CHECK POINT

Company Under the AI Attacks Pressure

Jiří Kohout

Cybersecurity Strategy Advisor - CEE, CISM

YOU DESERVE THE BEST SECURITY

Why We Do Not Start with Technology

AI changed attacks — but even more, it changed decision-making inside organisations

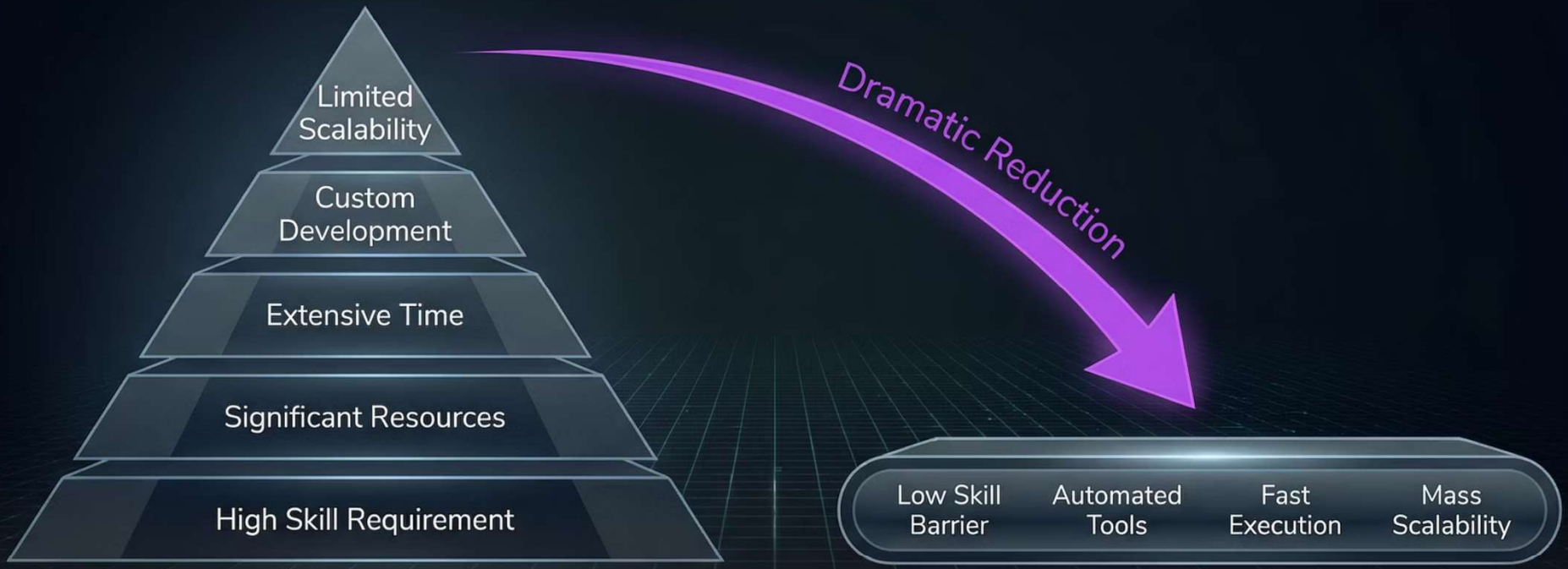
Technology is not the main problem. Lack of clarity is.

AI Is Already Operational Reality

- Embedded in daily operations
- Public LLMs used without oversight
- Shadow AI is the standard

“The risk is present now, not in the future.”

AI Changed the Economics of Attacks



Traditional Attack Cost Structure

AI-Enabled Attack

Anyone can now represent real risk. Motivation is the only barrier left.

Why Phishing Still Works

Perfect language. Deep personalisation. The attacker knows your organisation.

The user is not the error — technology must compensate.

Brand Abuse and Trust Breakdown

CHECK POINT

Authentic Brand Communication

AETERNA
TECH

Authentic brand communication

- Trusted visual identity with formed identity
- Verified tone with connters and sone.

AI-Generated Fake Replica

AETERNA
TECH

Identity brand Communication

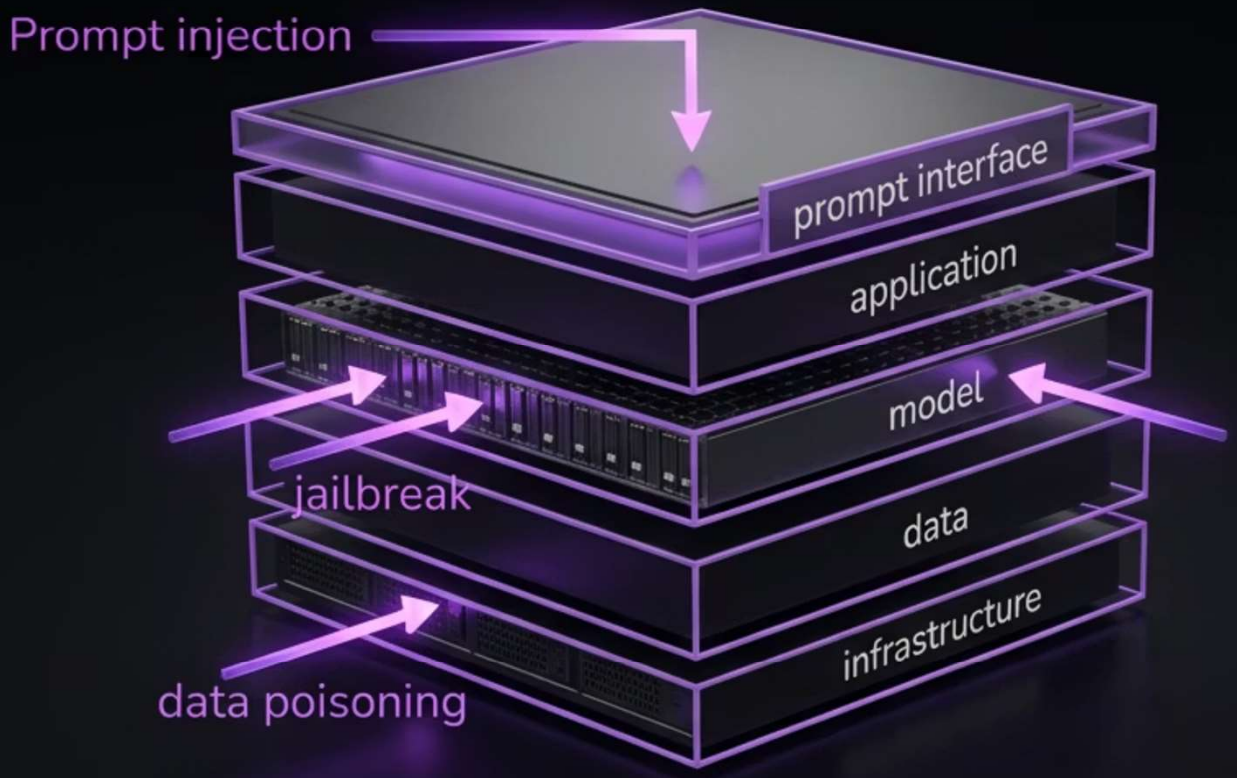
- Trusted visual identity with farmed identity
- Verified tone with coarchers and zone.

Digital identity can be replicated in minutes.

Generated in minutes No system access required Reputational damage precedes detection.

Trust breaks before systems detect an incident.

AI Is a New Attack Surface.



Prompt injection.
Jailbreak.
Guardrail bypass.

Who controls
AI behaviour?

Security must move beyond infrastructure to decision logic.

Models Change Without You Changing Code

No Change Management for AI Behaviour

Guardrails Without Data Governance

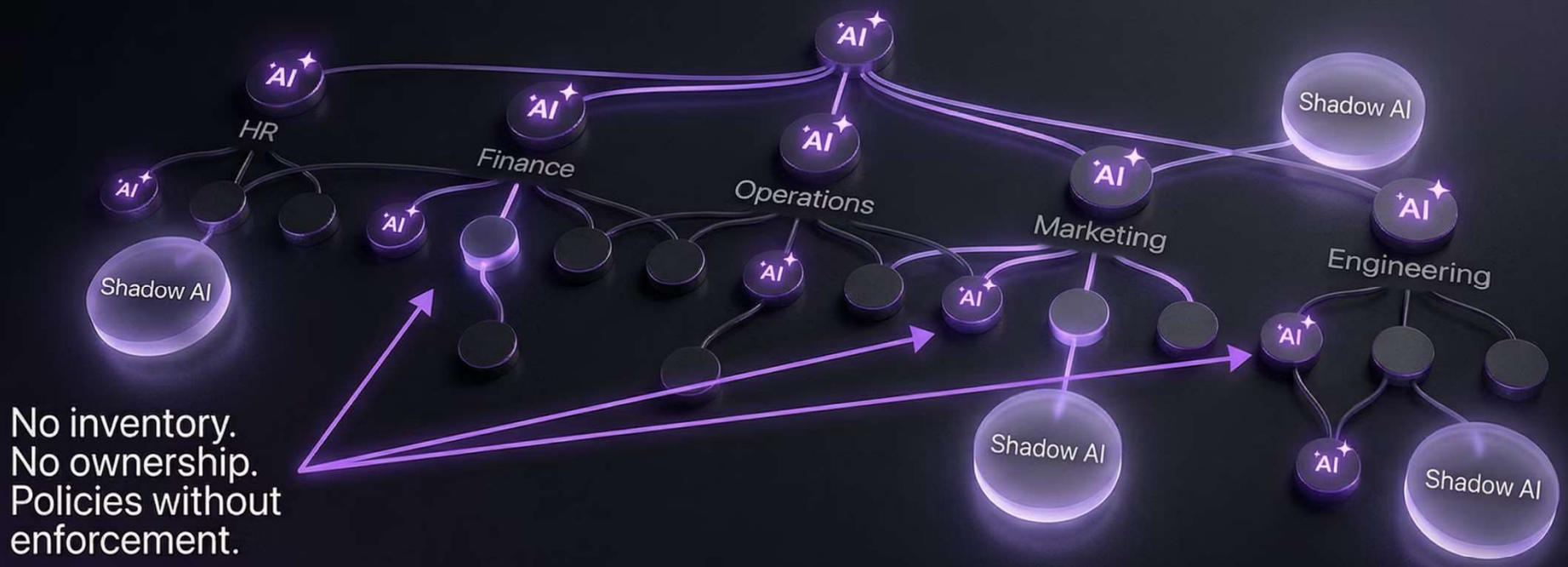
AI Understands Meaning, Not Just Format

AI Agents Change Risk Level

Agents are autonomous operators, not tools.

Permissions × Chaining = Multiplied Risk.
IAM and PAM alone are insufficient.

AI Is Everywhere and Nowhere



No inventory.
No ownership.
Policies without enforcement.

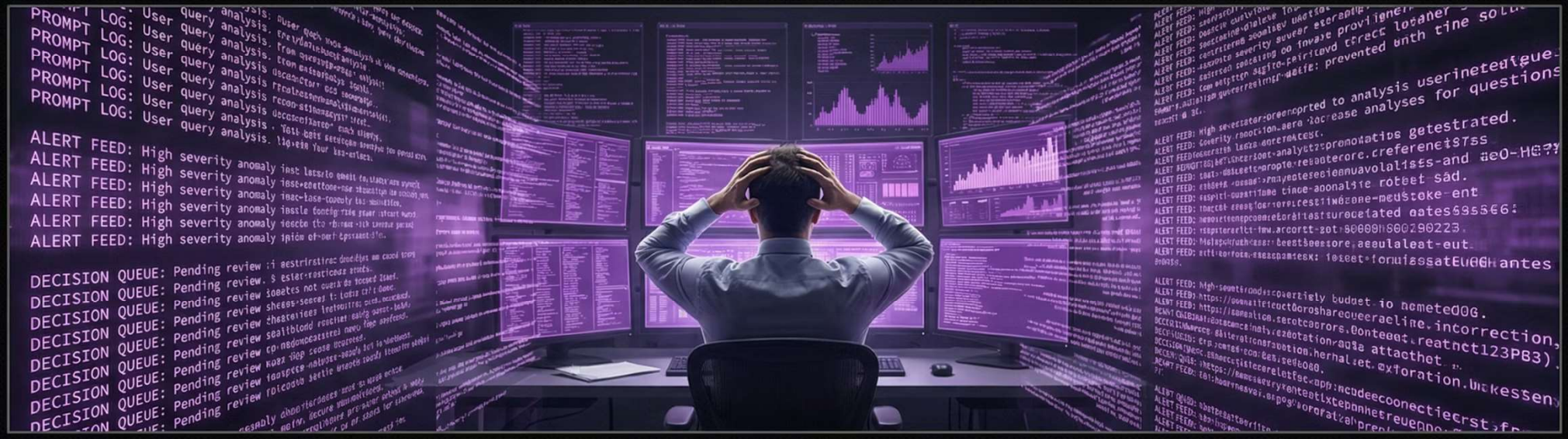
The biggest risk is uncontrolled internal usage.

You cannot govern what you cannot see.

AI Risk Is a Management Decision

AI risk is not an IT problem. It is a choice between efficiency and control.

Governance Alone Is Not Enough



- Volume exceeds human capacity
- Prompts cannot be manually reviewed
- SOC teams are already at saturation.

Governance defines direction. It cannot execute at machine speed.

Practical Governance Model

5. Technical Enforcement

4. Set Governance

3. Define Risk Appetite

2. Assess Impact

1. Identify AI Use

Why Defence Must Use AI

AI attacks cannot be handled without AI defence.

Triage at scale Automated prioritization	Contextual correlation	Humans handle exceptions

Security must operate at machine speed.

Governance + Technology = AI Resilience

AI Defence Model — Detect / Govern / Protect

	Users	Applications	Agents
Detect	Usage visibility	Shadow AI mapping	Action logging
Govern	Policy & awareness	Risk appetite rules	Permission scoping
Protect	Prompt filtering	Data loss prevention	Autonomous action limits

Governance connects visibility with enforcement.

CHECK POINT™

Thank you for your attention

Jiří Kohout

Cybersecurity Strategy Advisor - CEE, CISM

YOU DESERVE THE BEST SECURITY