Interconnected by design: The convergence of IT, OT and CPS

Thursday 12 November 2026

Chair

Professor Andrew Clark
Content Advisor, SASIG

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; laptops should not be used in the room, 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

Rethinking Operational Resilience in an Era of Geopolitical Risk
11am, Friday 13 November

Communicating Cyber Risk: Enhancing Cyber Resilience through Compelling Communication
11am, Monday 16 November

The Business Case for AI Security: Aligning CISOs and CFOs on Agentic Risk
11am, Friday 20 November

AI SOC Build vs Buy: What Happens After the Prototype In Production
2pm, Monday 23 November

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

Upcoming in-person events

SASIG of the North
Thursday 19 November, Manchester

Financial Services SASIG
Thursday 26 November, London

SASIG Christmas Luncheon
Tuesday 8 December, London

CNI Critical National Infrastructure SASIG
Thursday 14 January, London

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

Help Shape the Future of the UK Cyber Security Sector

If your organisation develops or provides cyber security products or services, we'd encourage you to take part in the UK Cyber Security Skills and Sector Study, commissioned by the Department for Science, Innovation and Technology (DSIT).

Scan the QR code to complete the survey

Your input will help inform government policy, measure sector growth, and identify future skills and workforce needs.

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.

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.

Interconnected by design: The convergence of IT, OT and CPS

Thursday 12 November 2026

Chair

Professor Andrew Clark
Content Advisor, SASIG

Keynote presentation: Why should I be bothered?

Peter Wood
Lead Consultant, Naturally Cyber

N@turally Cyb3r

Why should I be bothered?

The invisible attack surface



Peter Wood

N@turally Cyb3r

Helping companies develop cyber security instincts

Peter Wood

N@turally Cyb3r

- Lead Consultant at Naturally Cyber
- Engineer, IT and security professional for over 50 years
- Founded one of UK’s first cyber security firms in 1989
- Fellow of the BCS, Chartered IT Professional, CISSP
- Security evangelist
- Car enthusiast
- Occasional musician

Hackable supermarkets

N@turally Cyb3r



ID 462199296 | © Yuliia Brunner | Dreamstime.com

12 October 2026

Hundreds of French supermarkets hit by a cyber attack that caused their fridges and freezers to heat up, spoiling fresh and frozen food estimated to be worth millions of euros.

Hackers gained control of the software that regulates the temperatures of the refrigeration units, forcing some to warm to 50C (120F) overnight, according to one supermarket chain affected.

https://www.bbc.co.uk/news/articles/crq5nzxv9q4yo

Hackable fish tank

N@turally Cyb3r



In 2017 a North American casino had a smart thermometer in the lobby aquarium, connected to the network.

Attackers found a vulnerability in the thermometer, used it as a foothold, moved laterally to the casino's high-roller database, and pulled 10GB of data back out – through the thermometer – to a device in Finland.

Not the actual fish tank!
https://www.flickr.com/photos/davidstanleytravel/8226785671/

Some boring basics

N@turally Cyb3r

Term	Defining question	Authority	Example
IT	Does it process, store or move information?	—	ERP, email, cloud storage
OT	Does it monitor or directly cause change in the physical world?	NIST SP 800-82	SCADA, PLC, building automation
IoT	Is it an internet-connected device reporting on or lightly interacting with the physical world, managed individually?	NISTIR 8228	Smart thermostat, IP camera, badge reader
CPS	Does it close the loop — sense, compute and act on the physical world in real time, with OT/IoT as its components?	Gartner / NIST CPS framework	Smart grid, autonomous vehicle, self-regulating BMS

Surely it’s only manufacturing at risk?

N@turally Cyb3r

The Jaguar Land Rover cyberattack is widely considered the most economically damaging cyber event in UK history, incurring an estimated total cost of £1.9 billion.





A cybercriminal collective called “Scattered LAPSUS$ Hunters” reportedly deployed ransomware, used social engineering, and compromised internal SAP management systems.

Office-based firms haven't (*yet*) had their Jaguar Land Rover moment.

When OT or physical exposure doesn't look like a traditional factory floor with assembly lines and heavy machinery, organisations frequently fall into a false sense of security.

Why is there a problem with OT?

N@turally Cyb3r

Visibility gap: Only 46% of assessed OT environments have adequate network monitoring in place *(Dragos, 2026)*

Ownership going backwards: CISO/CIO ownership of OT fell from 69% to 60% in a year *(Fortinet, 2026)*

Intrusions climbing: 71% of industrial organisations reported between one and nine intrusions in the past year, up from 47% *(Fortinet, 2026)*

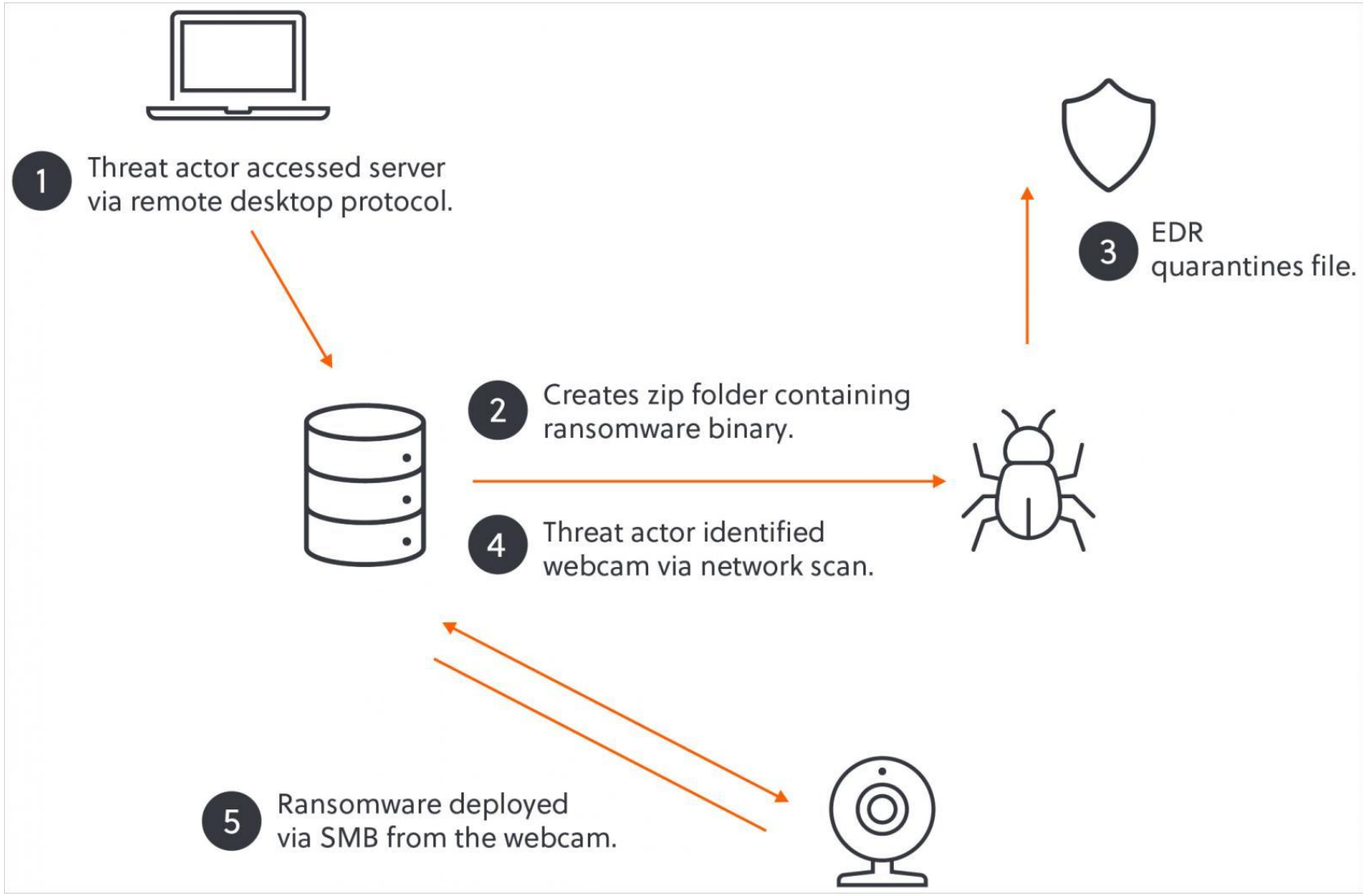
Legacy-by-design weakness: Many OT/CPS systems were built for availability and functionality, not security – default passwords, no encryption, unpatched firmware still common

Why ‘invisible’ matters

N@turally Cyb3r

2025: Webcam ran lightweight Linux OS with remote shell capability and no EDR* support (too little storage to run an agent)

Which is exactly why it was invisible to the security tooling even though it sat on the same network

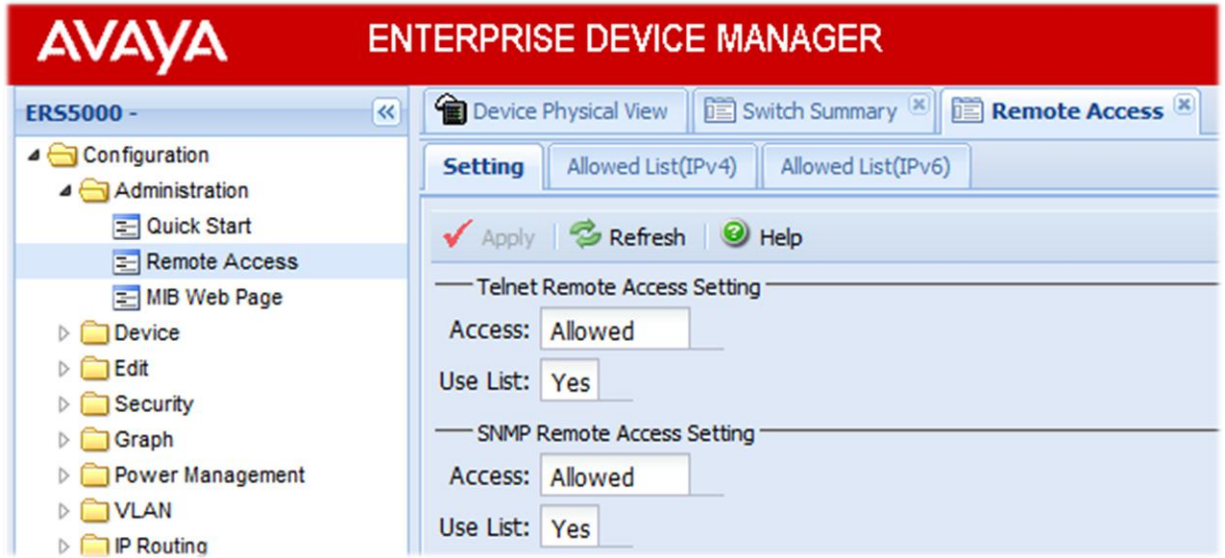


Source: S-RM
https://www.s-rminform.com/latest-thinking/camera-off-akira-deploys-ransomware-via-webcam

**Endpoint Detection and Response*

Invisible infrastructure: accessing IT and IoT

N@turally Cyb3r

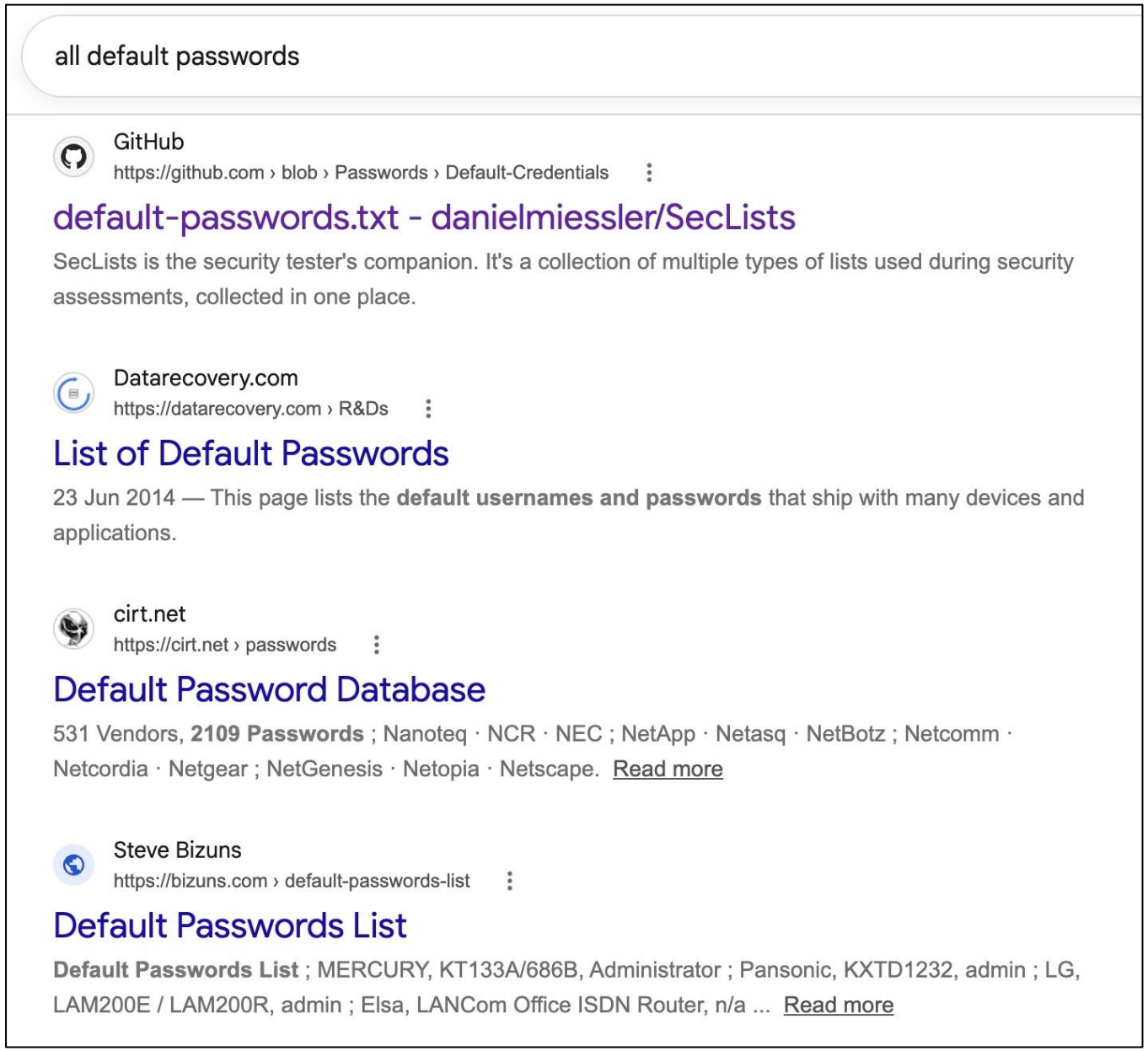




- Most networks have devices like these - installed and forgotten
- Blank admin passwords means no authentication
- Anyone can cause a denial of service with that device manager
- Anyone can snoop throughout the building with the CCTV

Invisible infrastructure: accessing IT, OT, IoT and CPS

N@turally Cyb3r

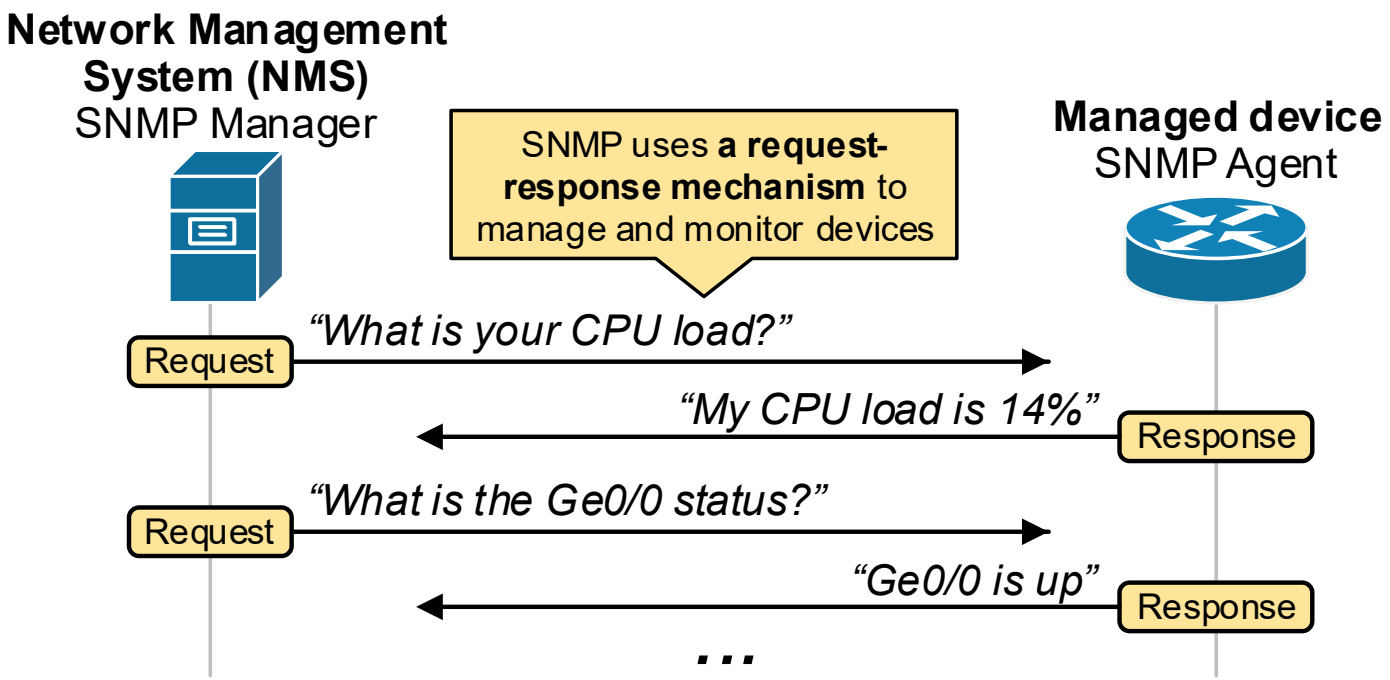


- Almost every network we've tested has devices using default admin passwords
- Gaining access to the infrastructure is easy
- Intercept traffic
- Pivot to other devices
- Install backdoors
- Control the network silently

Google result 23/10/2026

Mapping (or hacking) networks with SNMP

N@turally Cyb3r



- Map the network
- Enumerate users
- Dump configurations
- Crash the network repeatedly
- Modify settings with read/write
- Cause chaos!

https://cdn.networkacademy.io/sites/default/files/2025-01/what-is-snmp.svg

Should you be bothered?

N@turally Cyb3r

- **Find it:** include facilities and building systems in asset discovery
- **Own it:** who signs off the risk for each device?
- **Test it:** include default credentials and SNMP community strings in the pen test scope
- **Map the minimum viable company:** what has to keep running, and what it depends on





N@turally Cyb3r

Helping companies develop cyber security instincts

https://naturallycyber.com

Peter Wood

pete@barnes-wood.com

Panel discussion: The landscape

Led by Liz Murray Chief of Staff, SASIG

Panellists
Tim Harwood CEO, Siker Cyber
Abel Archundia-Pineda VP Global Operational Technology, Kudelski Security
Peter Wood Lead Consultant, Naturally Cyber
Tim Nursall Sales Director, Cymulate

Tea, coffee & networking break

We'll be back at 11.15am

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





Securing the factory that builds the factory

Matt Campbell
Senior Security Solutions Architect, Qualys

SASIG - INTERCONNECTED BY DESIGN - 12 NOVEMBER 2026

Securing the factory that builds the factory

CI/CD for operational technology, and the security of the physical product at the end of the line

Matthew Campbell, Qualys

The factory I grew up in...



Regulation now requires OT products to be updated for their whole support life

EU PRODUCT LAW

Cyber Resilience Act

Security updates for the support period, reporting required from Sept 2026

AUTOMOTIVE

UNECE R156

Certified software update management for type approval

INDUSTRIAL

IEC 62443-4-1

Security update management in the product life cycle

MEDICAL

EU MDR GSPR 17.2

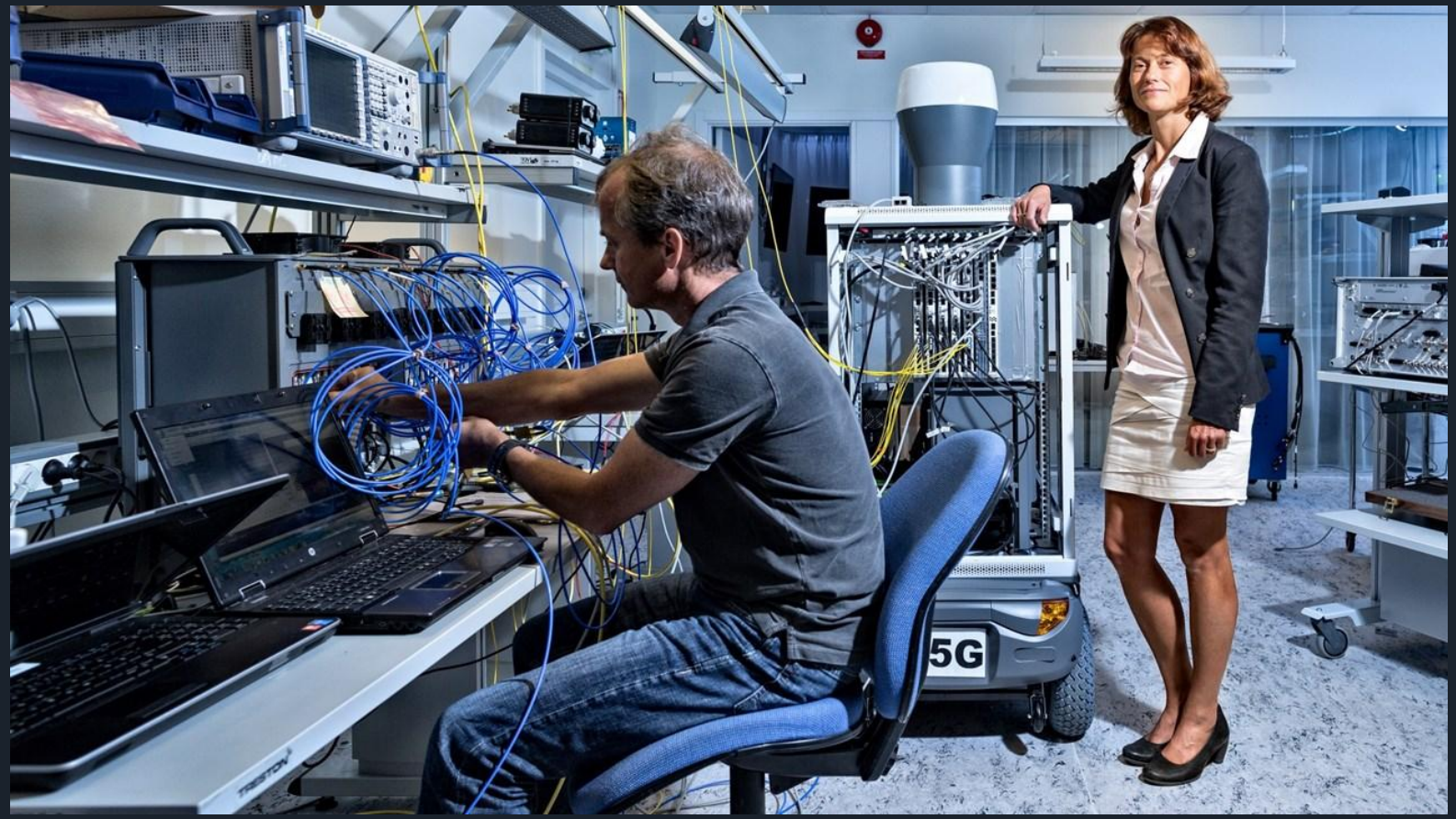
Cyber devices must be secure and patchable after release

OUTCOME

Years of security updates means a release pipeline, not a one-off certification.

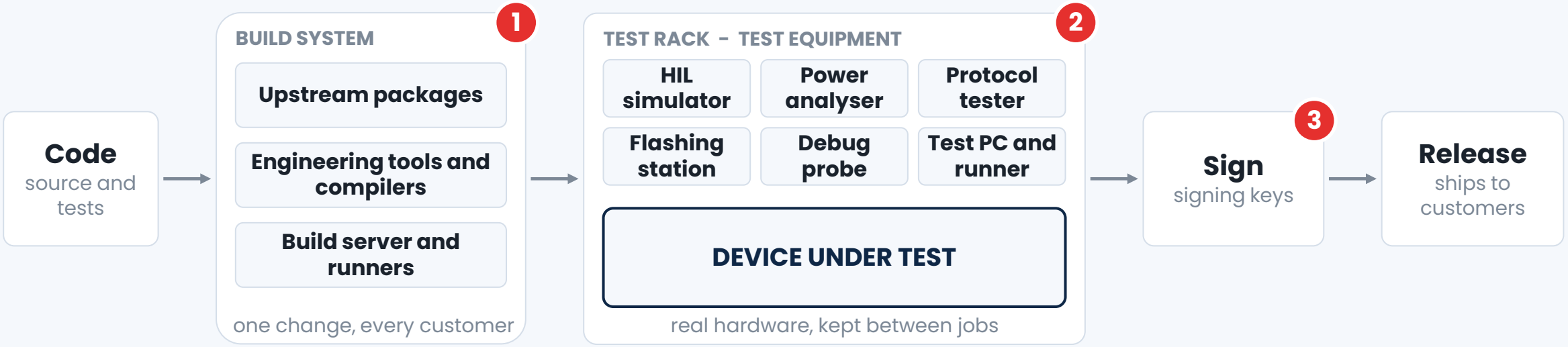
THE ARGUMENT

The pipeline that builds and tests OT products is itself an OT system.



It is usually managed like IT. That affects the security of the product at the end of the line.

Three places where a weak pipeline harms the product directly



1. **The build trusts whatever it is fed**
2. **Whoever controls the rig controls the result**
3. **A signature says who built it, not what was built**

Attacks on the build



Change one input to the build and every device built from it carries the change, shipped and signed by the vendor.

SHARP7EXTEND 2025

A fake copy of Sharp7, the .NET library used to talk to Siemens S7 PLCs, published on NuGet. It worked normally, then made PLC writes fail silently and killed processes at random.

INPUT ATTACKED: DEPENDENCY

JUNIPER 2012–2015

Attackers changed code on the server that prepared ScreenOS releases. Two compromises shipped in official firewall updates for three years.

INPUT ATTACKED: BUILD INFRASTRUCTURE

Sources: Socket, 6 Nov 2025; Juniper JSA10713, Dec 2015; Bloomberg, 2 Sep 2021

Whoever controls the rig controls the result

Code → Build → **Test rack** → Sign → Release

NI VERISTAND - CVE-2024-6806

No login needed to run code on the system that applies stimulus, scales readings and decides pass or fail.

TEKTRONIX MDO - CVE-2026-111853

OS commands as a privileged user, through the same SCPI channel the test reads measurements over.

THE POINT

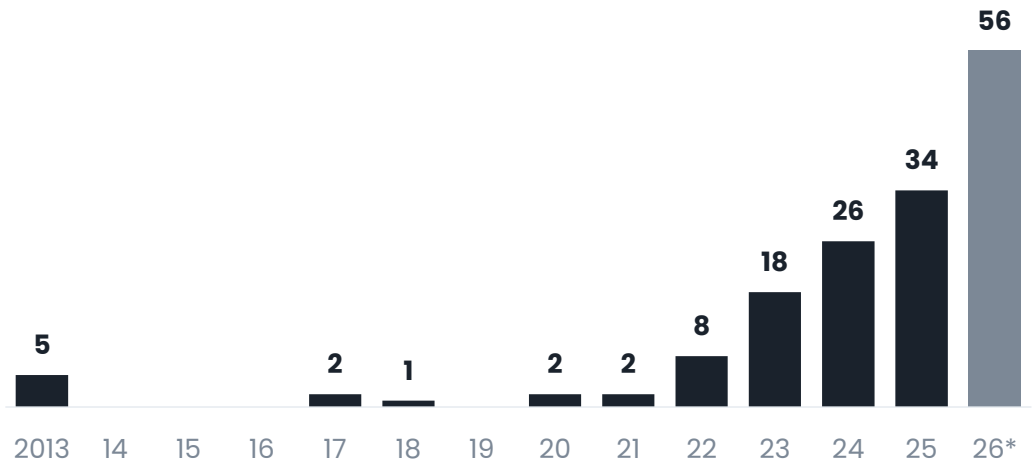
Neither is known to be exploited. Either lets a failing build pass using normal rig features.

Sources: NI; ZDI-24-1027; Tektronix TEK-PSA-002-092026; Mitsubishi Electric investigation report, 1 Oct 2021

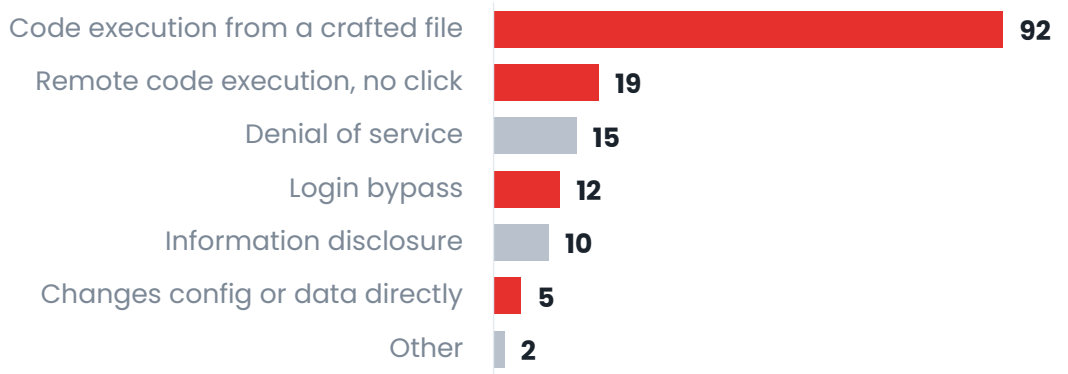
155 CVEs in test equipment, most of them since 2023

Code → Build → **Test rack** → Sign → Release

CVES PUBLISHED PER YEAR



WHAT THEY LET AN ATTACKER DO



THREAT **56 so far this year. 40 need no login and no click. None known exploited, yet.**

Sources: NVD; CVE.org; CISA ICS advisories and KEV; NI security advisories. Survey of instruments and test software, 6 Nov 2026. *2026 to 6 Nov.

2 - 3 - SIGN

A signature says who built it, not what was built

Code → Build → Test rack → **Sign** → Release

MSI 2023

Leaked keys: image signing 57 products, Boot Guard 116

Leaked with MSI's source code by a ransomware gang. Boot Guard keys are fused into the CPU and cannot be revoked.

BO TEAM 2025

Months inside a Russian industrial software vendor. Owned every domain, then reached its code-signing server. A backdoor there was blocked, but logs wiped.

SIGNING ZONE

off the corporate domain, own admins

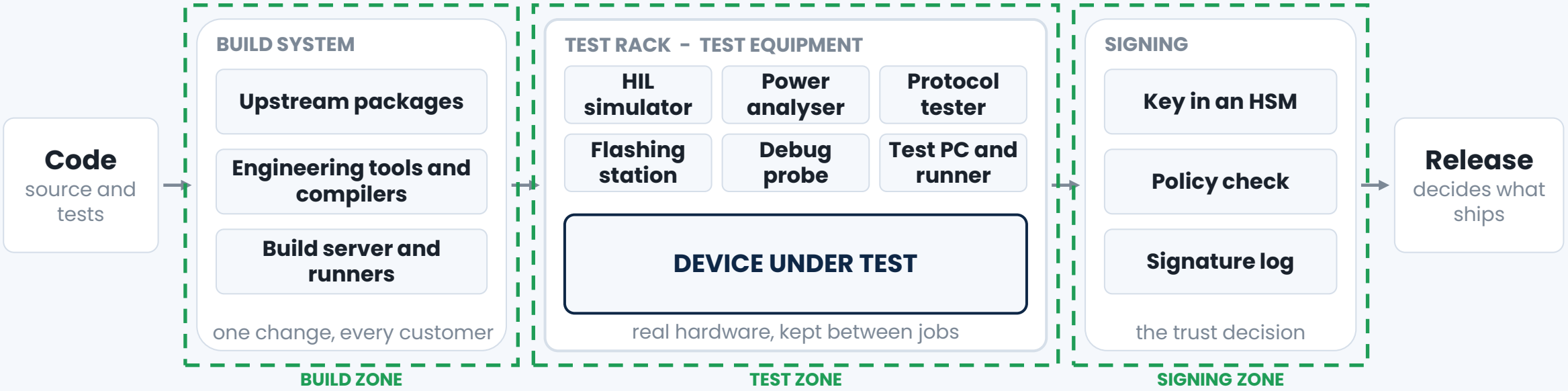
Key in an HSM
no key file to read or copy

Authorise each signing
ideally with automated checks

Logging and audit
kept separately with review process

Sources: Binarly via BleepingComputer, May 2023; Kaspersky ICS CERT, 5 Nov 2026; The Record, 2 Jun 2025; CERT Polska; CISA/FBI AA26-097A

The plant's playbook, applied to the pipeline



ISOLATE — SR 5.1, 5.2

Zones and conduits between rack, build, signing and corporate network

BASELINE — SR 3.4, 7.8

Rig firmware, instrument settings, test code. Detect change instead of rebuilding

MONITOR — SR 6.2

Passive OT network monitoring on the lab network, east-west too

COMPENSATE — Clause 4.3

Allow-list what talks to each instrument, jump hosts, documented countermeasures

Requirements: IEC 62443-3-3:2013 (SR = system requirement; clause 4.3 = compensating countermeasures). Zones: IEC 62443-3-2.

FROM THE PRACTITIONER

"Zoning the CI flow is vital. Access control, firewalling, and security risk assessment is needed for all phases of product test."



Security Architect, Radio Software Sub System Verification, Ericsson

How Do You Know Your Security Works Across IT, OT and AI?

Tim Nursall
Sales Director, Cymulate

cymulate

How do you know your security works across IT, OT and AI?

Validate Threats.
Build Exposure-Informed Defences.

SASIG · Interconnected by design: the convergence of IT, OT and CPS
London · 12 November 2026 · Tim Nursall, Cymulate

cymulate

ABOUT CYMULATE

Cymulate brings validation and security engineering into one platform to continuously prove, prioritise and adapt

Customers
1,000+ customers

Offensive security
>20 Elite cyber security researchers

History of Innovation
Founded in 2016
30+ awards for leadership & analyst recognition

Global footprint
Operating at 50+ countries

Trusted by Customers
Global organisations validating security controls with Cymulate.

Coca-Cola, Microsoft, SONY, sanofi, BNP PARIBAS, standard chartered, DELL, LUXOTTICA, Chevron Phillips, Nestlé, kyndryl, Raiffeisen Bank International, LATAM, Hitachi Energy, RALPH LAUREN, SIEMENS Healthineers, tsmc, GLENCORE





>300 5-star reviews

Cymulate
4.8 ★★★★★ (164)
Willingness to Recommend 94%

cymulate

THE INDUSTRY PROBLEM

Attackers got AI.
Defenders got more tickets.

1. AI finds vulnerabilities faster than we can fix them.
2. Teams can't tell which ones actually matter.
3. Compliance says we're safe. Breaches say otherwise.
4. Convergence connects all of it to the plant floor.

AI finds vulnerabilities faster than we can fix them

23,019

findings from one AI project in a month

Plus 48,185 CVEs published in 2025, up 20%

WORKING EXPLOITS WRITTEN BY THE AI



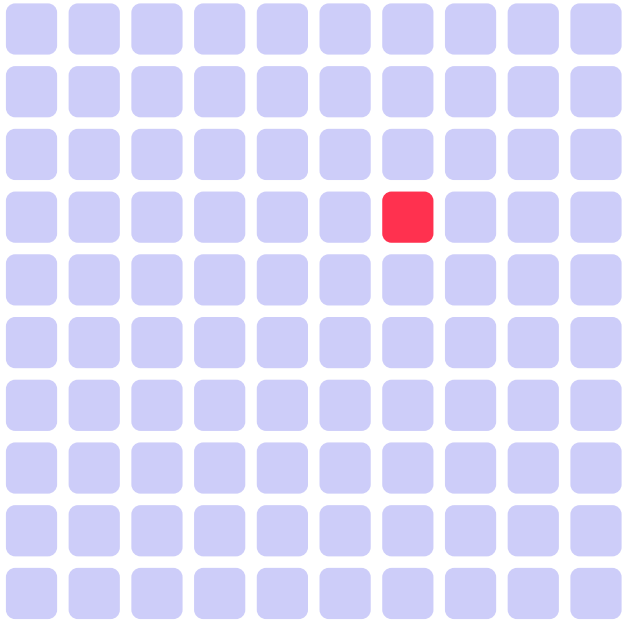
90× more working exploits than the previous model

Finding is solved. Fixing is the bottleneck.

cymulate

Sources: Anthropic, Mythos Preview & Project Glasswing (anthropic.com/research); jerrygamblin.com 2025 CVE review

Teams can't tell which vulnerabilities matter



>90%

of CVEs are never exploited in the wild

≈1 in 100 is exploited

~130
new CVEs published every day

32%
of exploited CVEs are hit on or before disclosure day

So teams patch by severity score, and work the wrong list.

Sources: VulnCheck 2026 Exploit Intelligence Report & 1H 2025 report (vulncheck.com); jerrygamblin.com

Compliant is complacency

JAGUAR LAND ROVER, 2025

ISO 27001 certified

£800m IT & cyber deal

Breached anyway.

£1.9bn

cost of the JLR breach to the UK economy



5 weeks of halted production

Without validation, security is an assumption.

Sources: Cyber Monitoring Centre (Oct 2025); Tata Motors / TCS (Sept 2023); public reporting on JLR, M&S and Co-op, 2025

Supplier access is now an attack path

Third-party support

Vendors, OEMs and integrators

VPN, RDP, SSH, screen share
Supplier accounts and laptops

1 **Supplier access is switched on**

Owned by the supplier

Level 2.5 industrial DMZ

Where IT and OT meet

Vendor VPN and jump hosts
File transfer and monitoring

2 **A valid account reaches a jump host**

Owned by network teams

OT and CPS

Operations and physical systems

MES, historians, OT apps
HMI, SCADA, building systems

3 **The path extends to HMIs and OT apps**

Owned by OT engineering

119 ransomware groups targeted industrial organisations in 2025, up from 80

3,300 industrial organisations impacted by ransomware in 2025

5 vs 42 days to contain OT ransomware with full OT visibility, vs the average

In OT you can't patch at AI speed. Prove the path is closed.

cymulate

Source: Dragos 2026 OT/ICS Cybersecurity Year in Review (Feb 2026)

THE MANUAL GRIND

You're already fighting back, by hand.

You take real action against threats. Each move is manual, slow and unowned, and every attempt to automate feels broken.



Organisations can’t prove which risks are real. So they fix the wrong things, slowly.

Prove

what's exploitable, here

Prioritise

what reduces real risk

Adapt

defences continuously

The industry has to close the risk-to-fix gap.

WHAT GOOD LOOKS LIKE

Test like an attacker. Fix like an engineer.

Attack

Safely run real attacker techniques against your live defences.



Measure

See what was blocked, what was detected and what got through.

Fix

Push rule and policy updates to your controls, then re-test.

Prioritise

Rank fixes by what's proven exploitable, not by CVSS score.

Agentic routines need to build validation into every security programme.

Agentic Cyber Defence Engineering

Defence Optimiser

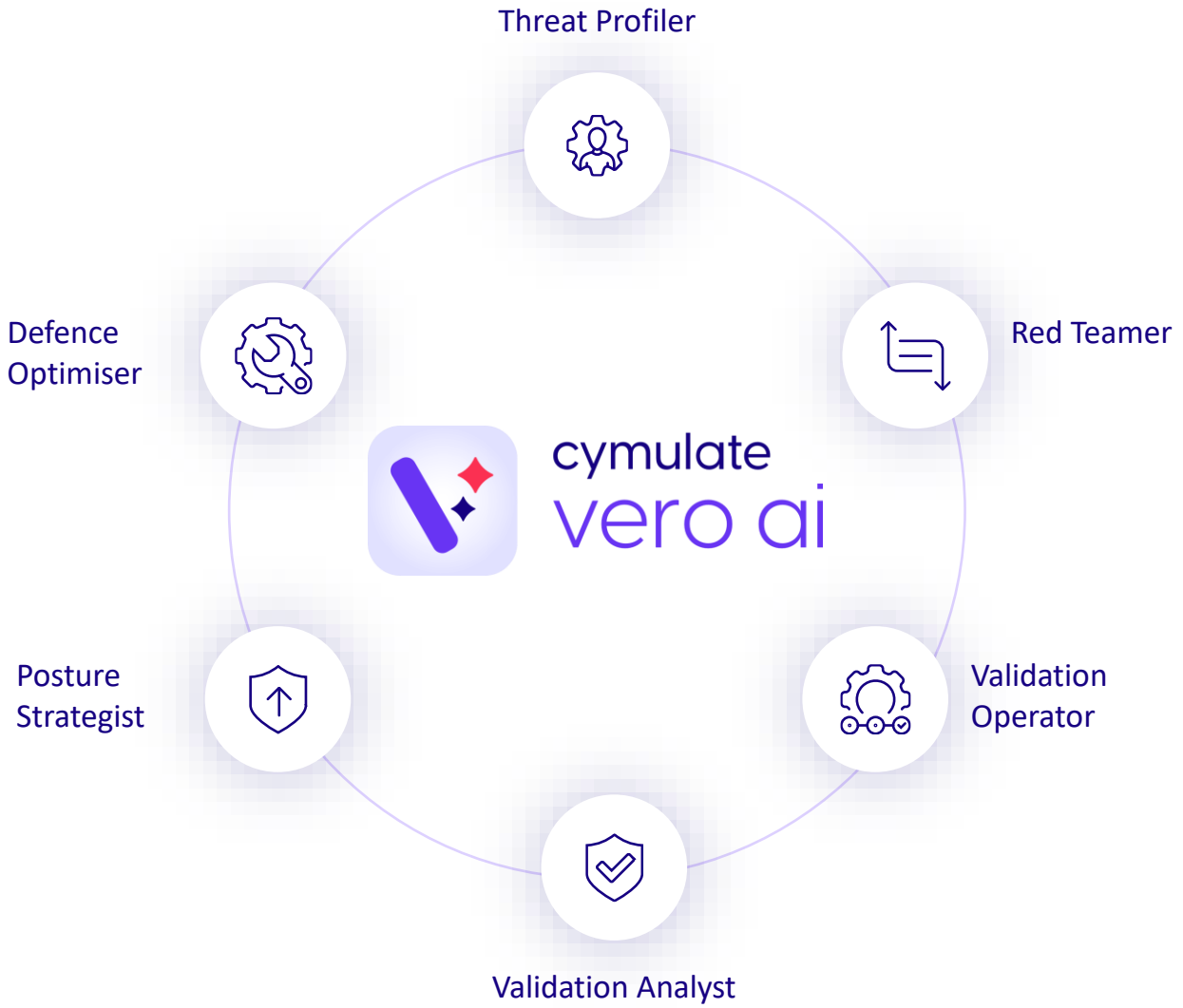
Pushes control and detection updates into your security stack.

Posture Strategist

Ranks fixes by proven real-world impact, not theoretical severity.

Validation Analyst

Measures what was blocked, what alerted and what got through.



Threat Profiler

Models the attacker behaviour relevant to your sector and assets.

Red Teamer

Scopes testing to your assets, exposures and control stack.

Validation Operator

Runs safe, realistic attack simulations in production, without production risk.

Safely prove the path into OT

Test scope: Level 2.5 and above

L4 Business and logistics

L3 Operations: MES, OT apps

L2.5 Industrial DMZ: test point

L2 Supervisory: HMI, SCADA

L1 Control: PLC, DCS

Attack simulation

Discovery only, where approved

No process control changes. Runbooks first.

Attacker-inspired scenarios, safely scoped

- ✓ **Initial access**
  Remote-support tools, SSH tunnels, valid accounts
- ✓ **Discovery**
  Remote system discovery, segmentation checks
- ✓ **Credentials**
  Default SSH and FTP logins on OT devices
- ✓ **Remote execution**
  RDP and remote sessions toward OT
- ✓ **OT visibility**
  Modbus, S7, EtherNet/IP, BACnet discovery
- ✓ **Detection**
  Did the SIEM, EDR and OT monitoring alert?

Re-prove the path every time supplier access is switched on.

Automation and Agentic Routines

Automation turns days into hours.
Agentic routines do it across IT and OT.

A new threat in the news

A critical CVE drops

A detection gap

The board asks

A vendor connects to OT

BY HAND	AUTOMATED	AGENTIC AI
read · map · script · run **days**	build & launch **~1 hour**	agentic routine **VALIDATED**
reproduce · patch blind **days**	find scenario · launch **~1 hour**	agentic routine **MITIGATED**
hand-write a rule · hope **days**	replay · tune **1-2 hours**	agentic routine **DETECTION DEPLOYED**
chase · reconcile · build **weeks**	export · assemble **1-2 hours**	agentic routine **REPORT CREATED**
ticket · trust · audit later **weeks**	run L2.5 template **~1 hour**	agentic routine **OT PATH PROVEN**

cymulate

Prove. Prioritise. Adapt.

>90%
Threat prevention

Less than 1 hr
To test a threat & update controls

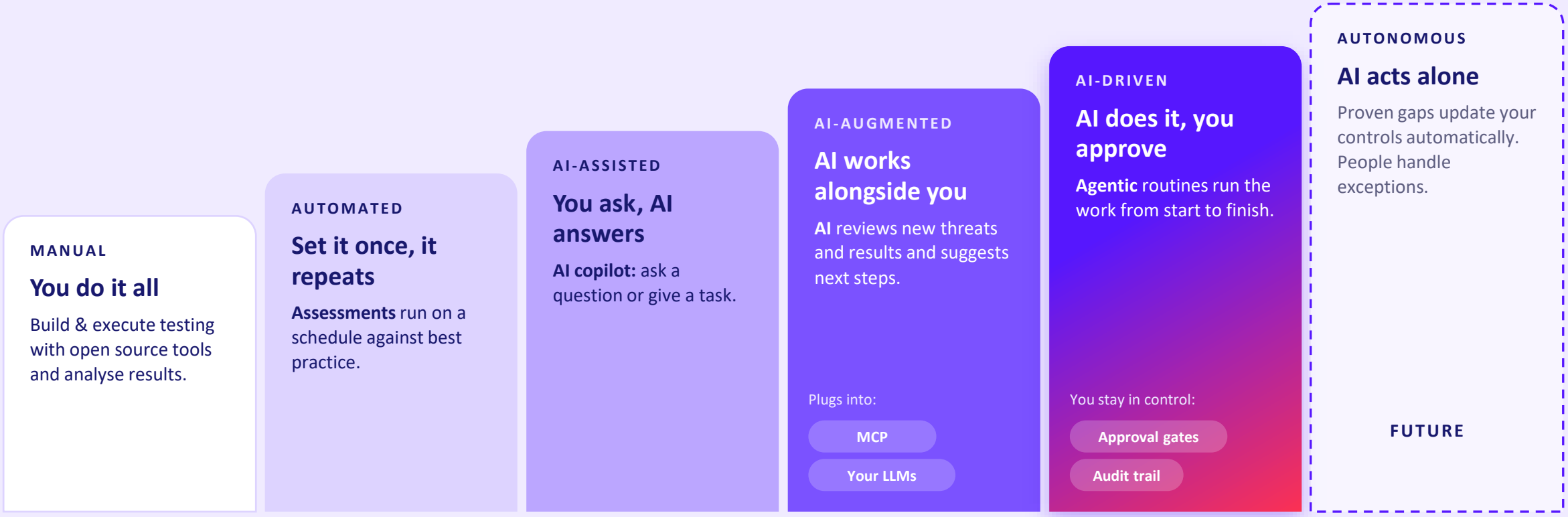
>50%
Better threat detection

95%
Fewer critical CVEs

Outcomes reported by organisations running continuous validation with Cymulate

VALIDATION MATURITY CURVE

Where is your validation programme today, *and where does it need to go next?*



DISCUSSION

Questions for the room

1. How do you decide what to patch first today, and how long does it take?
2. If a supplier's remote access into OT were abused tonight, could you prove your controls would stop it?
3. Where would AI in the loop help most, and where must people stay in charge?

See It in Action: cymulate.com

Networking lunch

We'll be back at 1pm

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**



From Air Gaps to Identity: Who Can We Trust in Connected Factories?

Florian Pouchet Head of Cybersecurity and Operational Resilience UK, Wavestone
Emeline Legrand Manager – Product & Industrial Cybersecurity, Wavestone

From Air Gaps to Identity:
Who Can We Trust in Connected Factories?



Florian Pouchet

Head of Cybersecurity & Operational Resilience UK

florian.pouchet@wavestone.com



Emeline LEGRAND

Industrial Cybersecurity Manager

emeline.legrand@wavestone.com



WAVESTONE

Wavestone, helping you lead cyber transformation in an uncertain world

1000+ cyber consultants

700+ trained in **AI security**
150+ trained in **AI engineering**

11 countries

Seamless delivery, local insight through strong ties with communities and regulators

4000+ tier-1 clients

Trusted for **20+ years** across public and private sectors

360° expertise

Covering the full spectrum **of CSO & CISO** priorities for **IT, OT** and **products**.
Recognized **by peers** at Black Hat, RSAC, DEFCON…

Human-led, AI-accelerated

We combine **human judgement**, **deep expertise** and our own AI platforms to **accelerate delivery** and **deepen analysis**.



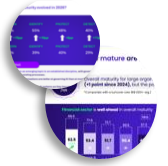
In-house AI platforms:
Risk Mgt., Benchmark, Sec By Design, Digital Identity, Pentesting, Crisis Ex.

From **strategy** to **forward-deployed engineering**

We design the roadmap, then build and deploy it with you, hands-on with leading vendors and our own engineering capabilities



Vision Top 30 for 2030



Cyber bench & CERT-W report



Deep vendors collaborations

Independent & Value-driven

We provide an unbiased approach to ensure the best choice for you, and we stay beyond go-live to drive sustainable adoption and tangible value



Numerous Market analysis



Cyber & AI Lab for testing & building



Value-driven project methodology

01

FROM ISOLATED TO CONNECTED FACTORIES

Why IAM in OT?

02

THE MULTIPLE SPECIFICITIES OF IAM IN OT

What is IAM in OT?

03

LESSONS LEARNED FROM THE FIELD

Where are we today?

04

OPERATING MODELS TO SCALE

How can you prepare now?

01

FROM ISOLATED TO CONNECTED FACTORIES

Why IAM in OT?

02

THE MULTIPLE SPECIFICITIES OF IAM IN OT

What is IAM in OT?

03

LESSONS LEARNED FROM THE FIELD

Where are we today?

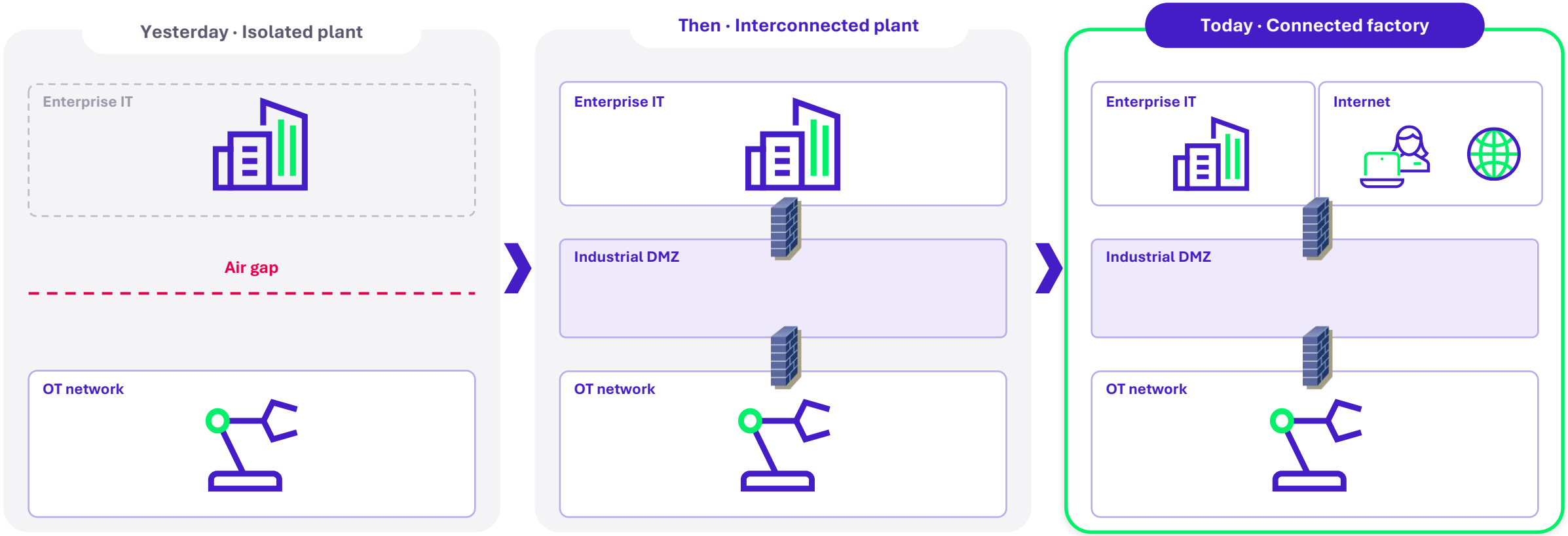
04

OPERATING MODELS TO SCALE

How can you prepare now?

IT/OT convergence started with the network

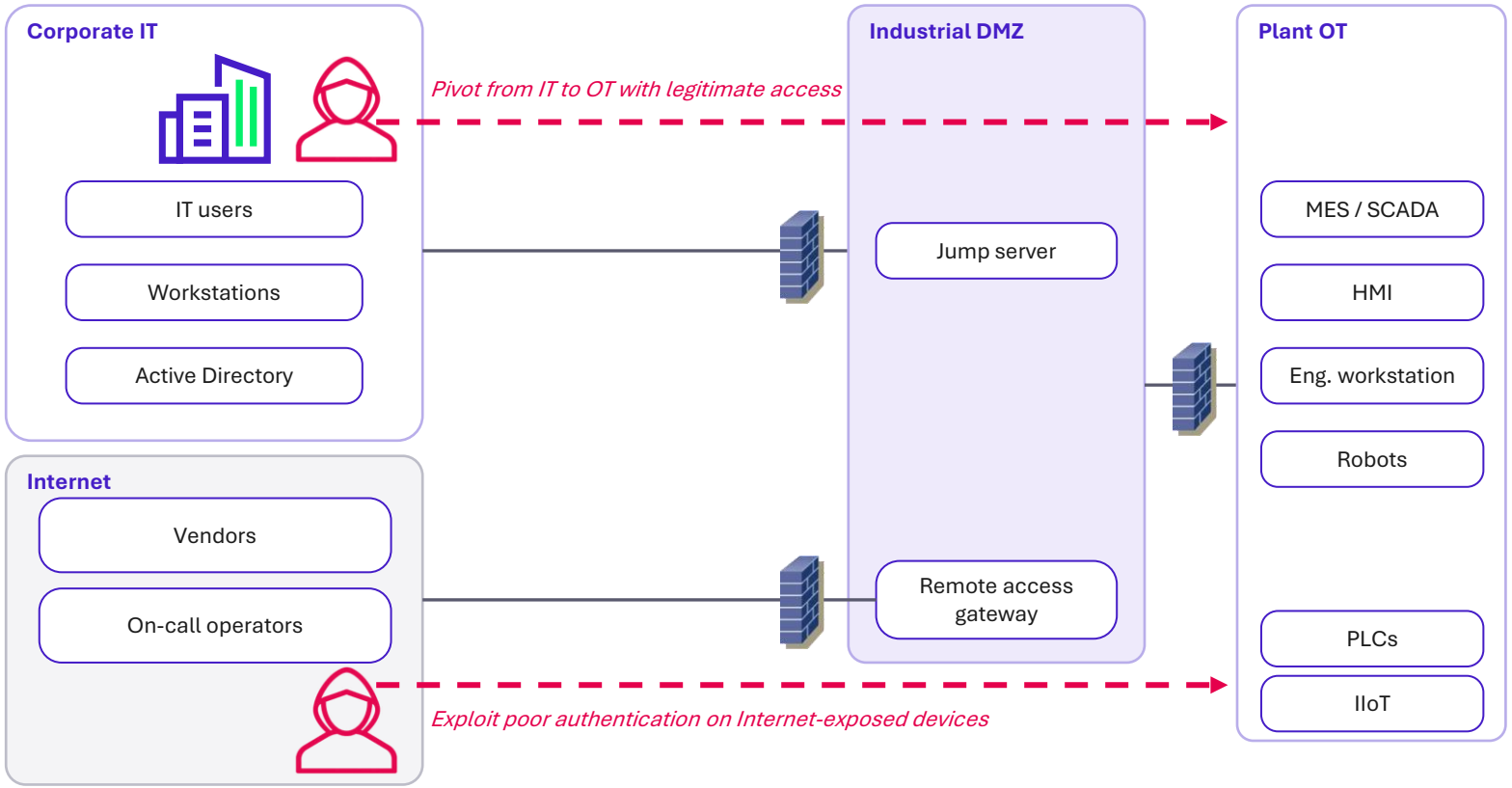
For years the key question was **“how do I connect my plant to the WAN?”**: interconnections, DMZ, IoT, remote access.



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

Why IAM becomes the new bastion of OT security

Network bricks secure the interconnection, but an attacker with a **valid identity** walks straight through them.




Jaguar Land Rover manufacturing and retail 'severely disrupted' by cyber incident

Carmaker says it has shut down its systems but there is no evidence customer data has been stolen


US cyber defense agency warns hackers are increasingly targeting water systems

By A.J. Vicens

July 30, 2026 11:43 PM GMT+2 · Updated July 31, 2026

Cyberattack Hits Hundreds of Supermarket Refrigeration Systems in France

The attack targeted a Danish software system in more than 400 supermarkets, forcing some shops to throw out frozen produce. The attackers have not been identified.


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

01

FROM ISOLATED TO CONNECTED FACTORIES

Why IAM in OT?

02

THE MULTIPLE SPECIFICITIES OF IAM IN OT

What is IAM in OT?

03

LESSONS LEARNED FROM THE FIELD

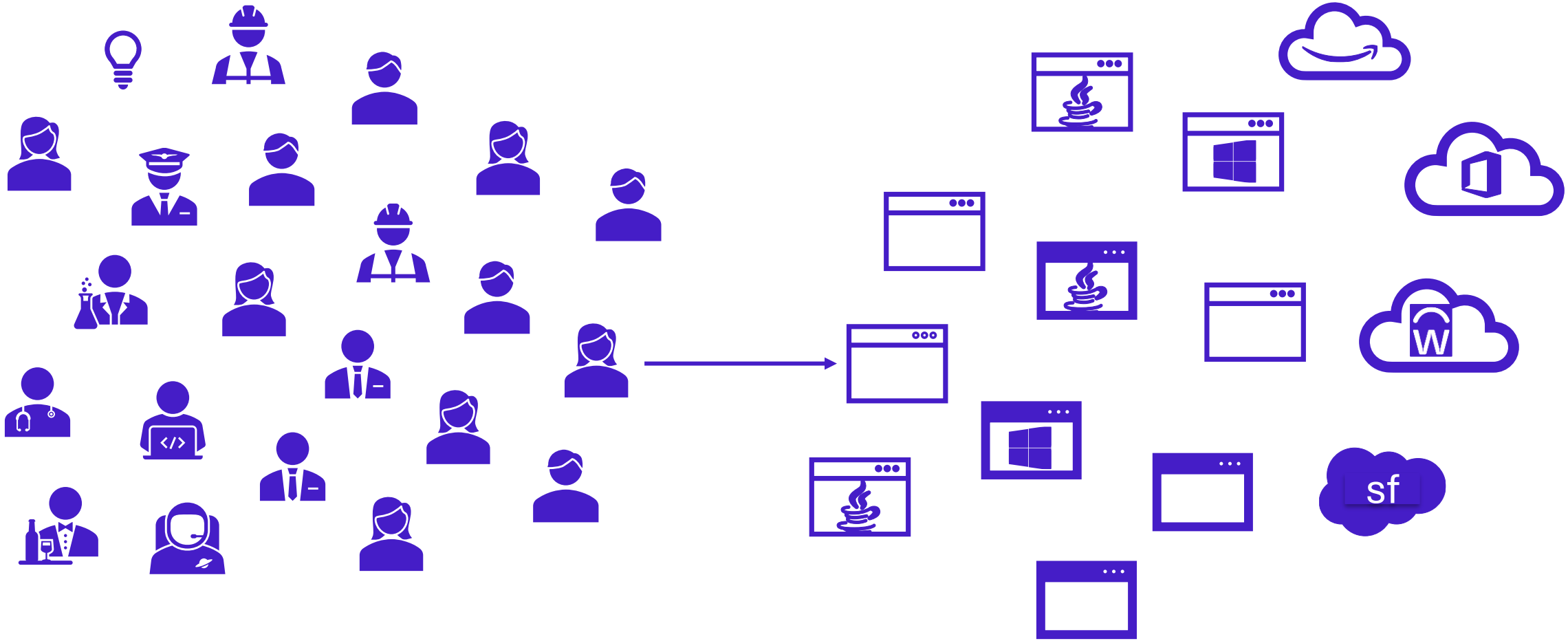
Where are we today?

04

OPERATING MODELS TO SCALE

How can you prepare now?

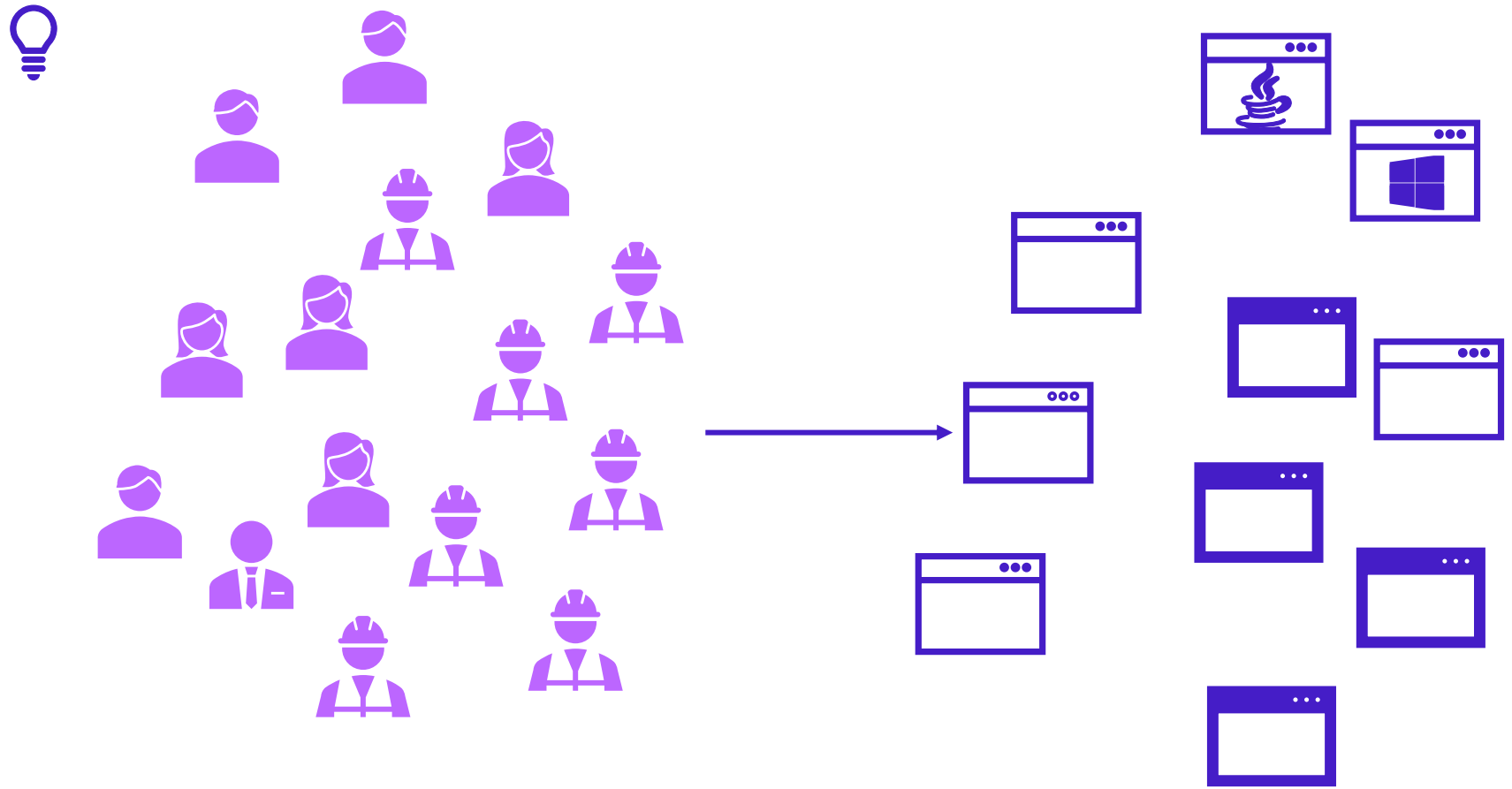
What is IAM in the OT world?





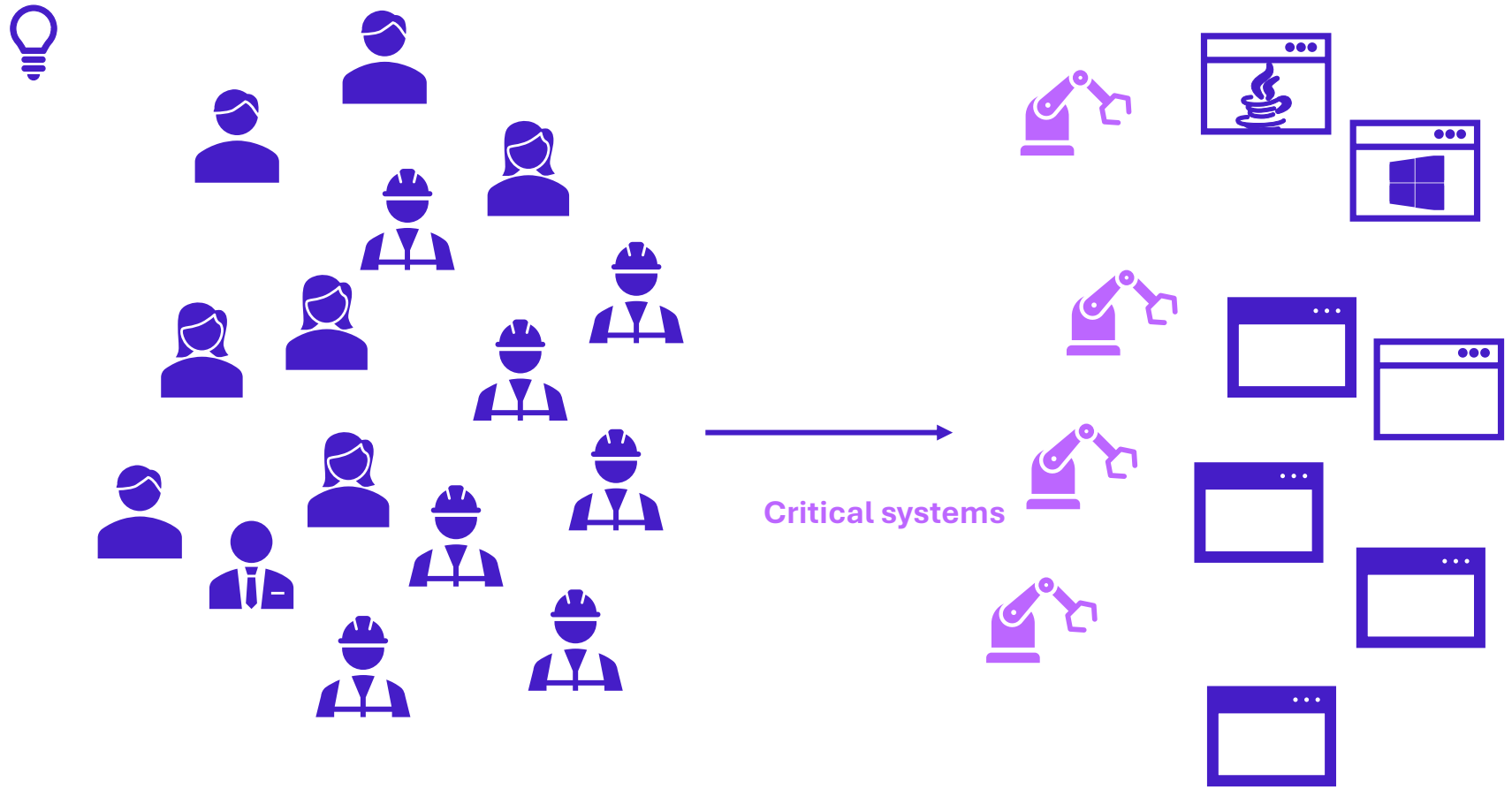
Emeline LEGRAND
Industrial Cybersecurity Manager
emeline.legrand@wavestone.com

What is IAM in the OT world?



What is IAM in the OT world?

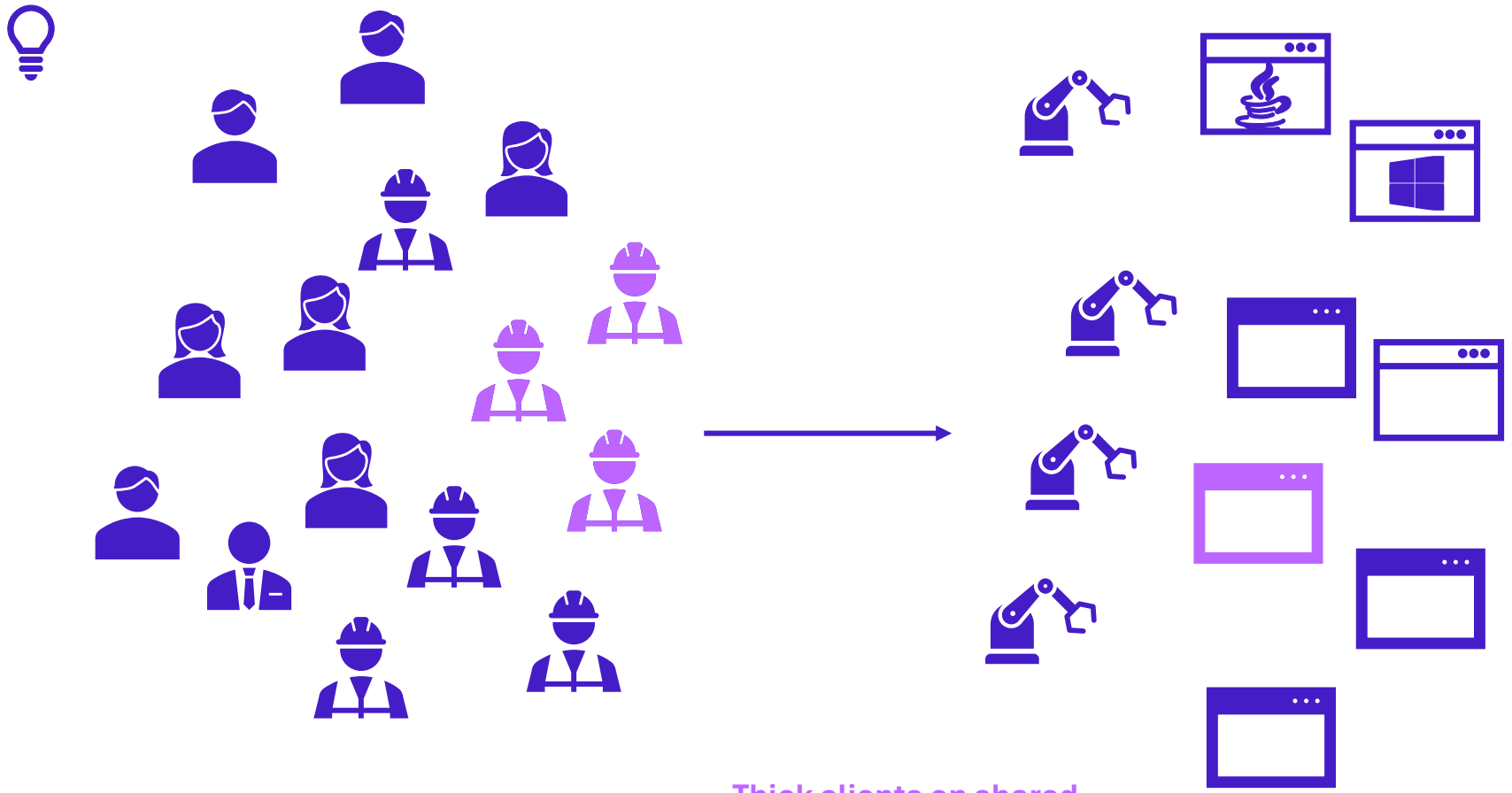
OT workers



What is IAM in the OT world?

OT workers

Critical systems



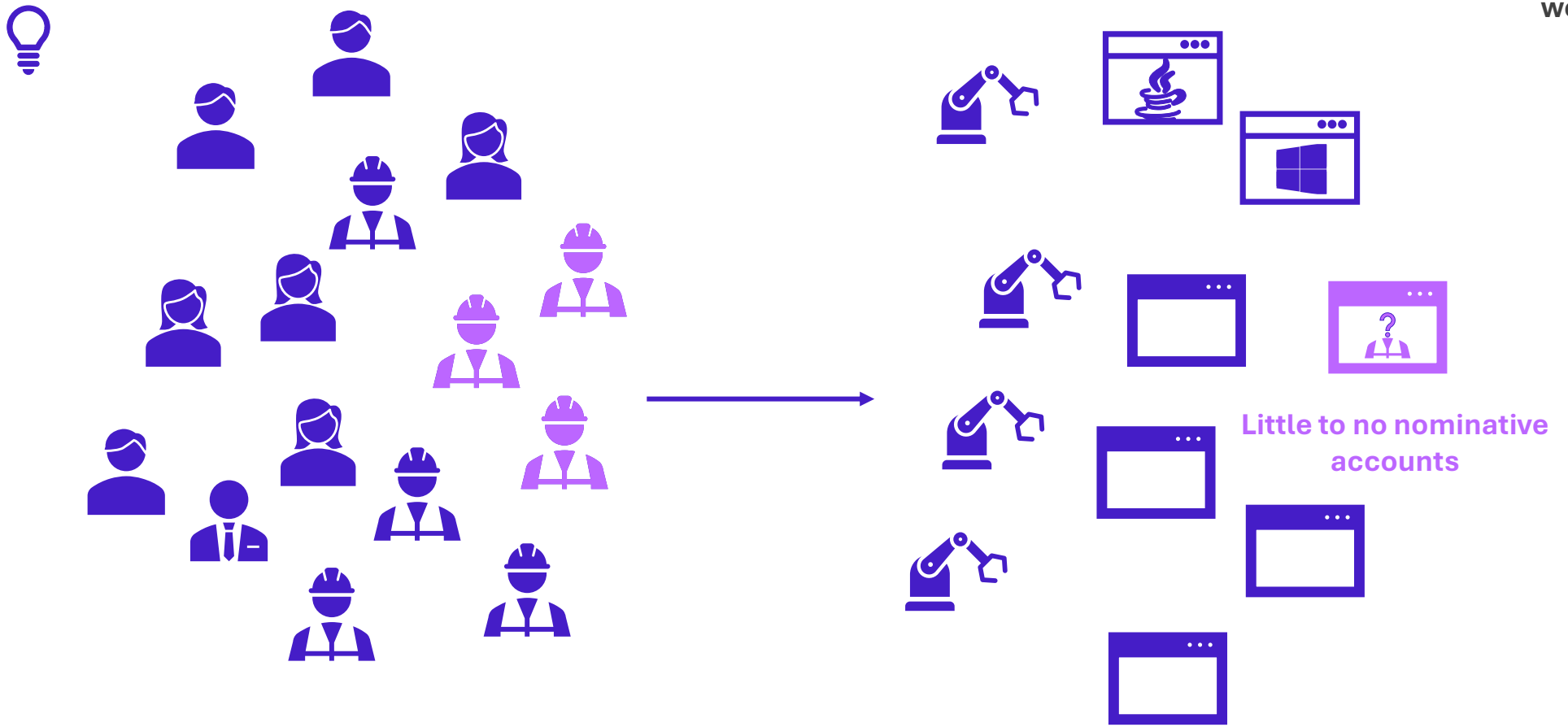
Thick clients on shared workstations

What is IAM in the OT world?

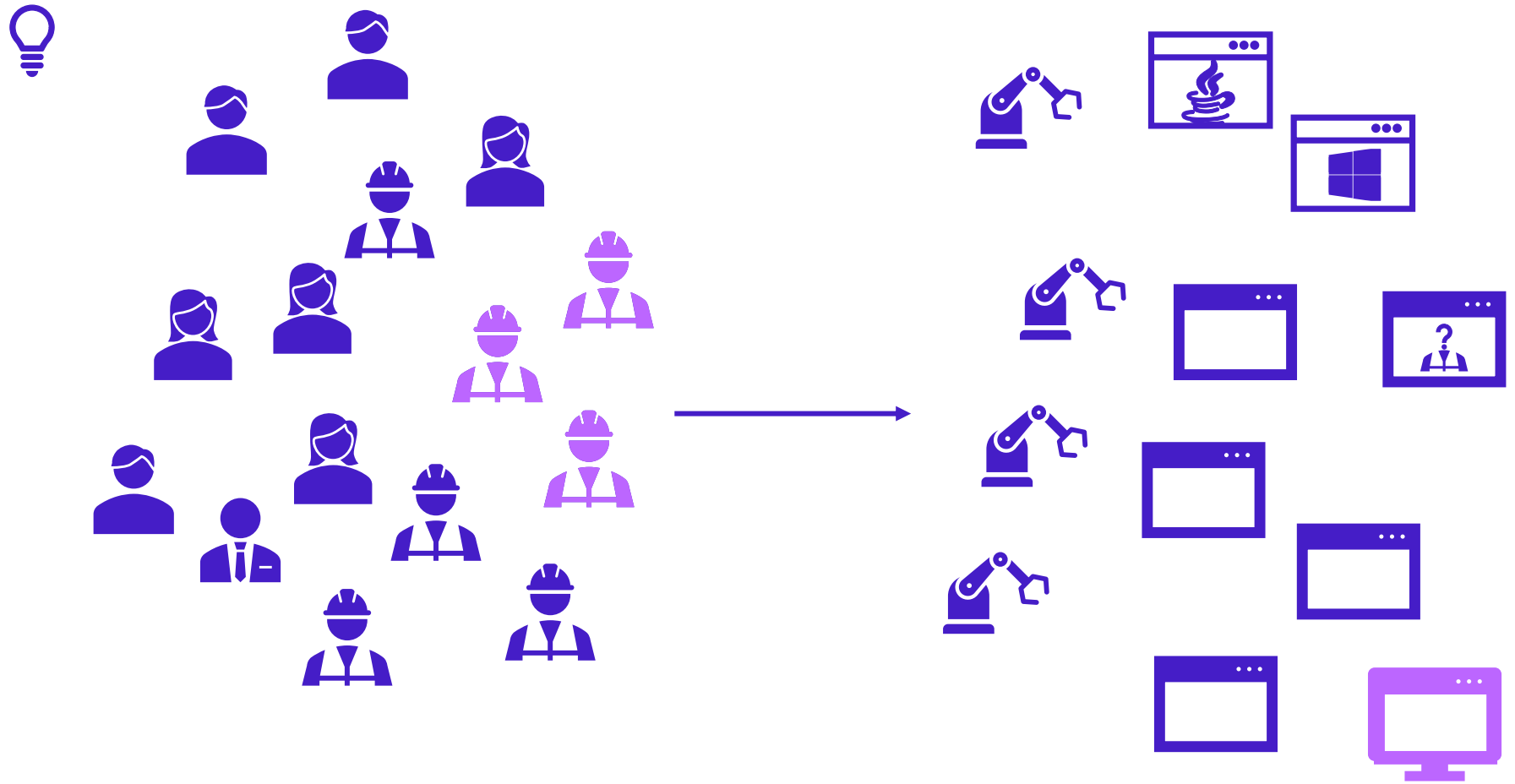
OT workers

Critical systems

Thick clients on shared workstations



What is IAM in the OT world?



OT workers

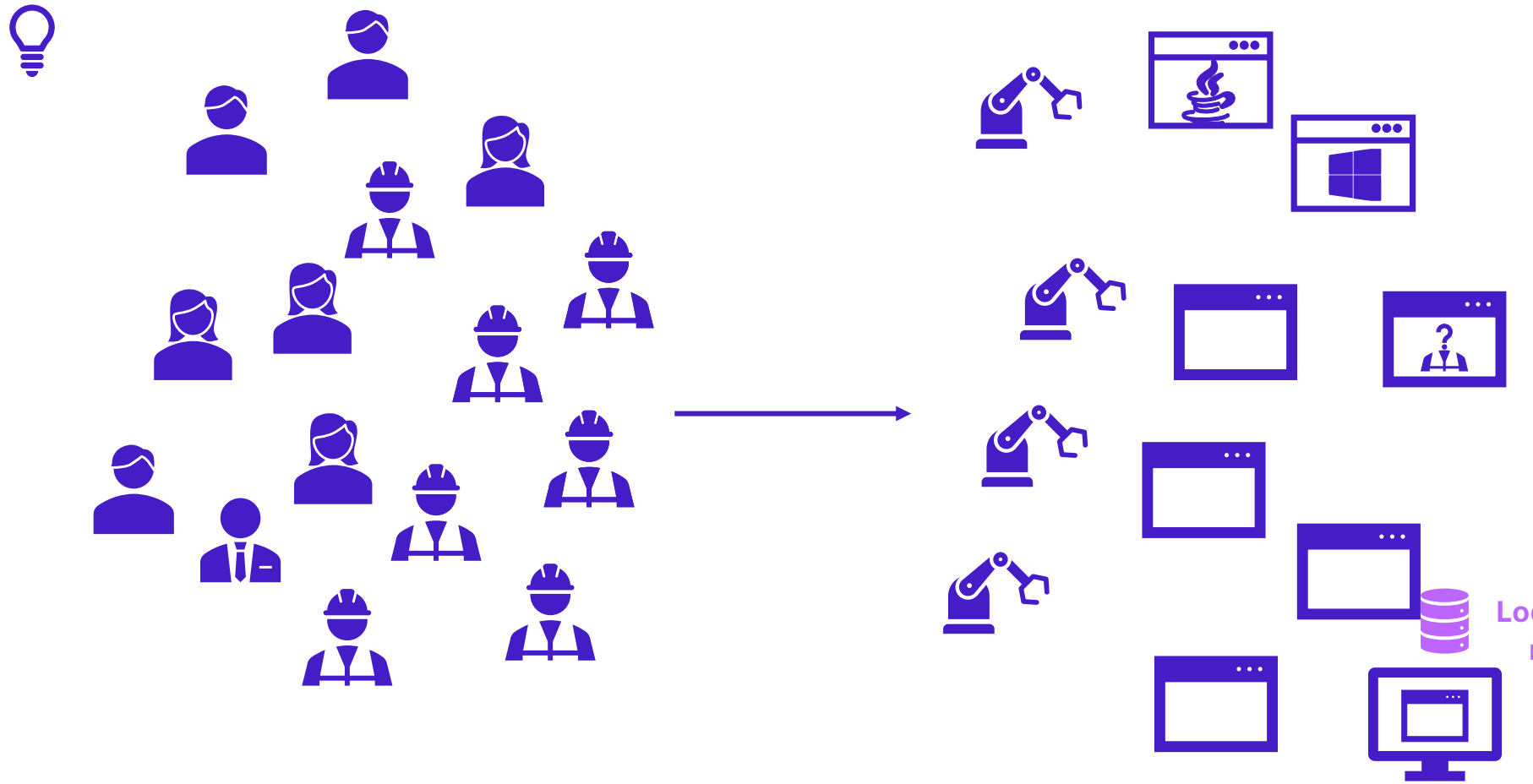
Critical systems

Thick clients on shared workstations

Little to no nominative accounts

OS authentication vs App authentication

What is IAM in the OT world?



OT workers

Critical systems

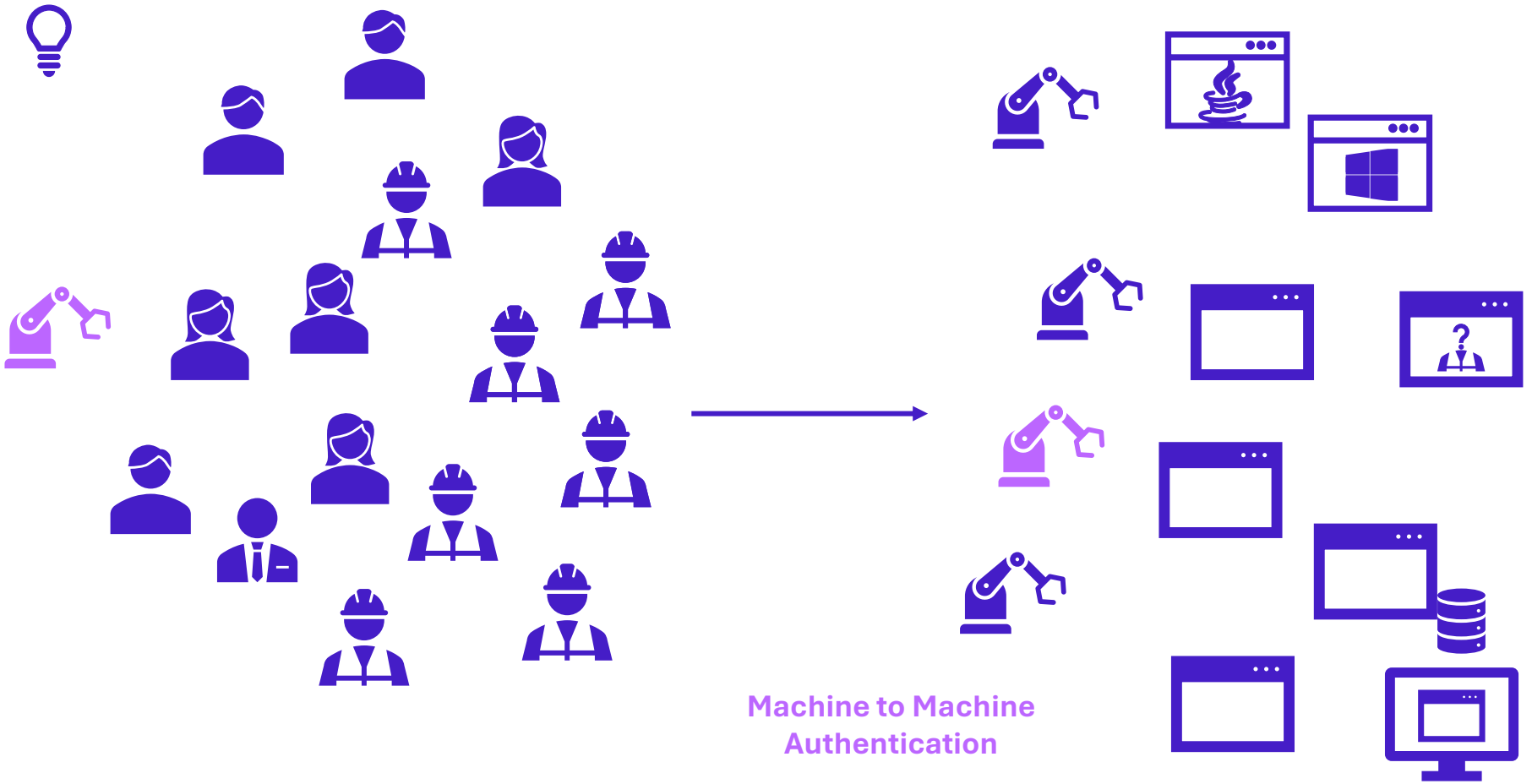
Thick clients on shared workstations

Little to no nominative accounts

OS authentication vs App authentication

Local OT identity repositories

What is IAM in the OT world?



Machine to Machine Authentication

OT workers

Critical systems

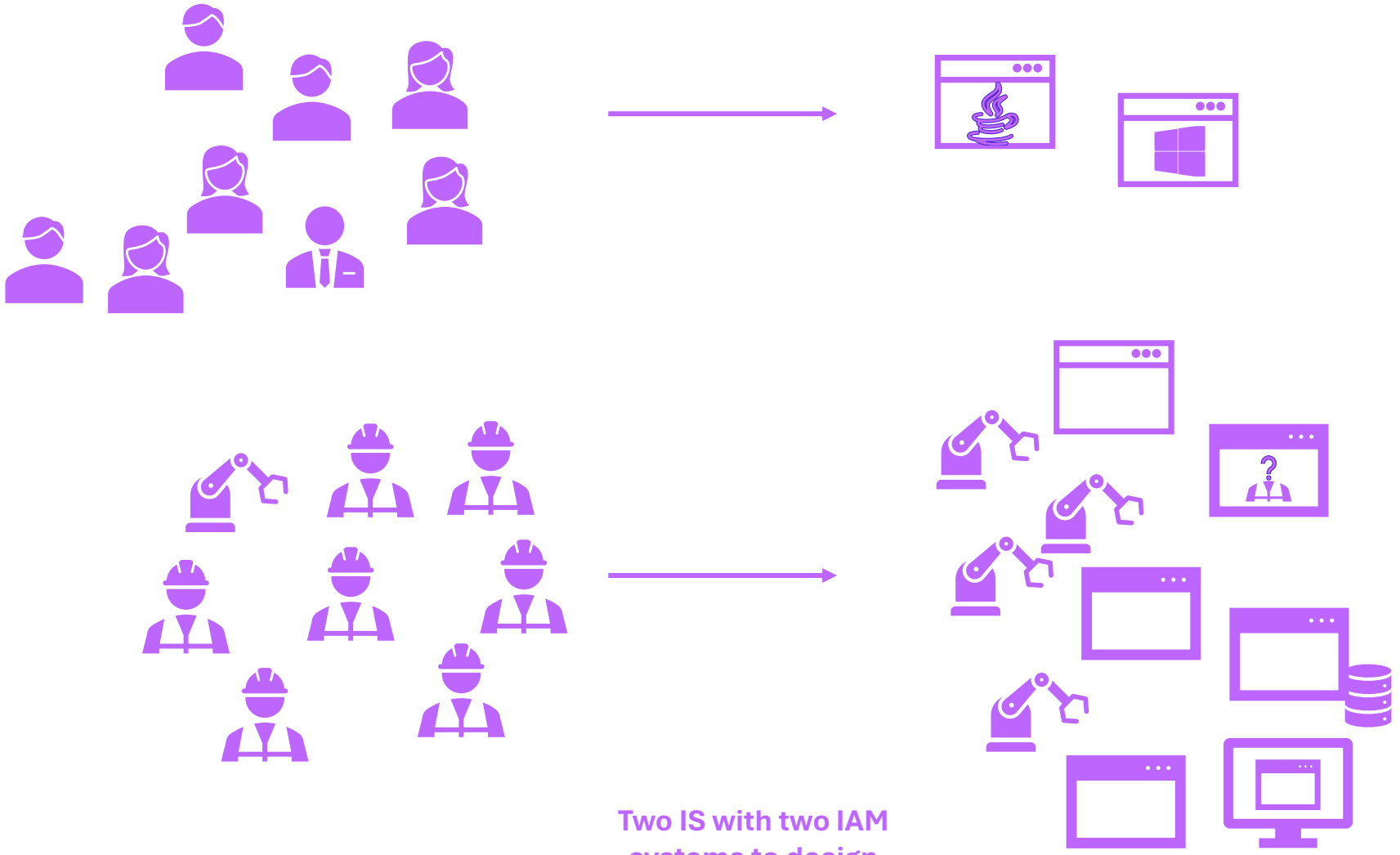
Thick clients on shared workstations

Little to no nominative accounts

OS authentication vs App authentication

Local OT identity repositories

What is IAM in the OT world?



OT workers

Critical systems

Thick clients on shared workstations

Little to no nominative accounts

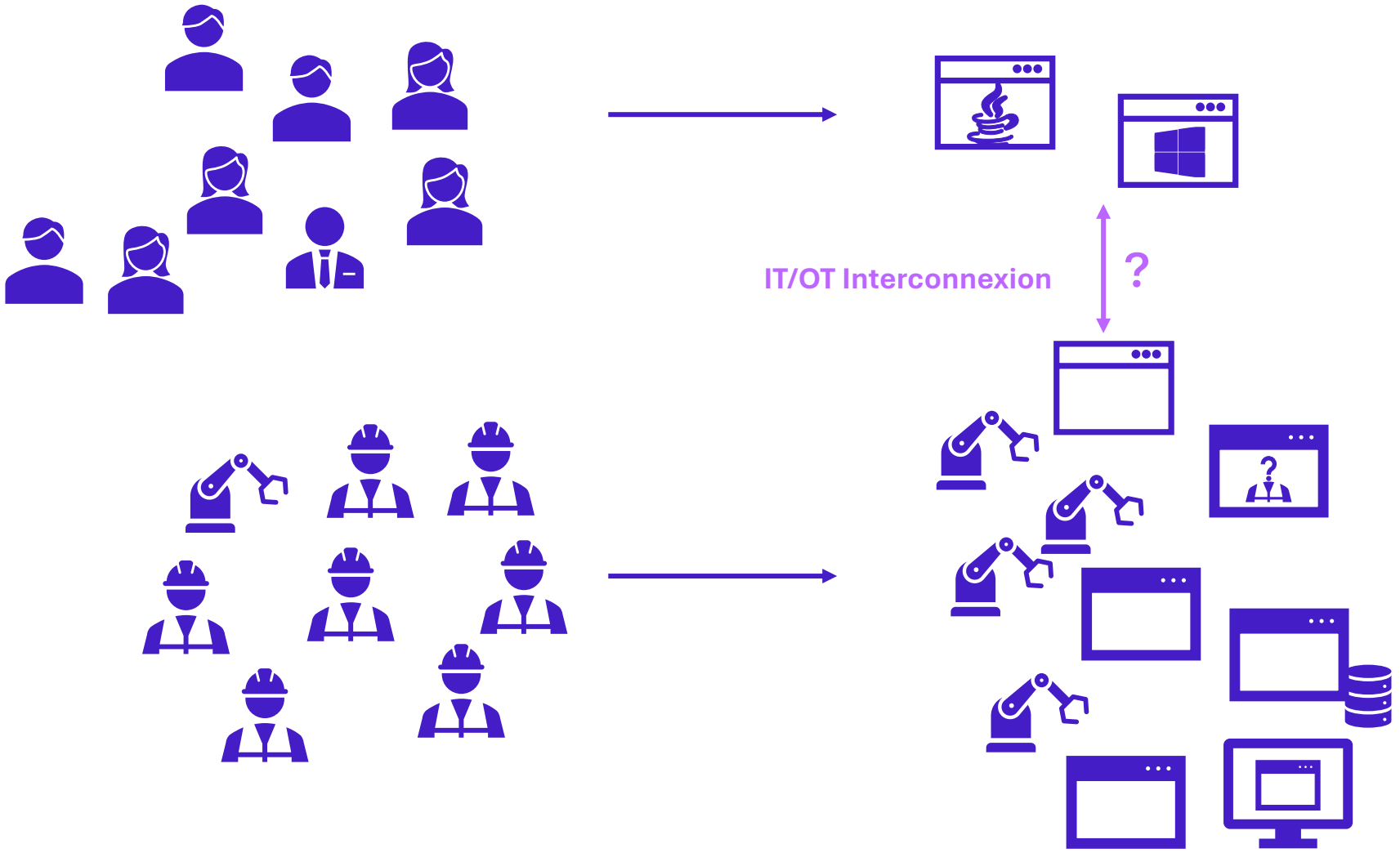
OS authentication vs App authentication

Local OT identity repositories

Machine to Machine Authentication

Two IS with two IAM systems to design

What is IAM in the OT world?



OT workers

Critical systems

Thick clients on shared workstations

Little to no nominative accounts

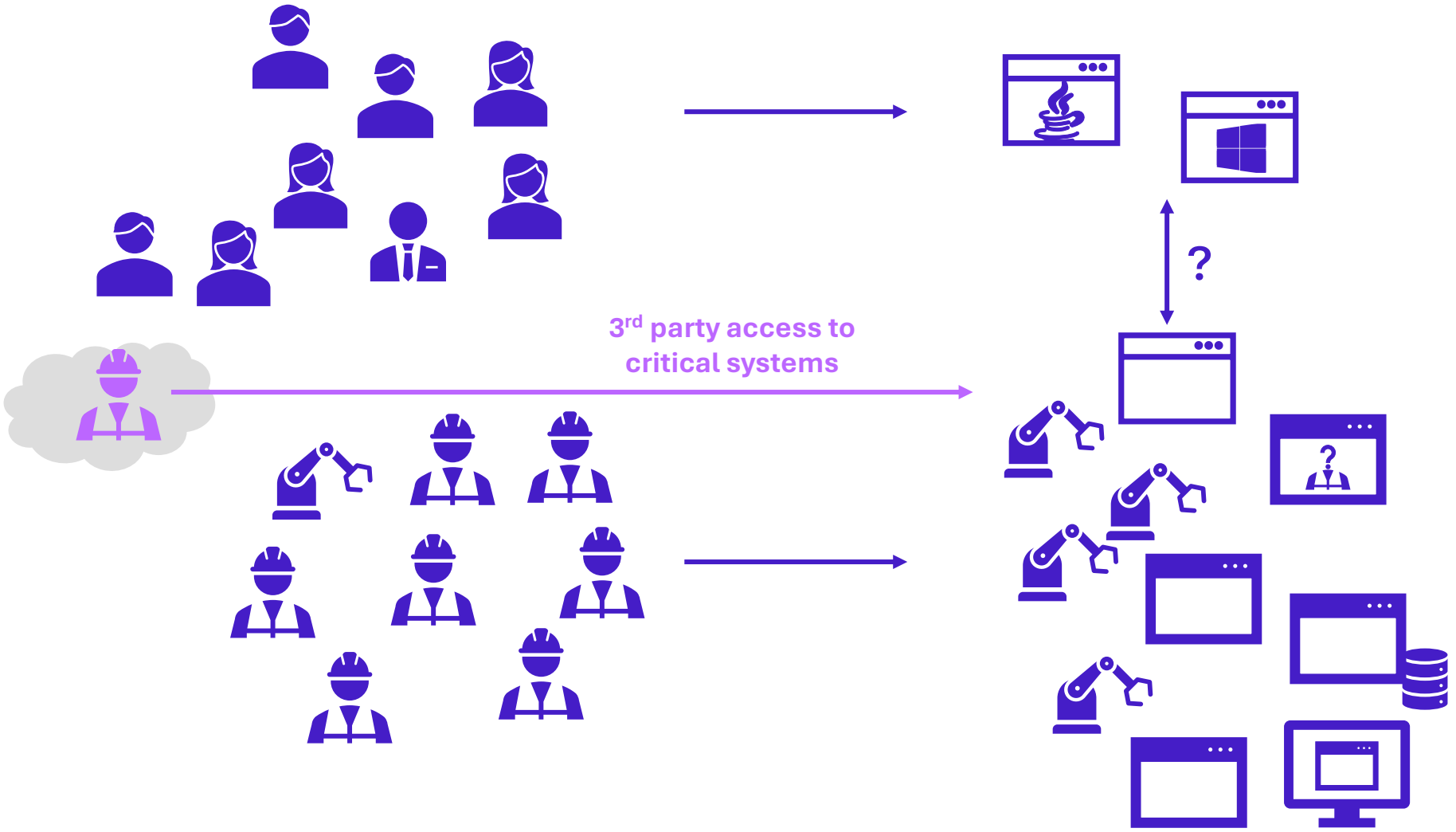
OS authentication vs App authentication

Local OT identity repositories

Machine to Machine Authentication

Two IS with two IAM systems to design

What is IAM in the OT world?



OT workers

Critical systems

Thick clients on shared workstations

Little to no nominative accounts

OS authentication vs App authentication

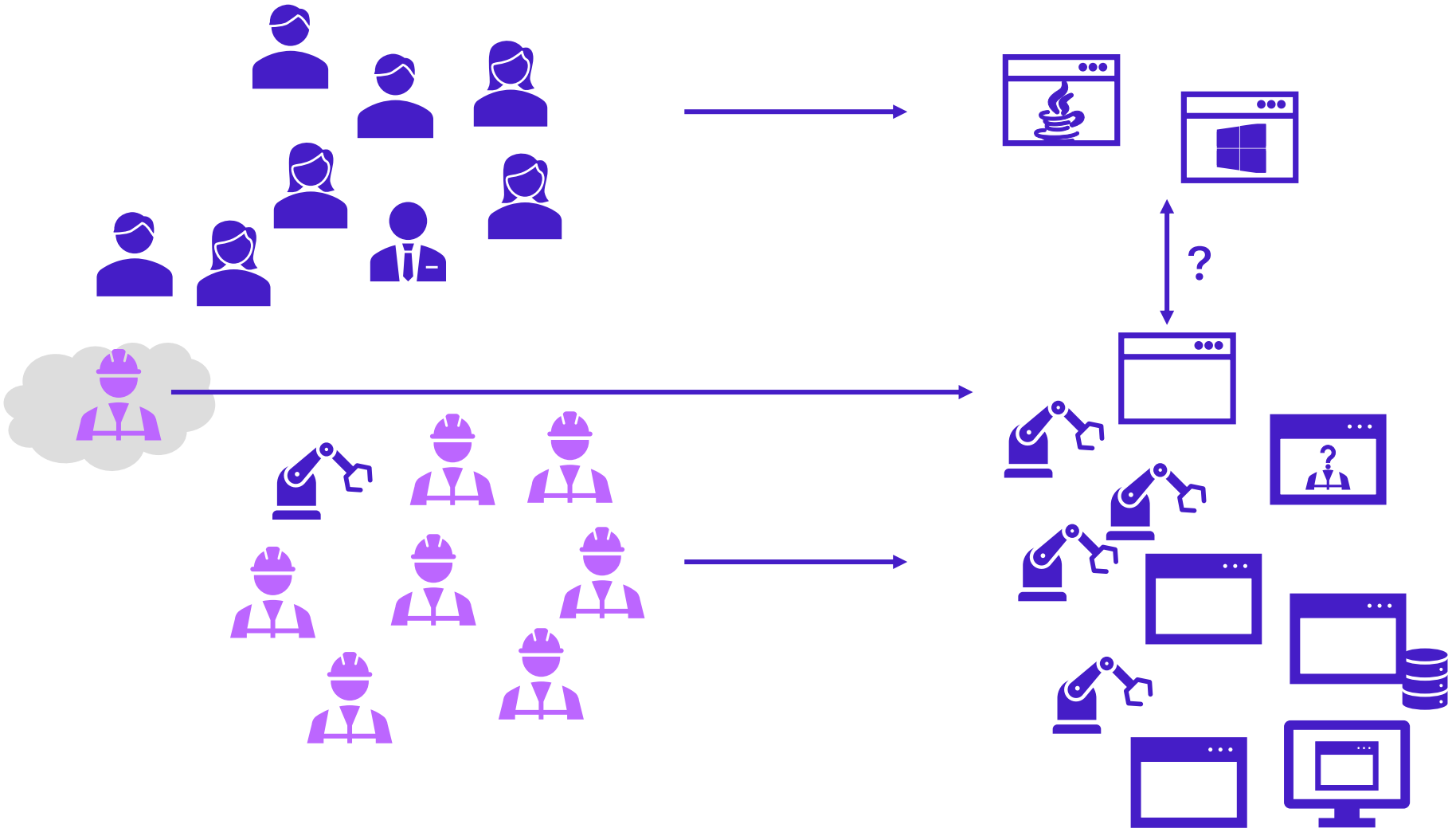
Local OT identity repositories

Machine to Machine Authentication

Two IS with two IAM systems to design

IT/OT Interconnexion

What is IAM in the OT world?



OT workers

Critical systems

Thick clients on shared workstations

Little to no nominative accounts

OS authentication vs App authentication

Local OT identity repositories

Machine to Machine Authentication

Two IS with two IAM systems to design

IT/OT Interconnexion

3rd party access to critical systems

Fast Joiner/Leaver

OT is specific in many ways that can impact IAM



OT present specific constraints on several areas:

Operational

- Systems can be **critical** and must be protected but **disponibility** is key
- **Roles and profiles are heterogeneous** with diverse skill sets/access needs
- Most of the time OT requires a **dedicated IAM system**, or even multiple
- Some of the identity repositories are local but **RACI** on administration, maintenance and operational **is unclear**
- Regular need to handle **fast Joiners/Leavers** especially for external vendors and maintainers who require **high privileges** on systems
- Devices that **record videos** or **take photos are prohibited** for certain industries

Physical

- OT workers might have **PPE constraints** that make usual authentication methods difficult (gloves, helmet, etc.)
- Some **physical zones** might require specific gear (ATEX zones, sterilized environments) where usual devices used for authenticated cannot be used
- Certain zones have specific environmental constraints (corrosion, high humidity) that **prevent the use of USB ports** (no keyboards)
- Many OT sites are **geographically remote or air-gapped**, preventing continuous connectivity to central authentication services

Technical

- The OT infrastructure was often setup **before IAM best practices** were standardized in IT
- Environments require **shared sessions** with little to **no nominative accounts**
- OT applications often rely on **one OS account** to support application
- Operators might need to authenticate on **both OS and applications** using sometimes different accounts
- Old SCADA and OT systems lack **compatibility** with modern IAM mechanisms like LDAP, SSO or MFA

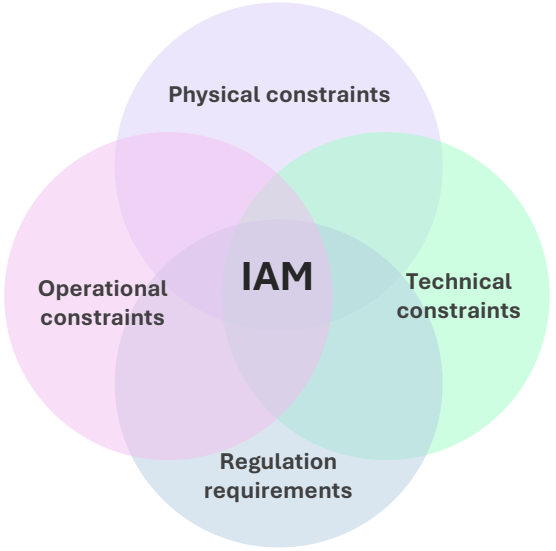
\+

Regulation requirements



Emeline LEGRAND
Industrial Cybersecurity Manager
emeline.legrand@wavestone.com

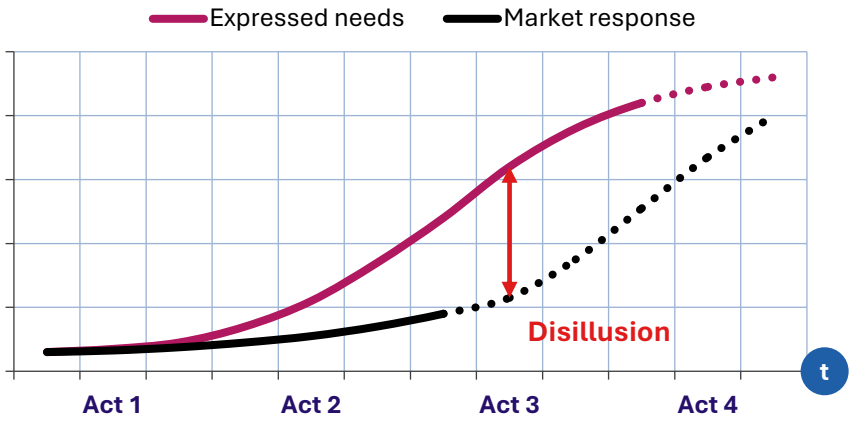
From IT to OT: Rethinking IAM in the face of industrial constraints



There is no "one-size-fits-all"!

The IT recipes will not apply on OT without being adapted

*IAM in OT must **not only secure critical environments**, but it must also be a response to **business needs.** IAM can be built around the OT tools to aim for **activity resilience.***



This approach is **not new to IAM strategies**

The importance of the business x IAM has been identified **more than 15 years ago on IT environments**!

Let's not make the same mistakes we did in IT:

Lack of Business Alignment
→ Solutions constraining the métier

Over-complexity
→ Processes over-engineered, too slow

Neglected awareness & change management
→ Leading to circumvention and Shadow IT

Let's skip these main mistakes made 15 years ago in IT to ensure efficient transition to secure IAM in OT while ensuring strategy is pragmatic.



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

01

FROM ISOLATED TO CONNECTED FACTORIES

Why IAM in OT?

02

THE MULTIPLE SPECIFICITIES OF IAM IN OT

What is IAM in OT?

03

LESSONS LEARNED FROM THE FIELD

Where are we today?

04

OPERATING MODELS TO SCALE

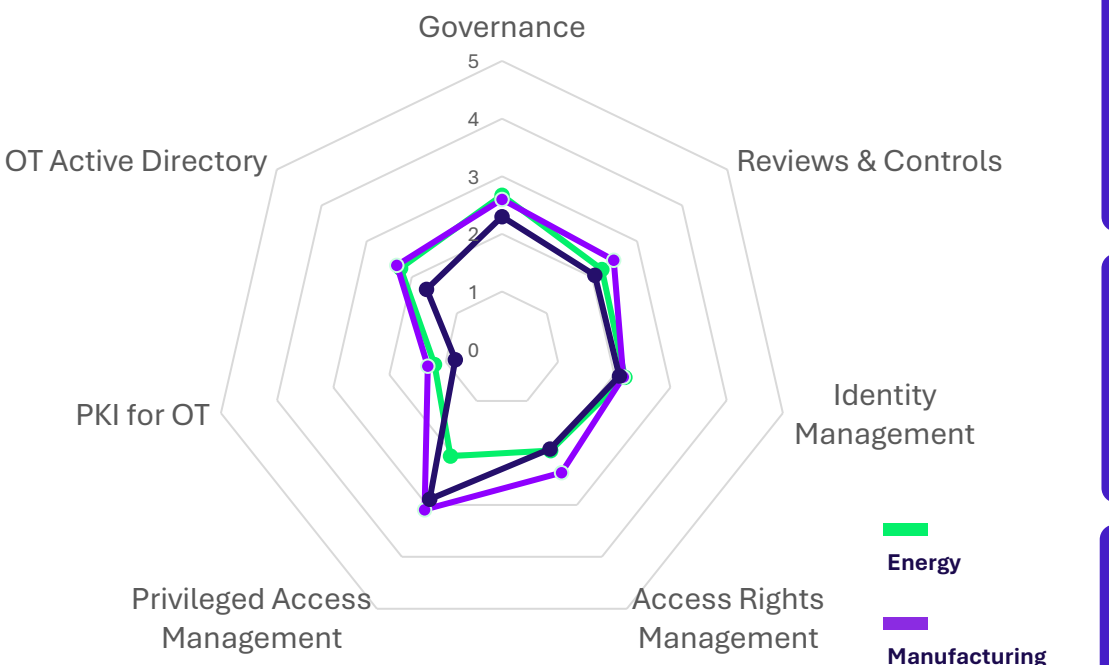
How can you prepare now?

2026 Wavestone benchmark: identity is on the agenda, foundations are uneven

IAM for OT maturity assessment of **industrial groups in 3 sectors**, across **7 control domains**.

13	3	18	2.1 / 5
Industrial clients	Industrial sectors	Use cases documented	Average maturity

Maturity by Theme and Sector



STRATEGIES EXIST, RARELY ROLLED OUT TO SITES

- **83%** Define an OT IAM Strategy at group level
- **25%** support, train and monitor sites on rollout

IT AD REUSED, TECHNICAL ACCOUNTS OVERLOOKED

- **75%** use the IT AD, at least partly, for OT needs
- **66%** have an OT identity management process
- **16%** structure their non-human identities

PRIVILEGED ACCESS BETTER SECURED

- **66%** inventory their privileged accounts
- **41%** Use nominative admin accounts with MFA



Emeline LEGRAND
Industrial Cybersecurity Manager
emeline.legrand@wavestone.com

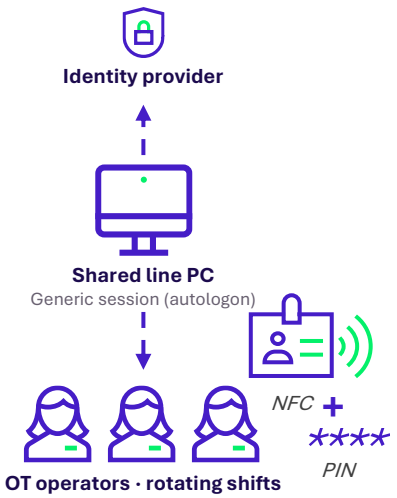
Patterns work when they secure reality instead of banning it

Four field-proven patterns from our engagements, and **what they taught us**.

What we did

What we learned

Shared workstations



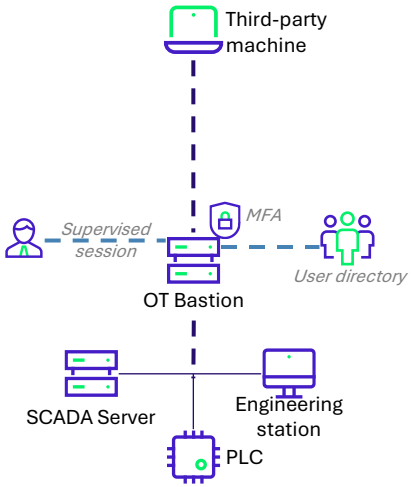
Workers access a **shared workstation** on site. The workstation is configured with **autologon account**

To connect to business application, they use a **NFC badge** with a **local PIN**

Business application use **Federation** with **global IdP** to ensure authentication of the users

Traceability without slowing handovers; plan the **lost-badge** process.

Vendor remote access



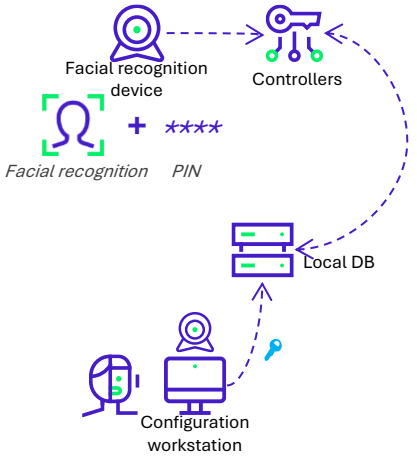
Remote access is provided by a **Bastion dedicated to OT**

Third party accounts are only enabled **when access is needed** and are **disabled by default**

Remote sessions must be **supervised by on-site employees**

Easy to design, harder to adopt: **planning maintenance ahead** is the real change.

PPE & sensitive zones



Identified employees that require access to **specific zones** register and **biometric templates** are stored

To access such zones, the OT worker **scans his face** and enters a **PIN code**

The facial recognition device sends identification data to the **controllers** that question the **access control database**

GDPR by design and an **offline degraded mode** are non-negotiable.



Emeline LEGRAND
Industrial Cybersecurity Manager
emeline.legrand@wavestone.com

01

FROM ISOLATED TO CONNECTED FACTORIES

Why IAM in OT?

02

THE MULTIPLE SPECIFICITIES OF IAM IN OT

What is IAM in OT?

03

LESSONS LEARNED FROM THE FIELD

Where are we today?

04

OPERATING MODELS TO SCALE

How can you prepare now?

Let’s learn from our past programs and adapt them to meet our needs



Think your IAM for OT programs jointly with the business

Secure cyber, business and digital sponsors before launching the program.
Co-build the roadmap with them to meet OT field constraints.
Share ownership and clear roles across teams.

IAM cannot succeed without the support of all teams



Prioritize Safety, Resilience then Cyber

Ensure security is process-driven, not tool-driven. Solutions must build around existing OT infrastructure to ensure process integrity and resilience.

IAM success in OT is also measured by its impact on process integrity, be pragmatic



Uniformization and centralization are key to scale up

Define the baseline (architecture, governance, tools) to ensure better operational efficiency and ensure clear governance. IAM baseline should be thought as a strategic enabler to start building your Zero Trust foundations.

IAM tools should be thought as scalable foundation that is future-proof



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



Where to Start? Your First 4 Steps for IAM in OT

Know your repositories

Map, secure, and centralize identity sources

What are your **identity databases** and how many do you manage on site?

What is your **main repository strategy** (Centralization vs. Local Management)?

Can you map **all your critical site applications**?

Know your identites

Establish a single source of truth for all users and devices

Who are your **users** (mono/multi-sites, temporary, third-party, etc.)?

What is the **access context** (Shared devices, remote)?

Where and why do you rely on **individual** or **generic accounts**?

Know your rights

Implement accountability and audit privileges regularly

Are **risky apps/systems** recertified on a regular basis?

Do OT applications enforce **advanced role management**?

How good is your **physical access** system working?

Know your access control

Secure the access path and enforce strong authentication

Where do users **authenticate** from (shared laptop, Bastion)?

Is there a justified need for **shared accounts**?

What are the main **operational constraints** for your operators (masks, gloves, sanity measures, etc.)?



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

WAVESTONE



Want to know more?

Drop us an email!



Florian Pouchet

Head of Cybersecurity & Operational Resilience UK

florian.pouchet@wavestone.com



Emeline Legrand

Industrial Cybersecurity Manager

emeline.legrand@wavestone.com

The threat lives in behaviour: From IT identity to OT impact

Jake Anthony
Principal Solutions Engineer, Exabeam

The Threat Lives in Behaviour:

From IT Identity to OT Impact

Jake Anthony | Principal Solutions Engineer, UK/EU

Copyright © 2026 Exabeam, Inc. All Rights Reserved.

They Didn't Steal Anything

The 2026 European freezer attacks: a changed setting, not stolen data

Remote Access	A Changed Setting	Alarms Suppressed	Physical Impact
Overnight, attackers reached the software controlling refrigeration units	Defrost and temperature settings were altered. Nothing was stolen	Defrost cycle reportedly stretched from 1 hour to 8 to avoid alerts	~700 of 10,000 French stores hit, then Belgium, Sweden and beyond

The goal wasn't data. It was physical consequence
The question: what looked different before the impact?

Sources: AP, Le Monde and trade press, Oct–Nov 2026. Details are still emerging.

Copyright © 2026 Exabeam, Inc. All Rights Reserved.

exabeam

IT, OT and CPS: One Attack Surface

Corporate IT

- ✓ Cloud and SaaS
- ✓ Directory identities
- ✓ Service accounts
- ✓ Remote access
- ✓ AI agents

The Bridge

- ✓ Vendor remote access
- ✓ Shared admin logins
- ✓ Internet-facing panels
- ✓ Weak segmentation
- ✓ Unclear ownership

OT & CPS

- ✓ Refrigeration
- ✓ HVAC and BMS
- ✓ Controllers
- ✓ Legacy equipment
- ✓ Safety systems

Copyright © 2026 Exabeam, Inc. All Rights Reserved.

exabeam

Three Identities, One Entry Point

H

Human

STOLEN CREDENTIALS

Staff, admins and vendors. Phished or reused credentials open the door.

EXAMPLES

Remote administrators
Third-party engineers
Privileged users

M

Machine

COMPROMISED IDENTITY

Service accounts, API keys and tokens. Rarely reviewed, rarely watched.

EXAMPLES

Service accounts
API keys and tokens
Certificates

AI

AI Agent

ROGUE OR SUBVERTED

Autonomous agents with real permissions, acting at machine speed.

EXAMPLES

Workflow agents
MCP-connected tools
Digital workers

STOLEN CREDENTIAL → LATERAL MOVEMENT → OT IMPACT

Copyright © 2026 Exabeam, Inc. All Rights Reserved.

exabeam

Allowed Is Not the Same as Normal

What Access Control Sees

- ✓ Valid credential
- ✓ Permitted session
- ✓ Authorised command
- ✓ Known device
- ✓ Approved role

What It Misses

- ✓ Odd time or source
- ✓ Rare target systems
- ✓ First-time changes
- ✓ IT-to-OT movement
- ✓ Quiet alarm changes

What Behaviour Reveals

- ✓ Own-baseline drift
- ✓ Peer-group drift
- ✓ Rare sequences
- ✓ Intent in context
- ✓ Early warning

Copyright © 2026 Exabeam, Inc. All Rights Reserved.

exabeam

Behaviour as the Detection Layer

Baseline each identity against itself and its peers

Baseline



- People, machines, AI
- Self and peer norms
- Time, source, targets

Know normal first

Correlate



- Link IT to OT activity
- Follow one identity
- Tie logins to changes

Watch the path, not just the endpoint

Detect



- Rare critical changes
- Odd sequences, timing
- Peer-group outliers

Don't monitor events, monitor behaviour

Respond



- Prioritise by risk
- Alert before impact
- Revoke and isolate

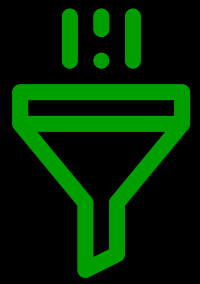
Stop it before it reaches OT

Copyright © 2026 Exabeam, Inc. All Rights Reserved.

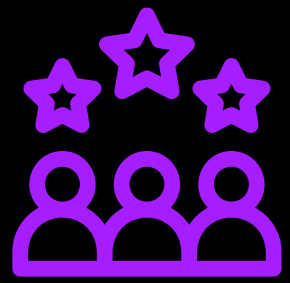
exabeam

Applying the Freezer Lens

Illustrative: each stage leaves behavioural evidence before the physical impact







STAGE 1 – ENTRY

- Login from an unusual source or time
- First-time use of remote management
- Service identity acting like a human
- Agent calling tools outside its role

STAGE 2 – MOVEMENT

- Rare path from IT towards OT
- Access to systems peers never touch
- Credential reuse across zones
- Spike in discovery activity

STAGE 3 – IMPACT

- Setpoints changed on many sites at once
- Alarm thresholds loosened
- Change outside a maintenance window
- Same change repeated at scale

The signal appears long before the freezer warms

Copyright © 2026 Exabeam, Inc. All Rights Reserved.

exabeam

Why Behaviour Matters for AI Agents

Agents are identities too: they execute towards objectives, within constraints

Destination Driven	Illusion of Security	Shadow AI	Environment is Key
AI Agents pursue objectives unpredictably and relentlessly	Guardrails are the AI security tax but they only define what's allowed	Registration is one mechanism but you can't govern what you can't see	When you can't confidently define the target, observe the environment

The goal isn't to monitor more identities, it's to understand behaviour
Behaviour is the common language for humans, machines and AI agents

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

Copyright © 2026 Exabeam, Inc. All Rights Reserved.

exabeam

Ask Yourself This – Who Is Watching Behaviour?

Three questions every organisation should be able to answer:

01 Which identities can reach OT?

02 Who can see when behaviour changes?

03 Who has the authority to stop it?

Discussion prompts for your IT, OT and security teams

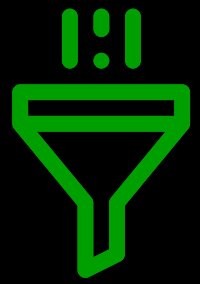
Is OT in your monitoring scope? | Do agents have distinct identities? | Where do you need human approval?

Copyright © 2026 Exabeam, Inc. All Rights Reserved.

exabeam

What Can You Do Now?

A practical 30/60/90-day plan to close the IT-to-OT visibility gap.



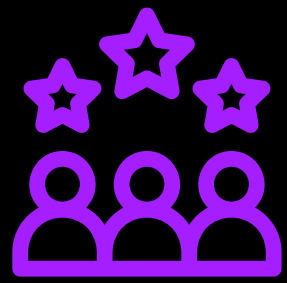
30 DAYS – DISCOVER

- Inventory connected controllers and owners
- Map identities with OT-adjacent access
- Keep management interfaces off the internet
- Find monitoring and ownership gaps



60 DAYS – EXTEND

- Segment IT from OT where possible
- Extend behavioural telemetry beyond IT
- Baseline humans, machines and agents
- Define escalation and intervention points



90 DAYS – EXERCISE

- Run an IT-to-OT attack scenario
- Test revoke, isolate and containment
- Validate event sequence reconstruction
- Capture lessons and close gaps

Start with visibility, then prove you can respond

Copyright © 2026 Exabeam, Inc. All Rights Reserved.

exabeam

exabeam™

The identity got them in.

The behaviour gives them away.

Jake Anthony | Principal Solutions Engineer, UK/EU

Copyright © 2026 Exabeam, Inc. All Rights Reserved.

Panel discussion: A broadened perspective

Led by Liz Murray Chief of Staff, SASIG

Panellists
Tim Harwood CEO, Siker Cyber
Stephen French Principal Security Consultant, Bridewell
Stuart Codack Principal OT Consultant, PA Consulting
Cathy McCann Founder, Invistra AI
Ian McGowan Managing Director, Barrier Networks

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**

