C VISION INTERNATIONAL

AGENDA

Resilience at the Speed of AI

Cybersecurity Think Tank

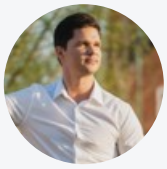
SPEAKERS



Wilbur Pires
CISO
Verizon



Henry Amadiegwu
CIO
Zenith Bank UK



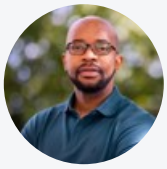
Mantas Marcinkevicius
CISO
Lloyd's List Intelligence



Christina Habib
C-Exec Customers Brands & Innovation | Non-Exec Boards & Strategic Advisory
Life Sciences Industry



Peter Hands
CISO
BMA



Don Mlambo
VP, Technology Audit
BlackRock



Enis Sahin
UK Head of Information Security
Federated Hermes

Click Here to Register

March 17, 2027

United Kingdom Time

Registration

8:30 AM-9:00 AM

Morning Networking

9:00 AM-9:30 AM

Opening Remarks

9:30 AM-9:40 AM

VISION VOICES KEYNOTE

9:40 AM-10:05 AM

Five Weeks Dark. What Britain's Biggest Attacks Taught Every Board About the First 29 Minutes.

In 2025 some of Britain's best known retailers and manufacturers watched stores, websites and production lines stop for weeks. Attackers can now move through a network in about half an hour, yet the decision to pull the plug often waits for a meeting. This keynote looks at who holds the authority to act in those first minutes, and how leading CISOs agree it with the board long before the night it is needed.

PANEL

10:10 AM-10:55 AM

Hire, Badge, Retire. Your Newest Employees Are AI Agents, and Nobody Checked Their References.

We spent twenty years learning how to trust people with access. AI agents and AI browsers are now joining the workforce, often hired by a business unit that forgot to tell security, and most of them never go through screening, onboarding or a last day.
This panel applies the employee lifecycle to digital workers. Who approves the hire, how an agent gets its badge and its manager, what a performance review looks like for software, and how to retire an agent cleanly so its access does not outlive its purpose.

Coffee Break

10:55 AM-11:15 AM

VISION VOICES

11:15 AM-11:30 AM

Is That Really Your CFO? Deepfakes, Help Desks and the Call That Cost Millions.

A familiar face on a video call, a calm voice asking for an urgent payment, a help desk asked to reset a password. Deepfakes have turned trust itself into an attack surface. In fifteen focused minutes, this session shows how the scams work and the simple checks that stop them.

PANEL

11:35 AM-12:20 PM

One Incident, Four Regulators. The UK Cyber Bill, DORA and NIS2 on One Very Bad Day.

UK security leaders are living through a remarkable convergence. The Cyber Security and Resilience Bill is close to becoming law, DORA and NIS2 reach every firm that serves Europe, and a single serious incident can mean reporting to the NCSC, the FCA, the PRA and the ICO on the same day.

This panel brings CISOs from regulated sectors together to compare notes. How they fold overlapping duties into one playbook, what supervisors are actually asking for, and how to turn compliance effort into genuine resilience rather than a mountain of paperwork.

Lunch

12:20 PM-1:20 PM

VISION VOICES

1:25 PM-1:45 PM

Hack Me If You Can. What an AI Red Team Found in 48 Hours.

The annual penetration test, with a thick report already out of date by the time anyone reads it, is giving way to something much faster. AI now lets red teams probe an organisation around the clock, and UK schemes such as the Bank of England's CBEST expect intelligence-led testing.

This session shares what continuous, AI-assisted red teaming finds that traditional testing misses, how to run it safely against live systems, and how to turn a constant stream of findings into fixes instead of fatigue.

DISRUPTOR

1:50 PM-2:05 PM

Your Supply Chain Now Has a Model in It.

Third party risk used to mean vendors, contractors and the software they shipped. Today it also means the foundation models you call, the open weights your developers download, the plugins and connectors your agents rely on, and the data those models learned from. Each one is a link in a chain you did not forge yourself.

This disruptor session maps the new AI supply chain and shows how to inventory it, assess it and set sensible guardrails without bringing innovation to a halt.

PANEL

2:10 PM-2:55 PM

The Patch Window Closed. What Replaces Thirty Days When AI Finds the Bugs First.

For years, security teams worked to a comfortable rhythm of thirty, sixty and ninety days. That rhythm is breaking. AI can now uncover and weaponise weaknesses that organisations have tolerated for years, and the UK's National Cyber Security Centre has warned leaders to prepare for a sharp rise in incidents as a result.

Our panellists share how they decide what gets fixed in hours, what happens to the systems that cannot be patched, and how they finally win the budget to retire the technology everyone has been meaning to replace. Bring your phone: the room votes, and the results are revealed at the close.

Networking Break

2:55 PM-3:15 PM

VISION VOICES

3:15 PM-3:30 PM

Secure by Design Becomes Law. Three Questions to Ask Every Supplier on Monday.

For decades, the cost of insecure software landed on the customer. You bought it, you patched it, you lived with the consequences. New rules, led by Europe's Cyber Resilience Act, are pushing that responsibility back to the people who build the products.
In fifteen minutes, this session turns that shift into action: the three questions to put to every supplier, what changes for the software you build yourself, and how to use this moment to raise the floor for everyone.

FIRESIDE CHAT

3:35 PM-4:10 PM

Off the Record. London Security Leaders on the Night Everything Went Wrong.

Every security leader has a night they will never forget. The breach that taught humility, the board meeting that changed how they speak, the warning they ignored once and never again.
Under the Chatham House Rule, this closing fireside shares the decisions, mistakes and lessons that rarely make it onto a stage. Honest, warm and practical, it is the conversation you usually only have late at night after an event, offered here to everyone in the room.

Closing Remarks, Poll Reveal & Raffle Giveaway

4:10 PM-4:20 PM

Cocktail Reception

4:20 PM-5:30 PM

PARTNERS

We are currently accepting partnership opportunities for this event.