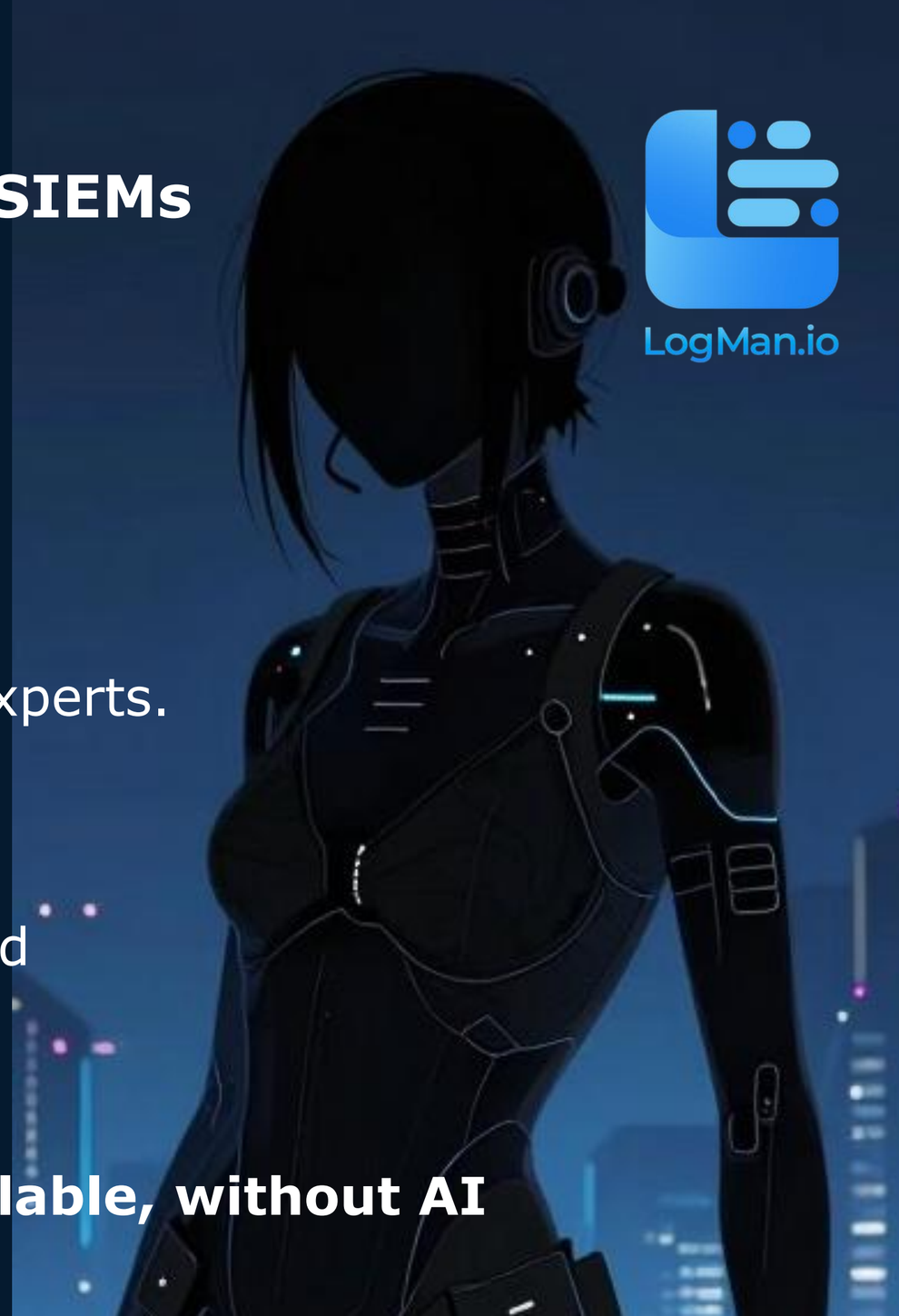

TeskaLabs
CYBER SECURITY
Aleš Teska
AI SIEM


Ministerstvo financí České republiky
UNIVERSITY HOSPITAL BRNO
O2
Bidfood
COMPOSITE SYSTEMS
nova
IK+E M
markíza
EUROVIA
Česká pošta
CME Group
Prima
MP SV
TeskaLabs
CYBER SECURITY
B R N O
SPORTISIMO
FAKULTNÍ NEMOCNICE VINOHRADY
EUROWAG
KSB
CETIN
ČLEN SKUPINY PPF
heureka!group

AI SIEM

The Market Problem: Nobody to Operate SIEMs



LogMan.io

The biggest challenge: shortage of cyber security experts.

Many alerts detected by SIEM are never investigated
SIEM often becomes just an expensive log storage

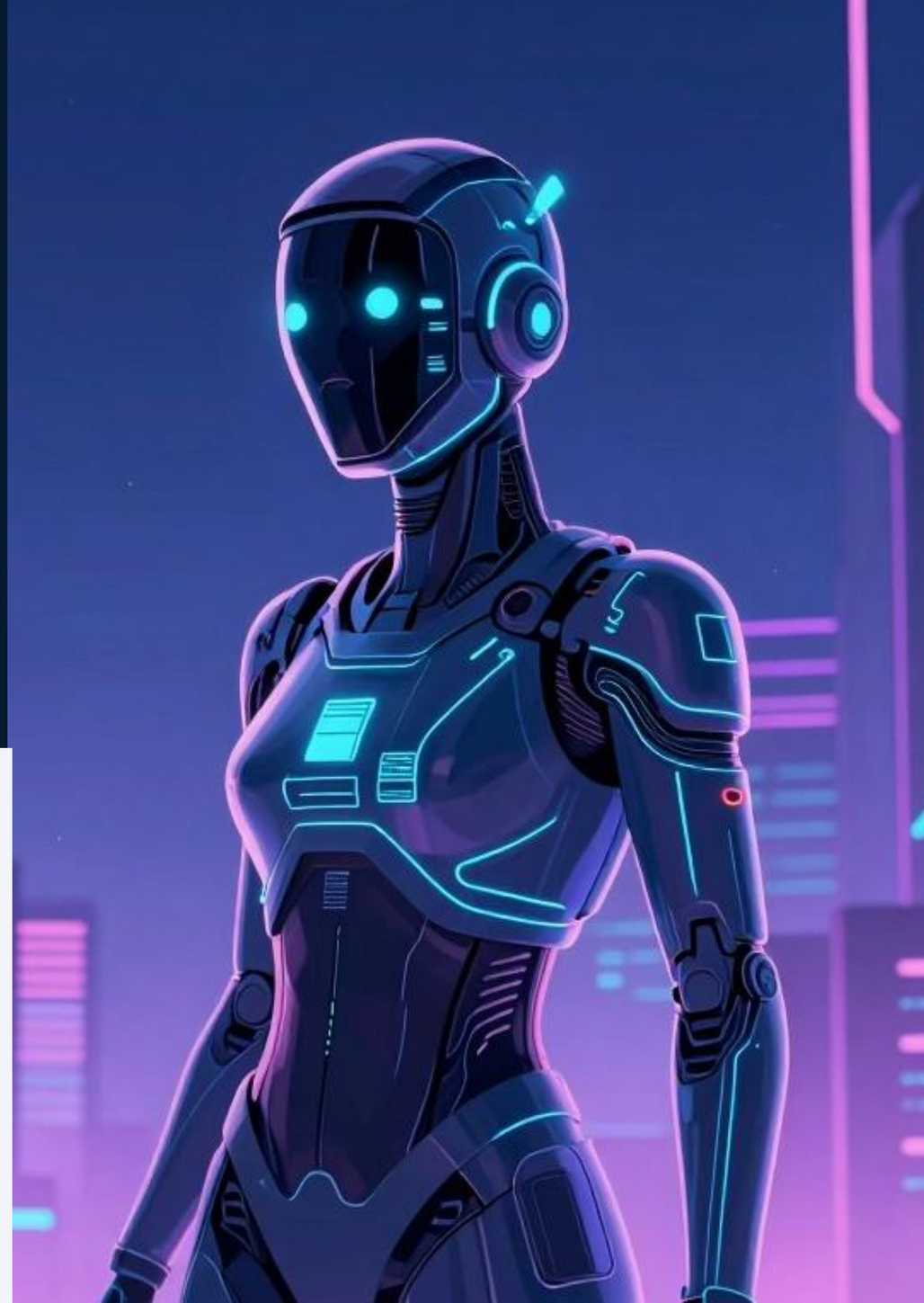
The current SIEM operational model is not scalable, without AI

AI SIEM
as an Automated Cyber Security Expert

Automation of routine cyber security activities:

- triage
- detection
- hunting
- response

AI is not “a chatbot over logs”,
it is active agent that performs tasks autonomously.



Parser Builder

Build a log parser for the given log examples and schema. Parsing is essential for log analysis and correlation.

Detection Agent

Authors and refines detection rules based on the latest threat intelligence. Backtests against historical data. Reduces false positives automatically using behavioral baselines.

Triage Agent

Enriches alerts with full context; correlating security events with business data, user behavior, and asset criticality. Prioritizes by actual risk, not just severity labels.

Hunting Agent

Proactively searches for threats using natural language queries across all of your logs. Translates analyst hypotheses into complex correlation queries.

Response Agent

Orchestrates automated response workflows. Isolates compromised assets, triggers notifications, creates tickets, and escalates to humans when judgment is needed.

LogMan.io



AI SIEM
Local AI inference

Data never leaves the EU jurisdiction.

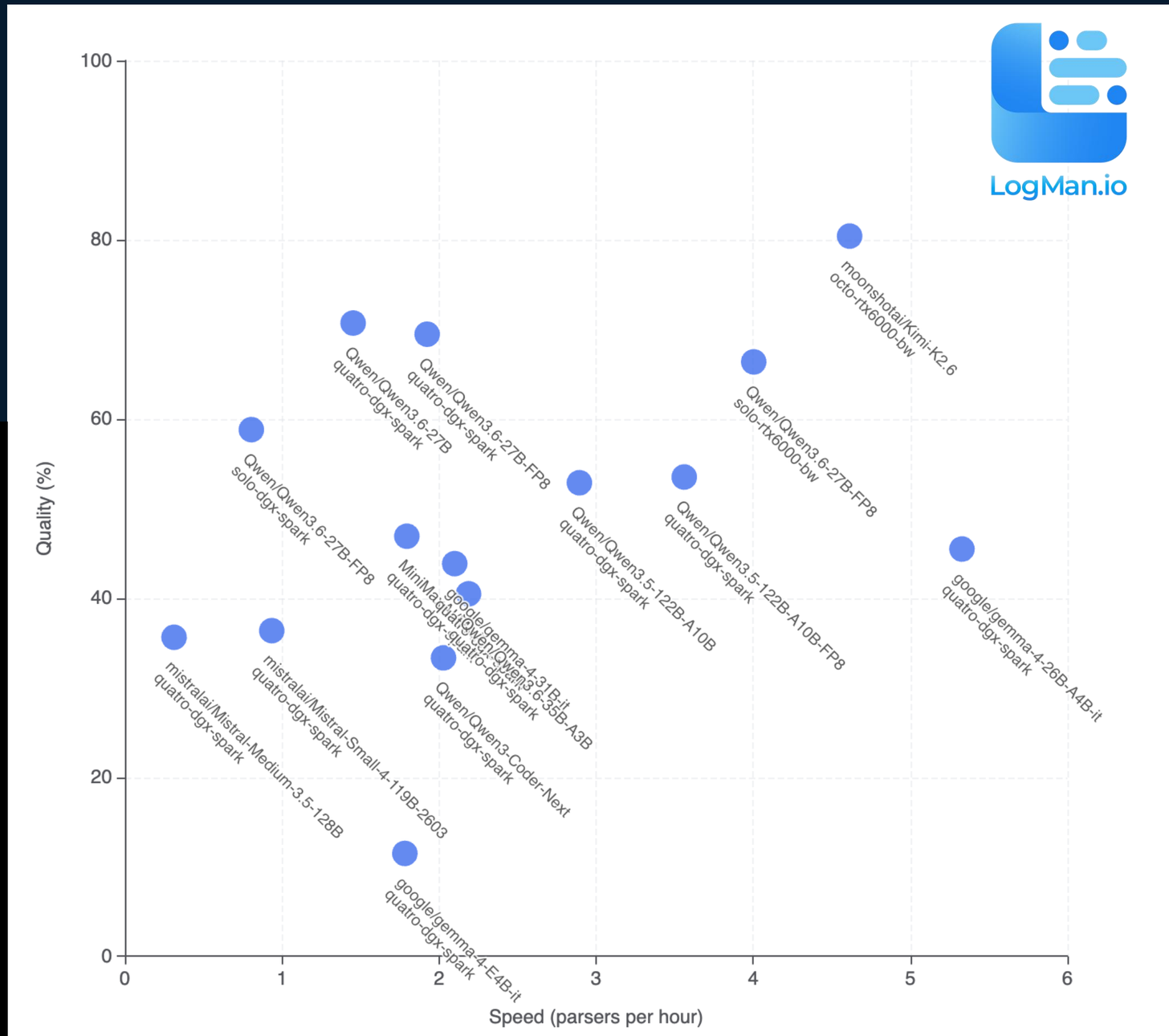
Local inference options:
- Our data centre in Czech Republic (EU)
- or fully on-prem deployment

Unparallel compliance with:
- GDPR
- NIS2
- EU AI Act

No sensitive data sent to to the US, to China or any public AI services.

AI SIEM
Technology Platform

Local AI inference by open-weight models in 1T class: Kimi K2.6



AI SIEM
Practical Use Case

1) A cyber security alert arrives

2) The AI agent:
- finds related logs and events
- builds context
- evaluates risk
- recommend next steps or
  execute the playbook as an automated response

Results:
- less manual work
- fully automated workflow for most common cases
- faster response times
- lower dependency on junior analysts
- better productivity of cyber security teams





AI SIEM Roadmap

LogMan.io

August 2026
- launch of pilot deployments
- onboarding of first early adopters
- selected customer integrations

Autumn 2026
- general platform availability
- commercial rollout

2027
- expansion of AI functionality

Current status
- actively recruiting pilot customers
- looking for early adoption partners
- opportunity for joint development of customer use cases

AI SIEM
Why This Is an Opportunity for you

AI transformation of the cyber security market is inevitable.

Customers will need:
- AI infrastructure
- GPU hardware
- local inference
- EU compliance-ready solutions



LogMan.io



AI SIEM

LogMan.io

We are looking for:
- pilot customers
- implementation partners

Opportunity to participate in:
- early adopter program
- pilot deployments
- joint customer projects

Benefits:
- early access to the technology
- ability to influence product direction
- joint business development opportunities

“AI will not replace SIEM. AI will change how SIEM operates.”


TeskaLabs
CYBER SECURITY
AI SIEM
Thank you.