C VISION INTERNATIONAL

# AGENDA

The Future of Cybersecurity

# Cybersecurity Think Tank

## SPEAKERS



**Oliver Wyler**
Group CISO
Bank Vontobel



**Katherine Elikwu**
CISO
VARO Energy



**Philip Skiba**
Director IT Risk
CACEIS Bank



**Przemyslaw Potrzasaj**
Cloud Architect - Associate Director
UBS



**Jean-Luc Turin**
Identity and Access Governance Director
JTI (Japan Tobacco International)



**Morgan Rosier**
IT Director
Alcon

**Click Here to Register**

**June 02, 2027**

Central European 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**

## 29 Minutes in Zurich. Who Gets to Act Before the Attacker Does?

The average attacker now moves from a first foothold to the rest of the network in about 29 minutes. Swiss banks, insurers, pharmaceutical companies and manufacturers run operations where an hour offline is measured in trades, production batches and client trust built over generations. Yet in many organizations the decision to isolate a system, cut a supplier connection or take a revenue platform offline still waits for a meeting and an executive who may be on a plane.
This opening keynote looks at the human side of speed. Who holds the authority to act in the first half hour, what they are allowed to break without asking, and how leading CISOs agree those decision rights with the CEO, the business and the board long before the night they are needed. The fastest response, it turns out, is the decision that was already made.

PANEL

**10:10 AM-10:55 AM**

## Hire, Badge, Retire. Running the Full Employee Lifecycle for AI Agents.

We spent twenty years learning how to trust people with access. We screen them, onboard them, give them only what they need, review their work and collect the badge on their last day. AI agents are now joining the workforce, often hired by a business unit that forgot to tell security, and most of them never go through any of those steps.
This panel borrows the employee lifecycle and applies it to digital workers, one stage at a time. 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. Expect honest stories, the controls that held up, and the ones that did not.

## Coffee Break

**10:55 AM-11:15 AM**

VISION VOICES

**11:15 AM-11:30 AM**

## The Browser Grew Hands. Securing AI Browsers That Click, Type and Buy for Your People.

The browser used to be a window. Now it is becoming a worker. AI browsers and assistants can read a page, fill in a form, approve a request and complete a purchase on someone's behalf, and a single hidden instruction tucked inside a web page can redirect all of it. In fifteen focused minutes, this session explains why the browser has become one of the most important places to defend, what prompt injection looks like when it meets real credentials, and which simple policies let your people enjoy the help without handing the keys to whoever wrote the page.

PANEL

**11:35 AM-12:20 PM**

## One Incident, Two Rulebooks. Swiss Reporting Duties Meet NIS2, DORA and the Cyber Resilience Act.

Swiss security leaders live at a busy crossroads. At home, a serious attack can mean a 24 hour report to the Federal Office for Cybersecurity, a notification to FINMA for banks and insurers, and a report to the Federal Data Protection and Information Commissioner when a breach puts personal data at high risk. Across the border, NIS2, DORA and the Cyber Resilience Act reach Swiss companies that serve European customers, run operations in the EU or supply its regulated firms. A single incident can now set several clocks running at once.
This panel brings CISOs from regulated sectors together to compare notes. How they fold overlapping duties into one playbook, what supervisors on both sides of the border 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**

## Think Like the Attacker. Why Swiss Security Leaders Are Investing in Offense Again.

For a long time, offensive security meant the annual penetration test, a thick report and a list of findings that was already out of date by the time anyone read it. AI has changed the economics on both sides. The tools attackers use to probe your defenses around the clock are now in your hands too, and security leaders are investing in offense again with real urgency.
This session explores continuous, AI assisted red teaming. What it 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**

## Who Built Your AI? Mapping the New Supply Chain Behind Swiss Enterprises.

Switzerland learned the cost of a weak link in 2023, when a ransomware attack on a single IT supplier led to the leak of sensitive federal government data. 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

## Small Country, Global Reach. When World Events Reach Swiss Networks.

**2:10 PM-2:55 PM**

Swiss companies are global by nature. Banks, insurers, commodity traders, pharmaceutical and industrial leaders run teams, suppliers, data centers and customers across the world, and international organizations from Geneva to Basel connect the country to every continent. A regional outage, a disruption at a key supplier, a sudden change in data rules or a wave of attacks aimed at one industry can cross borders and arrive in your logs before the morning news has caught up.
This panel helps security leaders see further. How to build threat intelligence that reflects where you actually operate, how to plan for the loss of a key supplier or region, and how to brief a board that wants to understand global risk in plain business terms. It is a conversation about preparation, so your organization is never the last to know.

## Networking Break

**2:55 PM-3:15 PM**

VISION VOICES

## One Call Away. Verifying Humans When Any Voice Can Be Cloned.

**3:15 PM-3:30 PM**

Some of the most damaging breaches of recent years began with a friendly phone call. An attacker poses as an employee, the help desk resets a password or a login device, and within the hour the intruder is inside with legitimate access. AI voice cloning and convincing video calls have made that call easier to fake than ever, and in a country where the same help desk may take calls in German, French, Italian and English, the pressure to be helpful is constant.
In fifteen focused minutes, this session shows how to rebuild trust for the moments when a human asks for help. Stronger proof for resets, safe words and call back rules for executives, and training that helps support teams say no kindly.

FIRESIDE CHAT

## What I Wish I Had Known. Security Leaders on the Decisions That Shaped Them.

**3:35 PM-4:10 PM**

Every CISO carries a private library of moments. The breach that taught humility, the board meeting that changed how they speak, the hire that transformed a team, the warning they ignored once and never again. These stories rarely make it onto conference slides, yet they are where real wisdom lives.
This closing fireside invites seasoned security leaders to open that library. 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, especially those still writing the first chapters of their own careers.

## Closing Remarks & 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.*