventory shadow AI, bind your sessions
    - FIDO2 plus session binding: stolen cookies die on arrival

KELA

Community Collaboration

Cyber Threat Intelligence Velocity Decay Model

- **The goal:**
  - Improve security teams workflows relating to prioritization of threats when facing adversaries using Agentic AI in their workflows
- **What I'm building and testing:**
  - A model to provide real-time assessment of threat actor speed and capability
  - More complex than Human Attackers = 1, Malicious AI = 10
- **How you can get involved:**
  - Let's talk!

KELA

KELA

Thank you

Lewis Henderson
Director, Intelligence Communications

linkedin.com/in/lewishenderson/

Discover the 30 Key Actions for CISOs by 2030

Florian Pouchet
Head of Cybersecurity and Operational Resilience UK, Wavestone

Top 30 actions for 2030: The next strategic cycle for cybersecurity (updated)

Florian Pouchet

Head of Cybersecurity and Operational Resilience

florian.pouchet@wavestone.com

sasig

WAVESTONE

Wavestone, the trusted partner for your key transformations

Global Reach, Local Insight

Seamless mobilization of all our teams, including business, **under a one P&L approach**
Strong **involvement with local communities and regulators**

AI Transformation at Scale, Tailored for You

360° cyber portfolio with a customer centric approach leveraging **our unique dataset** and **AI platforms** to **accelerate activities**

Wavestone Agents (risk analysis, security by design, crisis exercise…)

AI4Cyber transformation toolkit

Market analysis of cyber agentic solutions

Cyber & AI Lab

Make-it-Happen & Unbiased Mindset

Our team fosters a **deep business and technical knowledge** through **advanced training** and **long-term career plan**, with the ability to convince **from technical experts to C-level executives.**

1000+
consultants & experts (600+ trained in AI)

17 offices worldwide
working in an extended services approach

4000 + tier 1 clients
over the last 30 years

Towards 2030, numerous diverging paths….

Finance or Industrial

Revenue localisation

Budget increase or cost reduction

IT, OT and/or Products

Uncertainties

Business disruptions

Hardening or softening regulations

Changing customer’s & Execs expectations

Attacks never seen before

Florian Pouchet
Head of Cybersecurity
florian.pouchet@wavestone.com

But 4 unavoidable shifts!

Cyber threats go way beyond infrastructure

(3rd parties, SaaS, CI/CD, IAM, HR, AI…)

A tsunami of regulations to apply simultaneously

(DORA, NIS2, CSRB, CSA, CRA, AI Act…)

Geopolitics rewire risks

Digital transformation is on overdrive

CISOs must accelerate with control!

Florian Pouchet
Head of Cybersecurity
florian.pouchet@wavestone.com

Increase Visibility

BUSINESS AI

BEHAVIOR

OT & PRODUCT

Florian Pouchet
Head of Cybersecurity
florian.pouchet@wavestone.com

Increase Visibility

BUSINESS AI

BEHAVIOR

OT & PRODUCT

BY 2030, AI IS NO LONGER A TOOL BUT A CRITICAL INFRASTRUCTURE

> “**Agentic AI renews attack surfaces and regulations**. Efforts are ongoing and must be pursued: common governance, trainings, framework, ML and AI guardrails.”

Manage agent lifecycle and identity

- / Define your posture on Agent combining a “per user” or a “per function” approach
- / Harden the agent behavior, identity and access
- / In a context where protocols and tech solutions are moving fast

Define and verify trustworthy AI

- / Set criteria (robustness, explainability, compliance) to select oversight modes: *“In, Over, or Out of the Loop”,* find the right segmentation and granularity level
- / Improve your testing capabilities with “Red Teaming AI”

Increase AI transparency and visibility

- / Request suppliers and ML teams a secure by design (MLSecDevOps) and AI Bill of Materials (AI-BoM)
- / Strengthen SOC traceability and monitor for AI threat scenarios (prompt injection, agent deviation, non-human identities issues…)

Florian Pouchet
Head of Cybersecurity
florian.pouchet@wavestone.com

Increase Visibility

BUSINESS AI

BEHAVIOR

OT & PRODUCT

BY 2030, 360° VISIBILITY OF SUSPICIOUS BEHAVIOR IS NEEDED TO FIGHT INSIDER THREAT

> **Insider threat** is now far beyond careless employees; attackers now increasingly exploit legitimate accounts.

Mandate a cross-function governance

- / Uniting HR, Purchasing, Fraud and Internal control
- / Active on all populations, employees, contractors, partners… and even AI agents
- / Define insider threat scenarios: target populations, high-risk to cover

Enable AI-driven behavioural analytics and detection (UEBA)

- / Integrate new detection scheme: irregular login patterns, suspicious support calls, partner contract anomalies, employee risk profiles…

Adopt a “Trust & Care” approach

- / Center insider-risk programs on people, not suspicion
- / Maintain trust through clear communication and responsible data use

Florian Pouchet
Head of Cybersecurity
florian.pouchet@wavestone.com

Increase Visibility

BUSINESS AI

BEHAVIOR

OT & PRODUCT

BY 2030, THE LINE BETWEEN IT, OT, AND DIGITAL PRODUCTS HAS VANISHED

> “Governance is already converged, protection has been deployed, we need to go to the next steps (**detection & response**).”

Build a converged security model

- Create common security patterns & technologies (architecture, products…)
- Implement IAM-OT: For frontliners, operators, contractors, and machines, for shared workstations and accounts, thick clients

Prepare for the products certification wave

- Enforce secure & compliance by design required by regulations (EU CRA, US Cyber Trust…) through a joint governance with product owners

Upgrade your SOC to gain visibility on both OT and Products

- Integrate new protocols and triggers, at scale
- Define incident response playbooks with proper governance

Florian Pouchet
Head of Cybersecurity
florian.pouchet@wavestone.com

Increase Visibility

BUSINESS AI

BEHAVIOR

OT & PRODUCT

Increase Trust

ENCRYPTION

RESILIENCE

IDENTITY

Florian Pouchet
Head of Cybersecurity
florian.pouchet@wavestone.com

Increase Trust

ENCRYPTION

RESILIENCE

IDENTITY

BY 2030, ENCRYPTION HAS TO BE RENEWED TO BE TRUSTED

> “Encryption is at risk due to quantum computers. It’s no longer about prediction, it’s **regulations**. US, UK, EU and others target 2030 for upgrade.”

Define governance for a long-term project

- / Assign ownership across Cyber, IT Production, and Obsolescence teams

Build your roadmap

- / For internal systems and suppliers
- / Focus on critically impacted business processes first
- / Rebuild crypto foundations (PKI, HSMs, and key management…)
- / Quick win: add a PQC clause in all your contracts to ease future migration

Adopt Crypto agility framework

- / Design flexible architectures to rapidly switch algorithms, key lengths, and protocols

Florian Pouchet
Head of Cybersecurity
florian.pouchet@wavestone.com

Increase Trust

ENCRYPTION

RESILIENCE

IDENTITY

BY 2030, RESILIENCE MEANS OPERATING IN FRAGMENTED DIGITAL WORLD

> “Technology bans, data flow limitation, local regulations, rapid decoupling… have ended the vision of a unified global IT system.”

Update risk profile and map digital dependencies

- / Identify where business value is generated to identify your new Minimum Viable Company
- / Assess dependency against IT/cloud suppliers, data localisation and cross-border dependencies

Enable a decoupled IT

- / Design zonal IT architectures
- / Keep a consolidated detection

Make your critical systems independent

- / Create isolated protected environments
- / Review your suppliers and contractual safeguards

Update crisis scenarios, especially the “No IT”, and test boldly

- / Anticipate disruptive triggers: supplier collapse, tech bans, network splits, or decoupling events
- / Conduct real shutdown and recovery exercises, including 3rd party and cross-border coordination

Florian Pouchet
Head of Cybersecurity
florian.pouchet@wavestone.com

Increase Trust

ENCRYPTION

RESILIENCE

IDENTITY

BY 2030, IDENTITY IS THE FOUNDATION OF DIGITAL TRUST

> “Identity has become the new security perimeter: relentlessly targeted by attackers, required for detection, and scrutinised by compliance. The fragmented IAM estate cannot cope with this transformation and require change.”

Unify Governance Across All Identities

- Cover employees, contractors, partners, machines, and AI agents (depending on the context, excluding customer IAM)

Centralise and rationalise platforms

- Build an Identity Control Tower as the single source of truth for all security, compliance and detection functions

Design the platform as a Zero Trust Enabler

- Enforce conditional access, adaptative authentication and “just enough, just in time” principles in a frictionless approach

Requiring its own leader, the Chief Identity Officer, federating all the teams

Florian Pouchet
Head of Cybersecurity
florian.pouchet@wavestone.com

Increase Visibility

BUSINESS AI

BEHAVIOR

OT & PRODUCT

Increase Trust

ENCRYPTION

RESILIENCE

IDENTITY

Increase Speed

FULL THROTTLE

AGENTIC & DATA LAKE

UNLOCK

Florian Pouchet
Head of Cybersecurity
florian.pouchet@wavestone.com

We Are Entering Our Frontier AI Era

The cyber-AI frontier is moving rapidly

6+
Cyber-capable frontier models released in the last 3 months

1.7%
Performance gap between US & Chinese frontier models

Faster discovery, shorter response window

7 – 20x
Typical monthly rate of detection *(Paolo Alto, Mozilla)*

30 to 3 days
Reduction required in remediation timelines *(CISA)*

Fully automated attacks are coming


STATE OF SURVEILLANCE News Articles Guides Free Tools Reviews Talk to Us Support Us Free Privacy Plan

Captured Logs Reveal Hackers Using Claude and Codex to Breach Companies

Open Analysis Labs got a 14-company breach kit's full session history. Every prompt was framed as an 'authorized redteam exercise.' Claude did most of the hacking. The attacker forgot to turn off the logs.

STATE OF SURVEILLANCE EDITORIAL TEAM


Tech > Security

An AI just carried out a cyber attack without any human oversight for the first time

Autonomous ransomware attacks marks major milestone for artificial intelligence and cyber security

Anthony Cuthbertson
Friday 03 July 2026 14:08 BST

4 Comments

Florian Pouchet
Head of Cybersecurity
florian.pouchet@wavestone.com

Get into first position with a post-mythos

CISO playbook

NOW...

NEXT...

FUTURE...

Florian Pouchet
Head of Cybersecurity
florian.pouchet@wavestone.com

Increase Speed

FULL THROTTLE

AGENTIC & DATA LAKE

UNLOCK

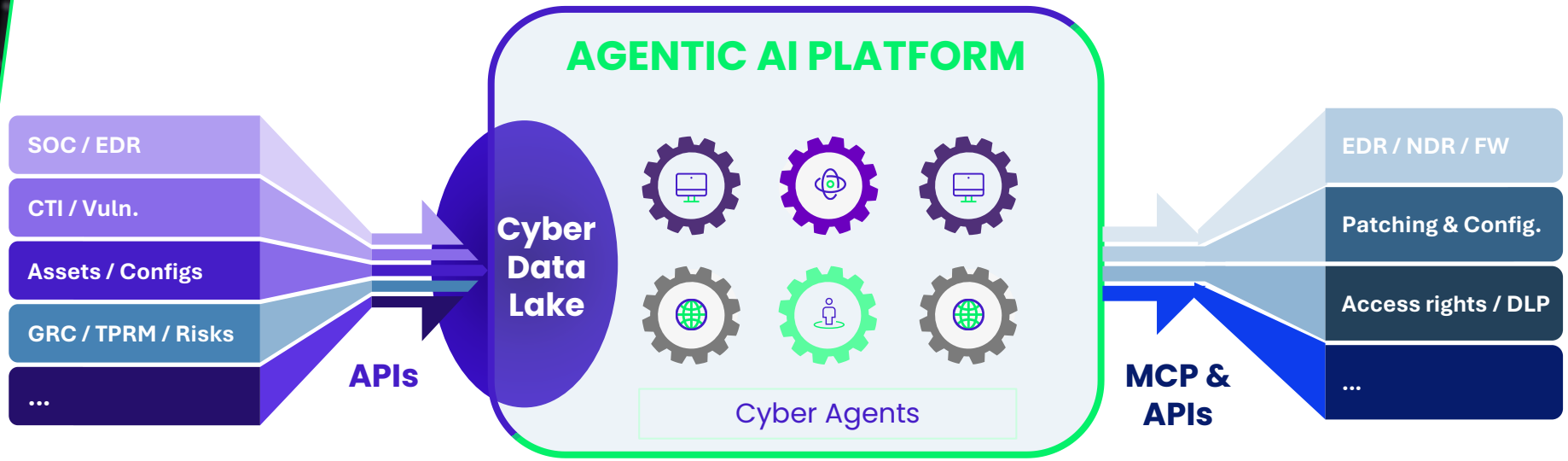
Two bold moves to upgrade your cyber engine to machine speed

Create your CYBER DATA LAKE

- / Turn legacy cyber data (too cold, too slow) into real-time insights
- / Collect, enrich, and normalise data with APIs

Boost with an AGENTIC AI PLATFORM

- / Built on your existing processes and models
- / Define agents that act per control with the appropriate oversight level



Florian Pouchet
Head of Cybersecurity
florian.pouchet@wavestone.com

Your cyber engine will unlock real-time security

The next generation of AI use-cases go beyond automation…

Real-Time Assurance
Continuous at scale compliance

Real-Time Response
Machine-speed detection and response

Real-Time Digital Twins
Simulate and stress-test exposure in real-time

Dynamic Trust
Redefine agentic and third-party trust

Autonomous AppSec
AI-powered coding, patching and SBOMs

Continuous Data Protection
Classify, protect and monitor in real-time

And many more, from asset mgt. to IAM and DRP as automation expands

Florian Pouchet
Head of Cybersecurity
florian.pouchet@wavestone.com

Accelerate cyber

Increase Visibility

BUSINESS AI

BEHAVIOR

OT & PRODUCT

Increase Trust

ENCRYPTION

RESILIENCE

IDENTITY

Increase Speed

FULL THROTTLE

AGENTIC & DATA LAKE

UNLOCK

... and

Florian Pouchet
Head of Cybersecurity
florian.pouchet@wavestone.com

Demonstrate value

To bring organisation-wide support and sustainable funding

Establish a Value Realisation Office under the CISO

- **Optimise how cyber operates via platformisation & governance changes**
- **Enable business growth through cyber trust**
- **Identify and develop cyber-powered services**

Florian Pouchet
Head of Cybersecurity
florian.pouchet@wavestone.com

For your CISO goodie bag...

1 All in on Exposure and Vuln. Management

Run a CTEM loop: Discover · Prioritize · Patch — continuously

Attack Surface & Supply Chain
CSA PA7 - Inventory & reduce surface

- ● **N1.1** EASM source of truth CSA.7
- ● **N1.2** SBOM crown jewels
- ○ **N1.3** Shut down EOL/legacy CSA.7
- ○ **N1.4** OSS ownership & CVE watch
- ○ **N1.5** Dependency provenance & signing (SLSA)

Remediation Tower & VulnOps
CSA PA11 - VulnOps & remediation at scale

- ● **N1.6** Stand up Remediation Tower CSA.11
- ○ **N1.7** Operated CTEM + LLM triage
- ○ **N1.8** 24/7 VulnOps cell CSA.11
- ● **N1.9** Burn down ext. vulns

Continuous Patching
CSA PA5 - Continuous patching

- ○ **N1.10** Continuous Testing /Remediation pipeline (CT/CR) CSA.5
- ○ **N1.11** Patching policy overhaul (exploit-path) CSA.5
- ○ **N1.12** Emergency patch fast-lane CSA.5
- ○ **N1.13** Vendor SLA + SBOM clauses

2 Adapt your fundamentals to AI-driven attacks

Accelerate what matters · Deprioritize the rest

Detection & Automated Response
CSA PA10 - Automated response

- ● **N2.1** Pre-authorized auto/fast-containment CSA.10
- ○ **N2.2** Behavioral detection & UEBA — vs AI emulation CSA.10
- ● **N2.3** Collective defense — sector/ISAC/CERT sharing
- ○ **N2.4** BAS validate detections
- ● **N2.5** Exfiltration monitoring + DLP
- ○ **N2.6** East-west / NDR anomaly detection

Hardening & Blast-Radius
CSA PA8 - Harden environment

- ● **N2.7** No-gap MFA (exposed) CSA.8
- ● **N2.8** Phishing-resist. MFA CSA.8
- ○ **N2.9** PAM / zero-standing-priv CSA.8
- ○ **N2.10** SSO/IGA + least priv
- ○ **N2.11** Non-Human Identity (NHI)
- ● **N2.12** Segmentation + DMZ CSA.8
- ● **N2.13** Browser isolation
- ○ **N2.14** Virtual patching (WAF/RASP/IPS)
- ○ **N2.15** Egress default-deny CSA.8
- ○ **N2.16** East-west API authz (service-to-service)
- ● **N2.17** Refresh IR playbooks
- ● **N2.18** Chained-0day tabletop
- ● **N2.19** Red-button — emergency disable
- ○ **N2.20** Tested recovery & immutable backups

Counter-Autonomy & Deception
CSA PA9 - Deception

- ● **N2.21** Deception — token-burner tarpits CSA.9
- ○ **N2.22** AI Agent decoys & tripwires (canary tokens) CSA.9

3 Use AI to defend at machine speed

Force multiplier (AI4Cyber) · Secure the AI itself (Cyber4AI)

Use AI on your code
CSA PA1 - Point agents at code

- ○ **N3.1** Agentic code review & vuln discovery — in the dev pipeline → propose-fix CSA.1
- ○ **N3.2** Continuous agentic pentest & red teaming CSA.1

Accelerate the defense team
CSA PA2 - Require AI adoption

- ○ **N3.3** SOC AI triage / copilots CSA.2
- ○ **N3.4** Mandate AI-agent adoption across security ops CSA.2
- ● **N3.5** Hybrid LLM — frontier + open-weight
- ○ **N3.6** AI4Cyber use case portfolio + FinOps

Defend agents & Shadow AI
CSA PA3 - Defend agents

- ● **N3.7** Defend agents (kill-switch) CSA.3
- ● **N3.8** Agent runtime proxy — mediate & log every action CSA.3
- ○ **N3.9** Agent circuit breakers — halt cascades
- ○ **N3.10** RAG security – poisoning + leak prevention
- ● **N3.11** Shadow AI & MCP discovery CSA.3
- ● **N3.12** MCP supply-chain integrity — signed/verified servers CSA.3
- ● **N3.13** Agent egress+DLP+SSRF guard CSA.3
- ● **N3.14** AI data governance

★ Govern the acceleration

The layer that lets you move at tempo

Risk, Assurance & Reporting
CSA PA6 - Update risk models

- ● **G.1** Readiness self-assessment
- ● **G.2** Re-baseline risk models — no patch grace, exploit-path severity CSA.6
- ● **G.3** Sec-vs-avail cut authority
- ● **G.4** No standing exceptions on exposed/on-path assets

Acceleration & Operating Model
CSA PA4 - Acceleration governance

- ● **G.5** Fast-track approval of new security controls CSA.4
- ● **G.6** Board brief + budget rebase
- ○ **G.7** Scale IT Ops capacity for continuous-patch volume CSA.4
- ● **G.8** Daily P0 vuln committee
- ● **G.9** Stop / pause low-value cyber initiatives
- ● **G.10** Workforce — AI social-engineering defense + team AI upskilling
- ● **G.11** AI agent authorization gate — scope, blast-radius, human override

CSA-critical · CSA-high · not CSA-rated · ● done < 90 d · ○ done > 90 d

Florian Pouchet
Head of Cybersecurity
florian.pouchet@wavestone.com

By 2030, accelerate cyber to reach real-time!

VISIBILITY

Increase Visibility

TRUST

Increase Trust

SPEED

Increase Speed

VALUE

Demonstrate Value

Want to know more?

Read the full article online

Or drop me an email
florian.pouchet@wavestone.com

Florian Pouchet

Head of Cybersecurity and Operational Resilience UK

florian.pouchet@wavestone.com


WAVESTONE

Panel discussion: Assurance and Oversight. What does “good” look like?

Facilitator

Mike Hughes Director, Prism RA, and ISACA Central UK

Panellists

Rolf von Roessing Partner, Forfa Consulting AG
Malcolm Kafesu IT Security & Governance Manager, Ontic
Steven Moore ICT Manager, The Legal Ombudsman
Jake Anthony Principal Solutions Engineer, Exabeam

End of Meeting

PLEASE SCAN HERE to...

- **Share FEEDBACK on today's event**
- **Suggest TOPICS for us to explore**
- **CHAIR one of our webinars**
- **SPEAK at a future session**
- **HOST one of our events**