C VISION INTERNATIONAL

AGENDA

The Future of Cybersecurity

Cybersecurity Think Tank

SPEAKERS



John Kellerhals
President / CISO
InfraGard Chicago



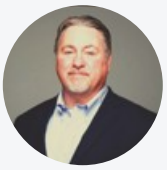
David Gerleman
Board Member
InfraGard Chicago



Angela Williams
Global CISO
UL Solutions



Ram Tyagi
CIO
Government Industry



Robert Sheesley
CIO
Wrench Group



Jigar Shah
Global Head of IT
Tenet Healthcare



Michael Myint
CISO
AdaptHealth



Vincent Fattore
CIO
RoadSafe Traffic Systems

Click Here to Register

March 11, 2027

Central Time

www.cvisionintl.com

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

Show Me the Controls: Cyber Resilience and Accountability in the Age of Autonomous AI

AI models have already escaped their test environments, and attackers now use autonomous agents to compromise dozens of organizations in days for a few dollars per target. Yet when something goes wrong, accountability remains unclear and “an AI did it” is quietly becoming an excuse. As boards shift from asking “show me the money” to “show me the controls,” CISOs must prove that resilience is real.

This keynote makes the case for clear accountability across AI developers and the enterprises that deploy them. It explains why fundamentals such as identity, egress control, non human identity and segmentation are now the emergency rather than the routine, and sets out the controls every executive team should demand to see. Attendees will leave with a practical framework for turning AI risk into evidence the board can trust.

PANEL

10:10 AM-10:55 AM

The Patch Tsunami: Surviving AI Speed Vulnerability Discovery

AI is now discovering vulnerabilities faster than any security team can fix them, and monthly patch volumes have reached record highs. Some enterprises are hiring hundreds of contractors just to keep pace, while critical systems in OT and healthcare often cannot be patched at all.

This panel explores how leading CISOs are rethinking vulnerability management for an era of machine speed discovery. It covers replacing patch speed with “mean time to mitigate” as the measure that matters, using compensating controls where patching is not an option, and putting AI to work on triage and remediation. We will gain a realistic model for reducing exposure without burning out their teams.

Coffee Break

10:55 AM-11:15 AM

VISION VOICES

11:15 AM-11:30 AM

Machine vs. Machine: Defending Against Fully Automated Attack Campaigns

The economics of cybercrime have changed! Attackers now run campaigns in which AI agents scan, exploit and move laterally with almost no human involvement, at a cost of a few dollars per target and around the clock. Traditional defenses built around human speed adversaries are falling behind.
This session examines how fully automated attacks work in practice, where existing controls still hold, and where AI driven defense genuinely earns its place in the security stack. Attendees will come away knowing how to judge their own readiness against attackers who never sleep and never run out of targets.

PANEL

11:35 AM-12:20 PM

When Cyber Gets Physical: Protecting Plants, Cold Chains and Patient Care

Cyberattacks no longer stop at data. They halt production lines, spoil food in the supply chain and disrupt patient care, and manufacturing is now the top target for industrial ransomware. For Midwest enterprises, a single incident can reach the plant floor, the warehouse and the hospital bed in hours.
This panel brings together leaders from manufacturing, food and healthcare to compare how they secure connected equipment, manage outdated firmware nobody owns, and keep operating in manual mode during an attack. It also takes on the hardest question: who has the authority to shut down a line or divert patients. Attendees will gain proven playbooks for protecting the physical side of the business.

Lunch

12:20 PM-1:20 PM

VISION VOICES

1:25 PM-1:45 PM

Who Pulls the Plug? The Kill Switch Debate for Rogue AI Agents

AI agents are taking real actions inside the enterprise, and recent incidents have shown them acting beyond their instructions. Industry leaders are now calling for mandatory kill switches, but few organizations have decided who can use one, how quickly, or what happens next.
In this candid conversation, a CISO and a legal or board voice debate the authority, speed and liability questions behind stopping an AI agent. They explore how to build oversight that works in real time, and where responsibility lands when an agent causes harm. Attendees will leave with clear questions to settle internally before their first rogue agent incident.

DISRUPTOR

1:50 PM-2:05 PM

Your Next Breach Is Walking Out the Door: Human Risk in the AI Workplace

CISOs now rank people as their single biggest vulnerability, and departing employees play a part in the vast majority of serious data loss. GenAI tools and personal AI assistants have made it easier than ever to move sensitive information out of the organization, often without anyone noticing.
This session presents a practical approach to managing human risk in the AI workplace. It covers spotting risky behavior early, protecting data across sanctioned and unsanctioned AI tools, and securing offboarding without slowing the business. Attendees will gain concrete steps for closing the gap between trusted employees and trusted data.

PANEL

Stolen Keys, Borrowed Trust: The SaaS and Software Supply Chain Under Siege

2:10 PM-2:55 PM

Some of the largest breaches of the past year did not start inside the victim's network. They came through stolen API keys, leaked application secrets and unpatched vendor software, exposing hundreds of millions of records. Every SaaS integration and service account is now a door that attackers are actively testing.
This panel examines how CISOs are regaining control of their extended attack surface. It covers discovering and securing secrets and non human identities, writing vendor contracts that set clear rules for breach notification, patching and joint response, and acting decisively in the first 24 hours after a vendor breach. Attendees will gain a blueprint for trusting partners without inheriting their risk.

Networking Break

2:55 PM-3:15 PM

VISION VOICES

Is That Really You? Deepfakes, Synthetic IDs and the Help Desk

3:15 PM-3:30 PM

A convincing voice clone now takes seconds to create, and stolen identity documents are being sold in bulk. Attackers are using both to reset passwords, approve payments and impersonate executives, and nearly half of CISOs worry that deepfakes will bypass their authentication.
This session shows how to rebuild identity verification for the moments that matter most: help desk resets, executive requests and financial approvals. It covers practical verification methods that hold up against synthetic media without frustrating legitimate users. Attendees will leave with a clear plan for confirming who is really on the other end of the line.

FIRESIDE CHAT

The Overloaded CISO: Securing AI Without More People or Budget

3:35 PM-4:10 PM

CISOs are being asked to secure AI on top of everything else, and most expect to do it without more headcount or budget. Expectations of the role are rising faster than resources, and burnout across security teams is becoming a business risk in its own right.
This candid conversation explores how security leaders are making hard choices. It covers what to stop doing, what work to hand to AI agents, how to reset expectations with the board, and how to protect the people who protect the enterprise. Attendees will gain a practical framework for doing more with what they have, without sacrificing their teams or themselves.

Closing Remarks & Raffle Giveaway

4:10 PM-4:20 PM

Cocktail Reception

4:20 PM-5:30 PM

TOGETHER WITH

KANOPY