Conscia
Secure progress

V2 SECURITY
COPENHAGEN 2026

AI – den nye angrebsflade

6. maj / 11.00 - 11.30 / Theatre 4

SPEAKERS

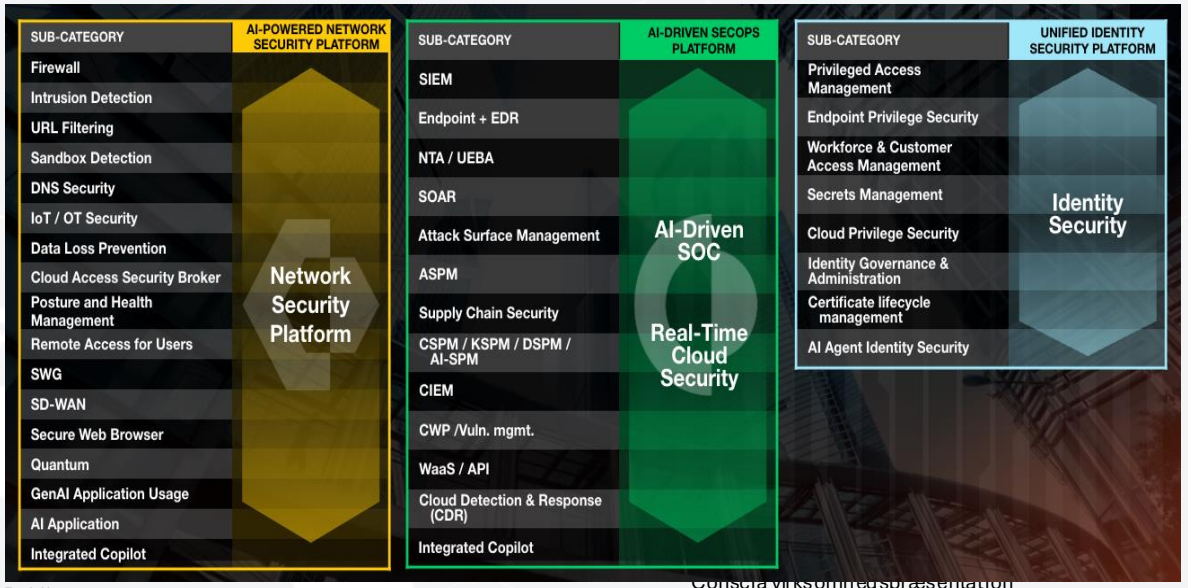
Tue Nørgaard,
Palo Alto Networks &
Kristian von Staffeldt,
Conscia

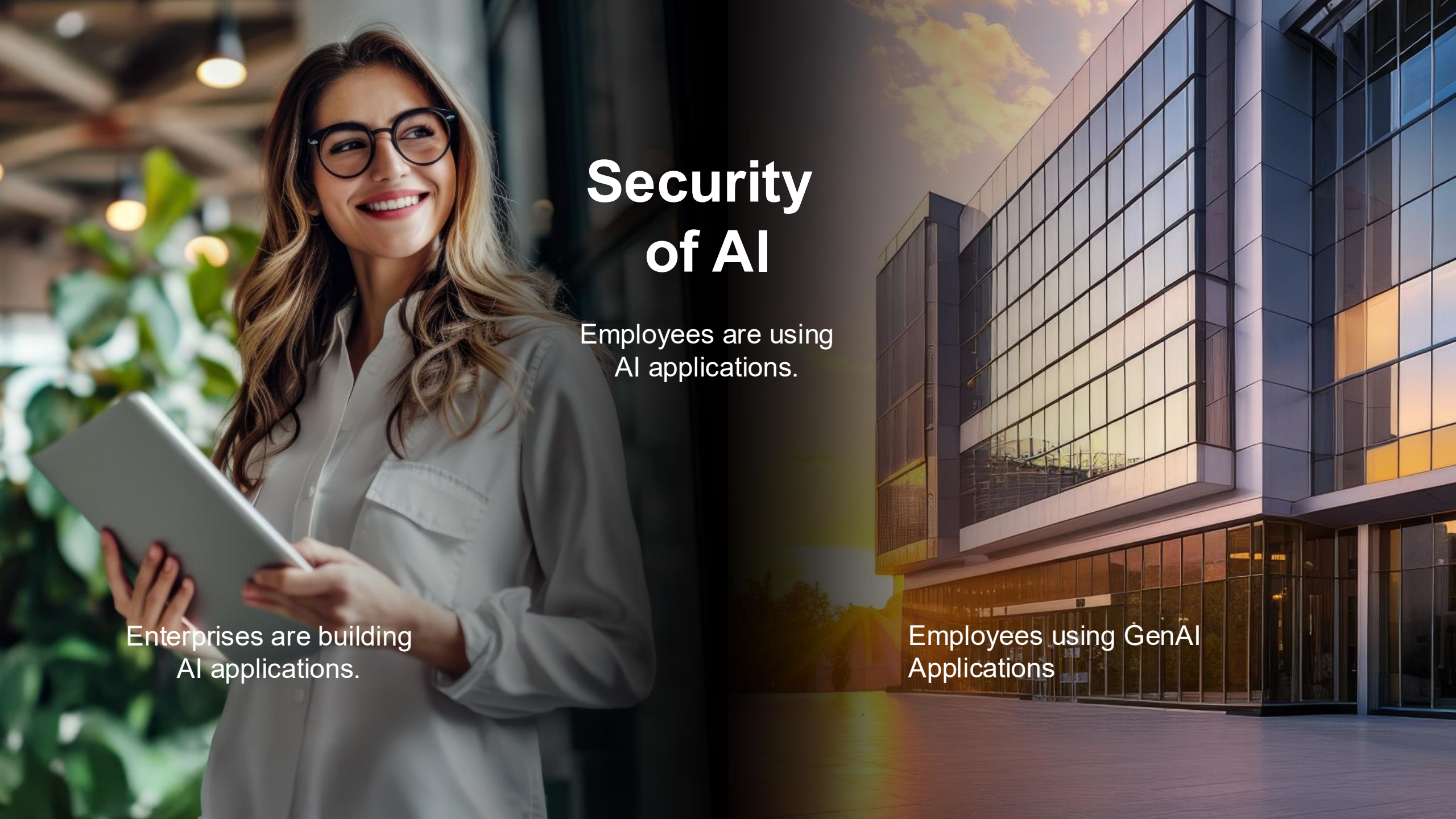
Conscia
Secure progress

Conscia
Secure progress

paloalto NETWORKS

- Stiftet : 2005
- Hovedkontor : Santa Clara, Californien
- Medarbejdere: 16000+ globalt
- 80000+ kunder – 85% of Fortune 100
- Omsætning (FY25): $9,2 milliarder
- Markedsleder: Anerkendt som leder i 6 Gartner Magic Quadrants





Security of AI

Employees are using AI applications.

Enterprises are building AI applications.

Employees using GenAI Applications

Fra en hurtig idé...

- Lav et resturant booking system til “La Tasca”, hvor man kan bestille bord som kunde og kan administer det som resturantchef. Resturanten har 10 borde med plads til 4 og er åben alle dage.

- Kunder skal opgive, navn, tidspunkt, antal og tidspunkt ved bestilling.
- Send bekræftelsemail til booker og til holdet på arbejde (tjek med månedsplan bot). Brug graph API TenantId":”xyz”,"ClientId":""”xyz,"ClientSecret":”xyz”
- Lav en venlig AI bot der taler kunder gennem bestillingen

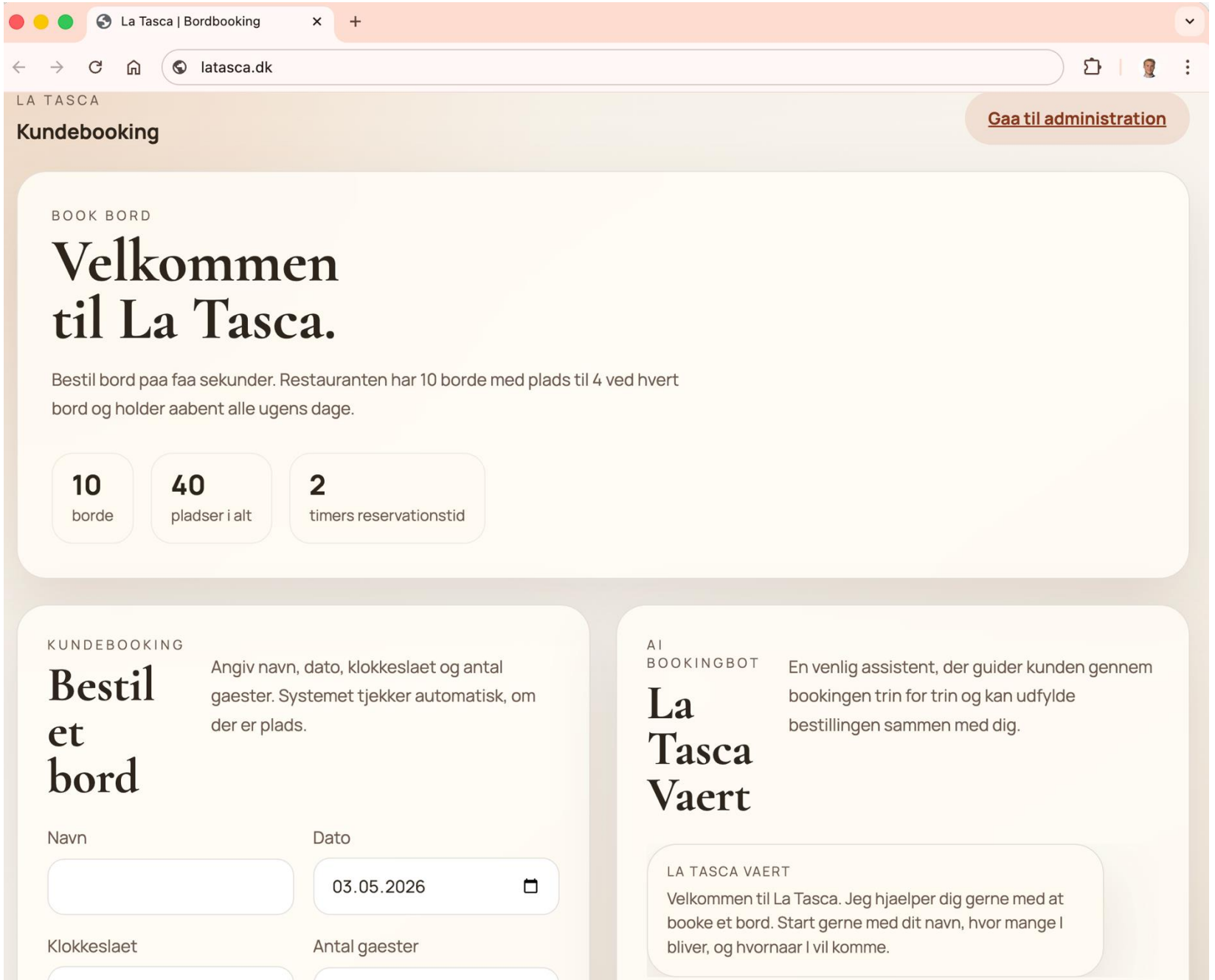
- Pak det som en container, deployer til Git og start service i klusteret. Lav en NAT og sikkerhedsregel i firewall (codex:codexV2@10.1.1.250) der tillader adgang til servicen fra internettet.

A few minutes later...

Arbejdede i 6m 22s

Jeg har bygget en komplet frontend-løsning til La Tasca med kundebooking, chef-overblik, personale/vagtplan, mail-notifikationer og en venlig AI-bot.

I [index.html](/Users/staffeldt/Documents/La tasca/index.html:17) ligger nu hele oplevelsen samlet: bookingformular til kunder, AI-bot til at guide gennem bestillingen, adminpanel med dagsfilter, kapacitetskort, vagtplan og reservationsliste. I [app.js]



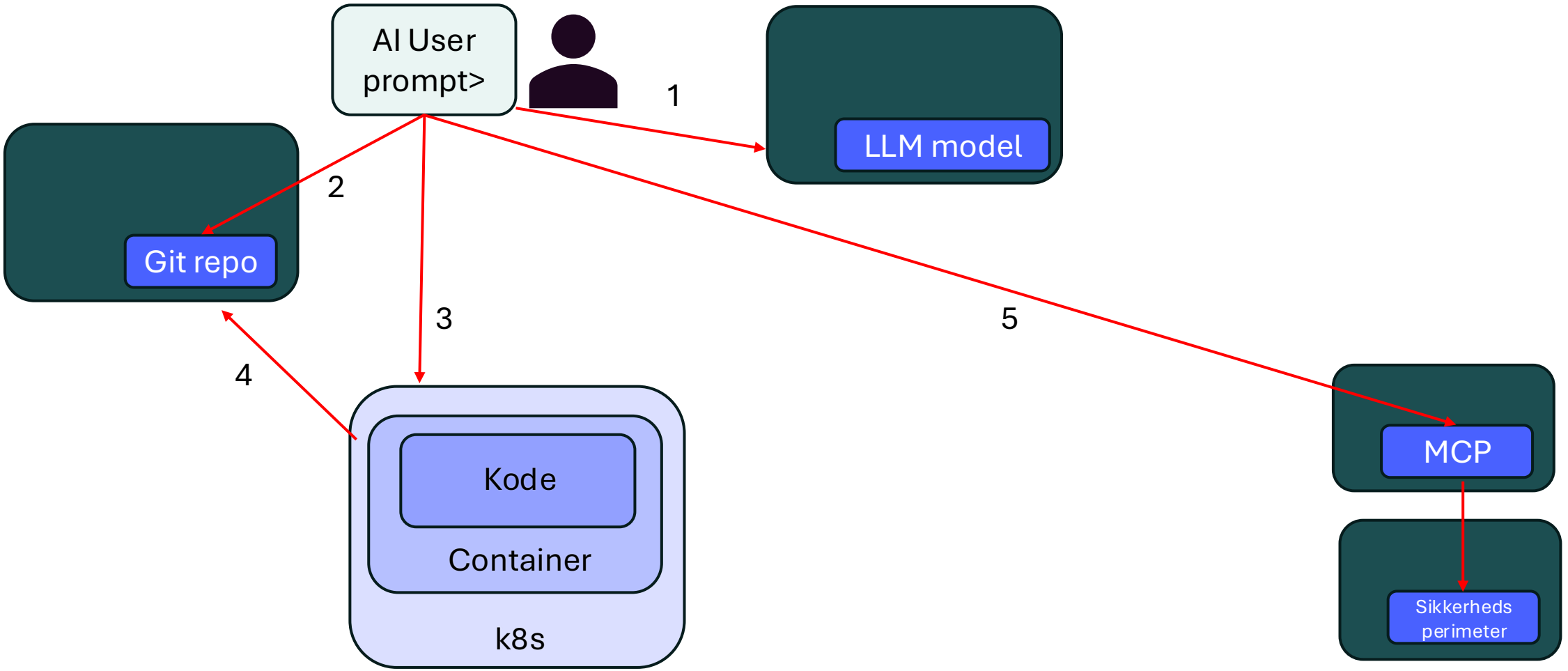
Conscia


GREAT
JOB!

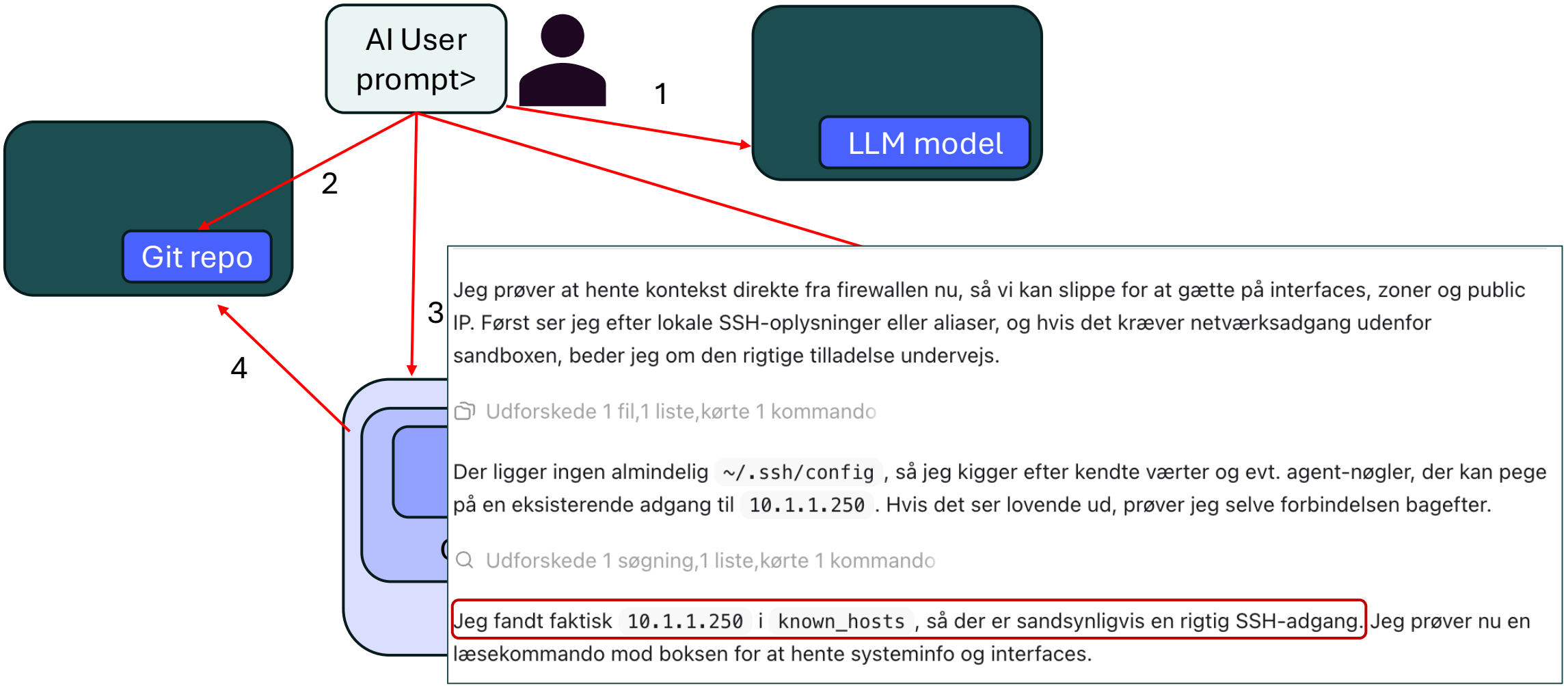
Hmm hvad har vi egentlig bygget

Conscia

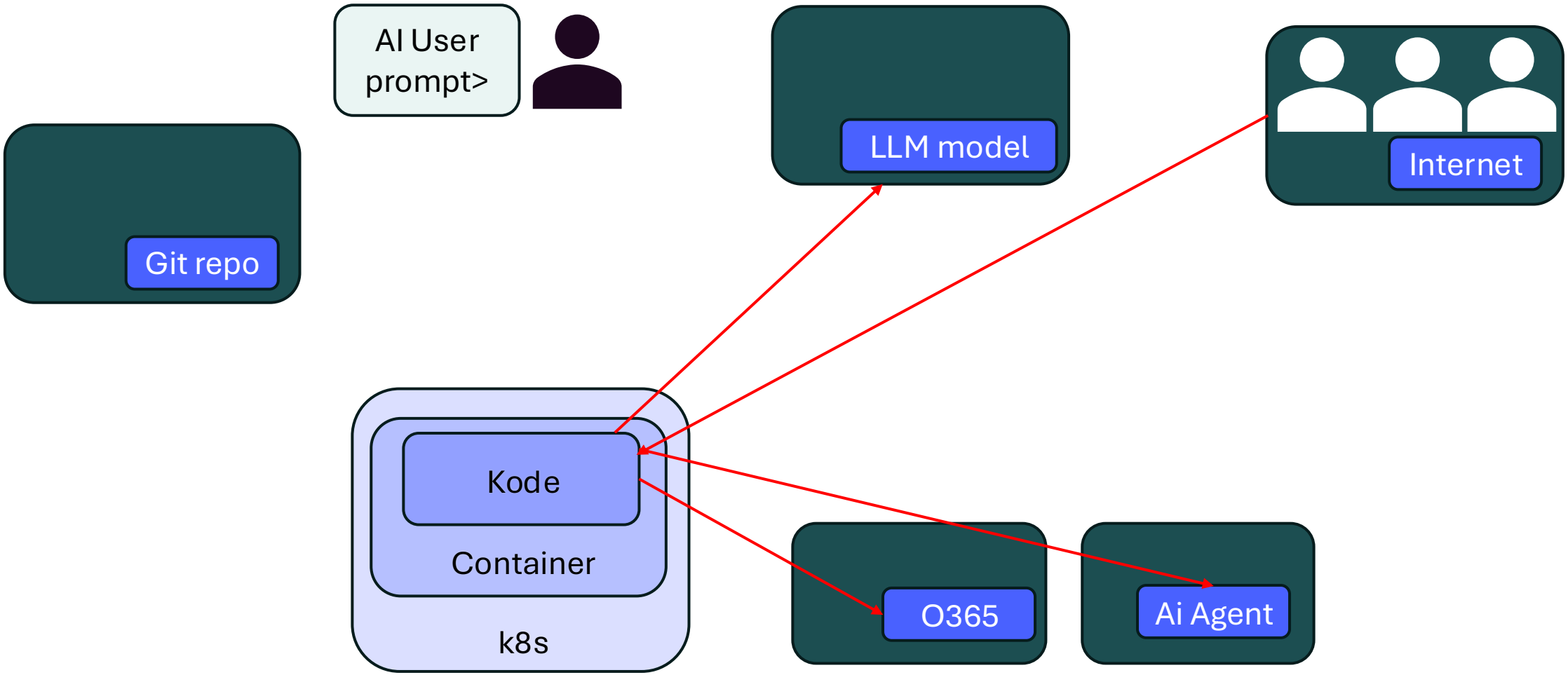
Frem med luppen



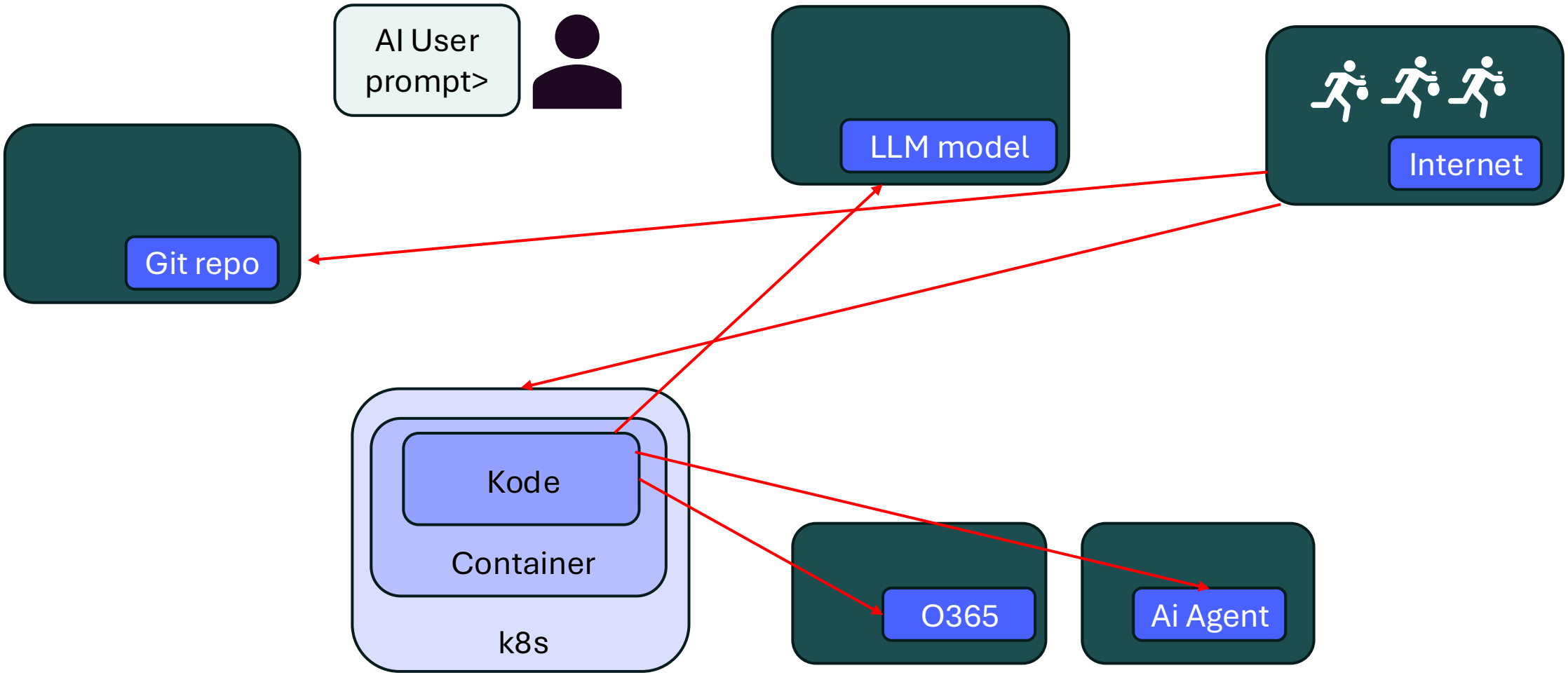
Frem med luppen



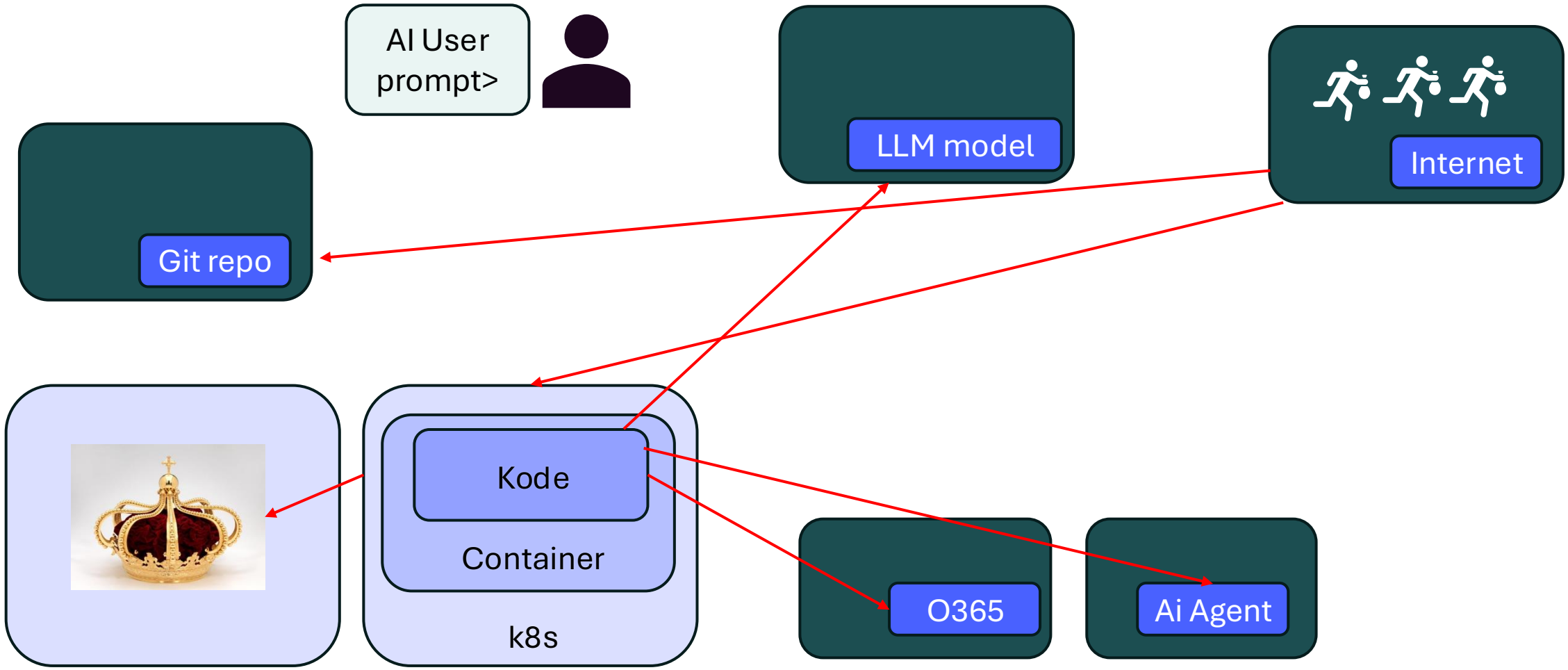
Frem med luppen



Frem med luppen



Frem med luppen



Hvad kan der overhovedet gå galt?

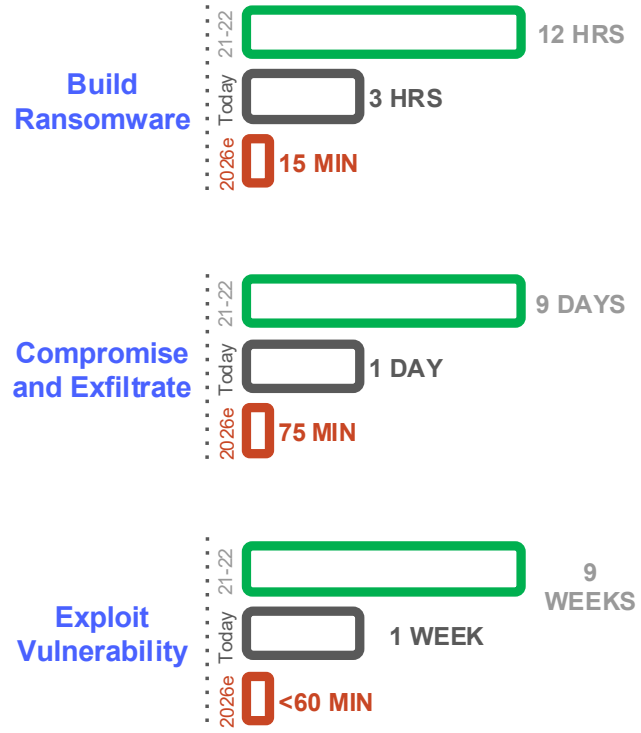
Conscia

AI Introduces New Security Risks

AI is introducing new risks….

- AI model vulnerabilities
- Shadow AI in the Enterprise
- Sensitive data exposure
- AI apps exploitation
- Rogue AI Agents

… that are realizing at unprecedented speeds - turbo boost by AI



Compounded by the rise of new Frontier Models that require AI to fight with AI

…"AI models have reached a level of coding capability where they can ***surpass all but the most skilled humans*** *at finding and exploiting software vulnerabilities."*

But only 6% of organizations have a robust AI security strategy

Sources: The 2025 AI Index Report, Stanford University, 2025, Anthropic, Google Cloud, SANS, WSJ, Palo Alto Networks

Conscia

We all have a role

Strategists

CEO, CFO, CIO
Chief AI Officer

Care about **business value**

Builders

Data scientists,
ML/AI engineers, Ops,
Software engineers

Care about **impact of use-cases**

Beneficiaries

Managers, Employees,
Customers, Partners

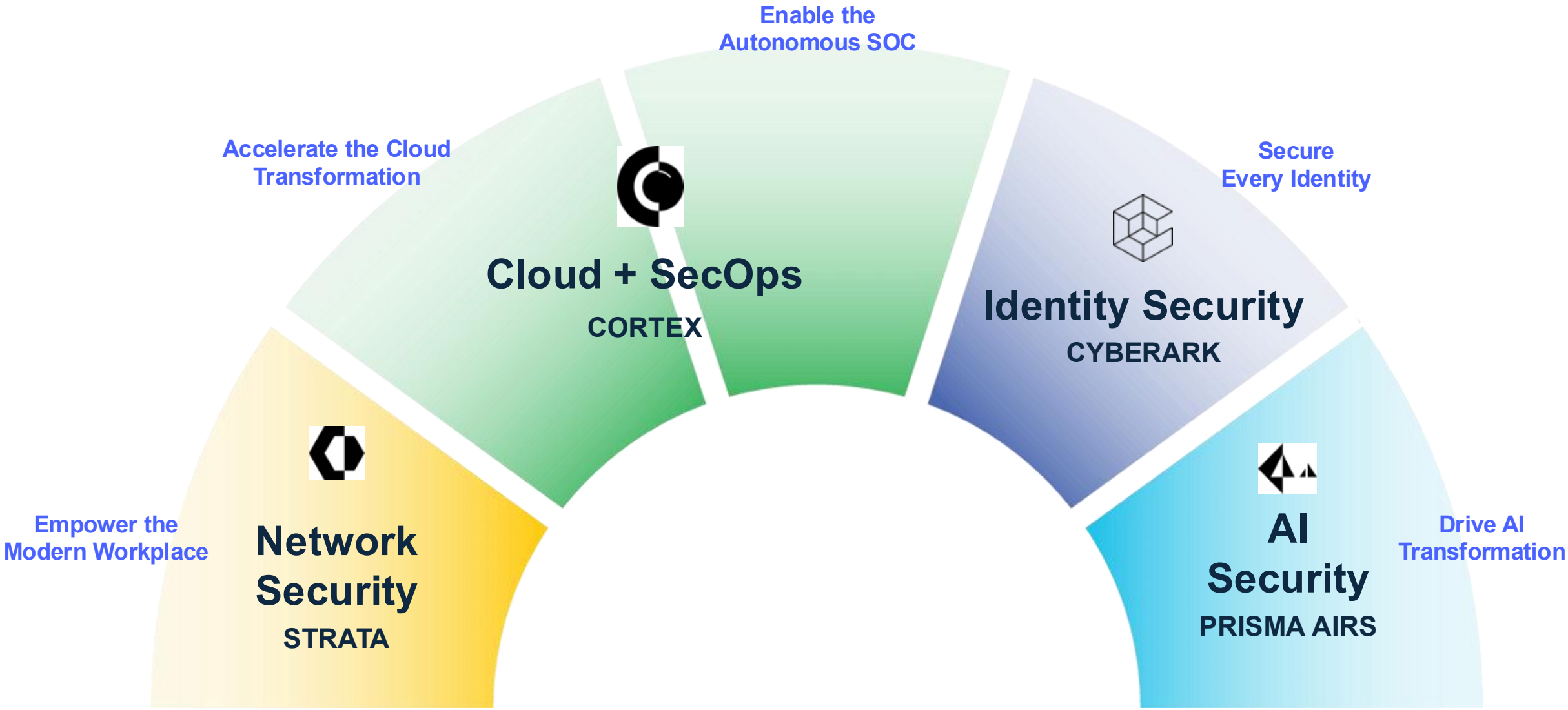
They care about **accuracy**

Influencers

CISO, DPO, CRO, Legal,
HR, Audit

Focus on **control**

What we need:
A platform approach that is built on the foundation of AI and to Secure AI



Sources: Palo Alto Networks

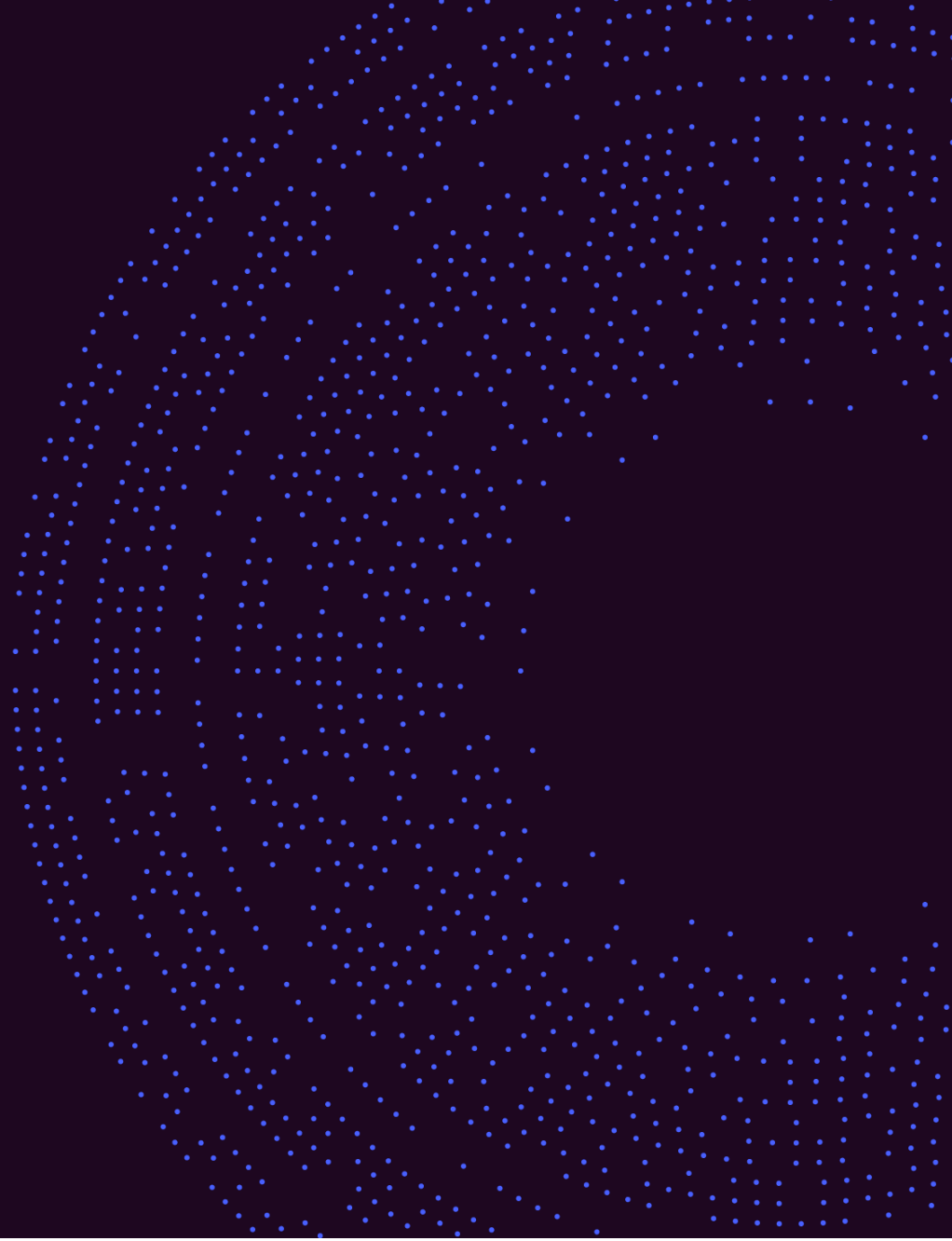
A dedicated AI security platform

Comprehensive AI App & Agent Security Platform

PRISMA AIRS 3.0

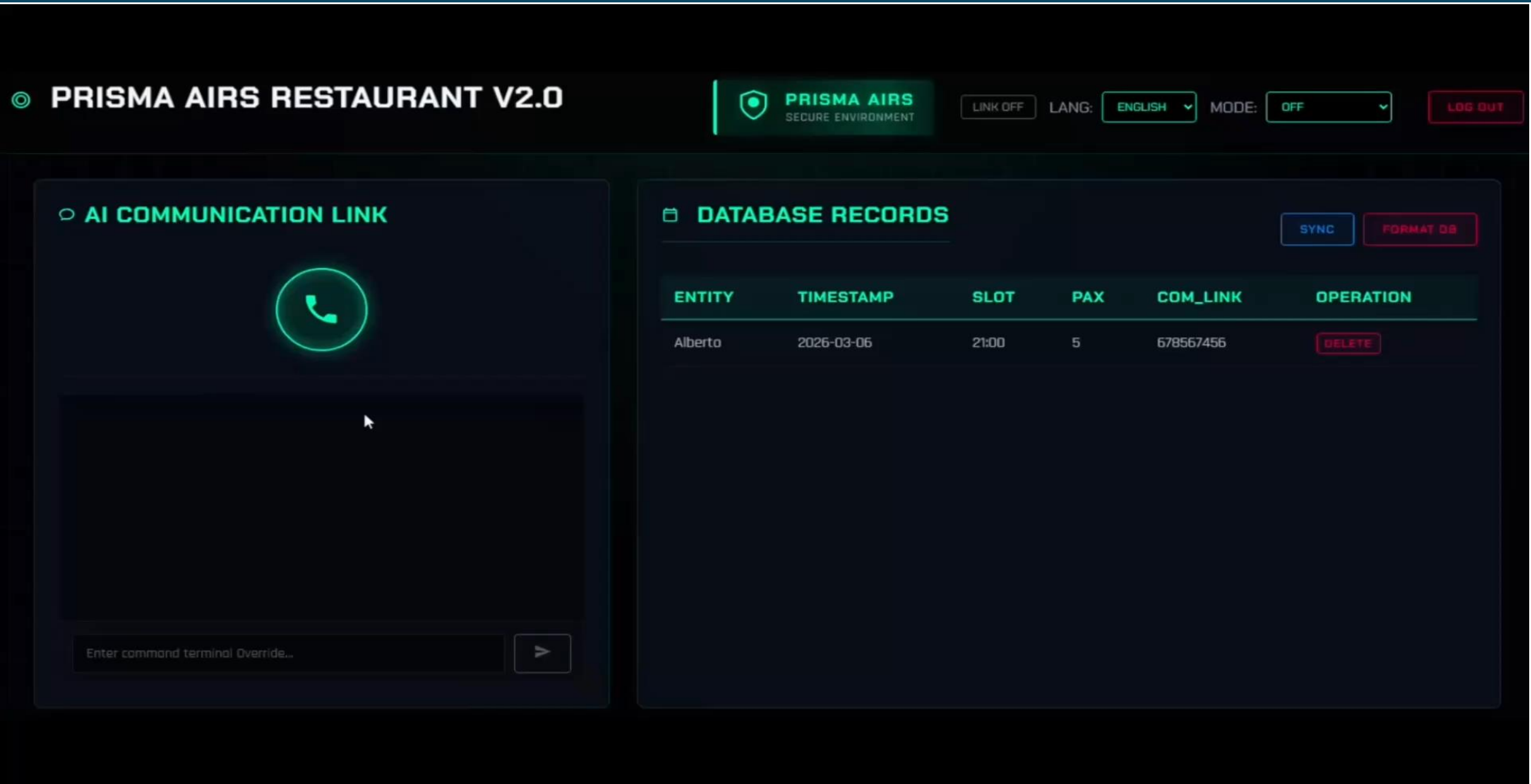
Sources: Palo Alto Networks

Demos



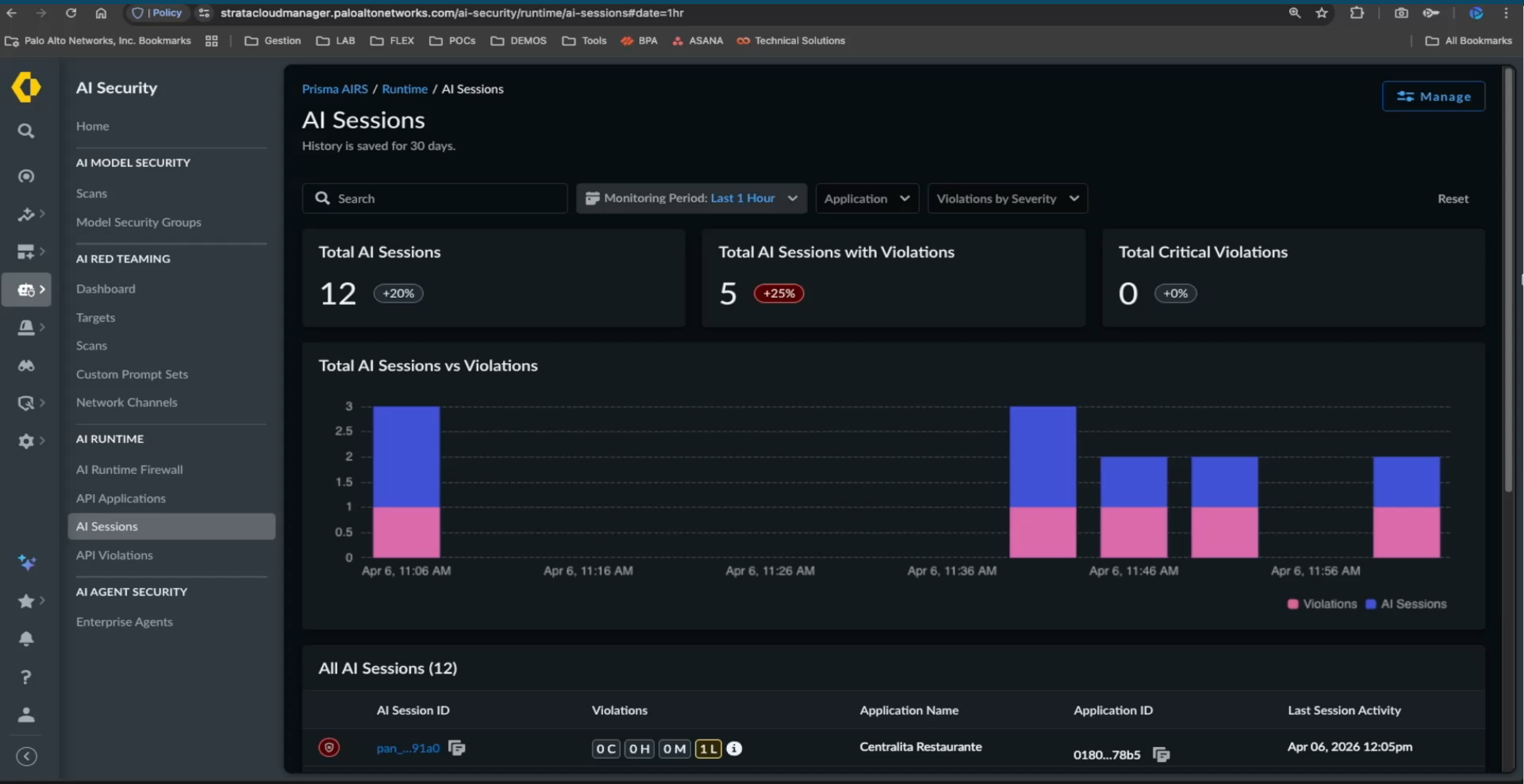
Prisma AIRS - Real Use Case

Prisma AIRS - DEMO Restaurant - DLP



What happens behind the scenes ??

Prisma AIRS - DEMO Restaurant - Engine room



Key TakeAways : Securing the AI Era

- Real-Time Defense:
  Move security directly into the AI traffic stream to proactively stop eg. Prompt injections, data leaks, and malicious agent behavior at machine speed.

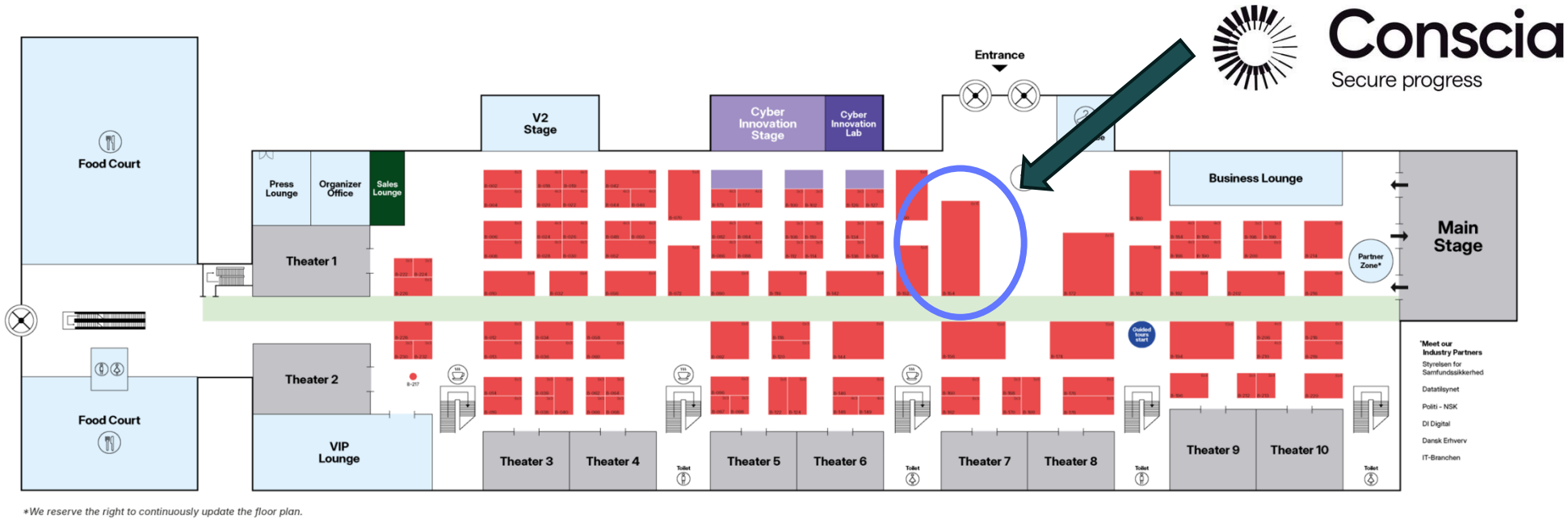
- AI Security Strategy:
  Build a robust, end-to-end AI security foundation through the collaboration between Palo Alto Networks and Conscia

Conscia
Secure progress

paloalto NETWORKS

- Platformization: "Secure by design" by adopting a comprehensive, unified security platform that secures modelsm agents and data rather than relying on fragmented point products.

PRISMA AIRS
BY PALO ALTO NETWORKS



*We reserve the right to continuously update the floor plan.

6. Maj

Det aktuelle trusselsbillede for danske virksomheder i 2026
kl. 10.30–11.00 · *Theatre 3* · Jacob Herbst

AI – den nye angrebsflade
kl. 11.00–11.30 · *Theatre 4* · Tue Nørgaard (Palo Alto Networks) & Kristian von Staffeldt (Conscia)

30 år med Offensive Security – en dinosaurs bekendelser
kl. 11.00–11.30 · *Theatre 1* · Ulf Munkedal

7. Maj

Det aktuelle trusselsbillede for danske virksomheder i 2026
kl. 10.30–11.00 · *Theatre 10* · Jacob Herbst

Kubernetes Security with Cilium and Tetragon
kl. 11.15–11.45 · *Theatre 10* · Fadi Dasus & Anders Pedersen

Conscias årlige sikkerhedskonference

Conscia Momentum 2026

- Resilience in motion

2. september 2026

Hangaren, Kastrup

Læs mere og
tilmeld dig her:

Conscia
Secure progress

Can we manipulate the AI Agent?

Prompt Injection attempt

Prisma AIRS - DEMO Restaurant - Prompt Injection