

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



- 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

SUB-CATEGORY	AI-POWERED NETWORK SECURITY PLATFORM	SUB-CATEGORY	AI-DRIVEN SECOPS PLATFORM	SUB-CATEGORY	UNIFIED IDENTITY SECURITY PLATFORM
Firewall	Network Security Platform	SIEM	AI-Driven SOC Real-Time Cloud Security	Privileged Access Management	Identity Security
Intrusion Detection		Endpoint + EDR		Endpoint Privilege Security	
URL Filtering		NTA / UEBA		Workforce & Customer Access Management	
Sandbox Detection		SOAR		Secrets Management	
DNS Security		Attack Surface Management		Cloud Privilege Security	
IoT / OT Security		ASPM		Identity Governance & Administration	
Data Loss Prevention		Supply Chain Security		Certificate lifecycle management	
Cloud Access Security Broker		CSPM / KSPM / DSPM / AI-SPM		AI Agent Identity Security	
Posture and Health Management		CIEM			
Remote Access for Users		CWP / Vuln. mgmt.			
SWG		WaaS / API			
SD-WAN		Cloud Detection & Response (CDR)			
Secure Web Browser		Integrated Copilot			
Quantum					
GenAI Application Usage					
AI Application					
Integrated Copilot					



Security of AI

Employees are using
AI applications.

Enterprises are building
AI applications.



Employees using GenAI
Applications

Fra en hurtig idé...



- > Lav et restaurant booking system til “La Tasca”, hvor man kan bestille bord som kunde og kan administrere det som restaurantchef. Restauranten 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]



LA TASCAS
Kundebooking [Gaa til administration](#)

BOOK BORD

Velkommen til La Tasca.

Bestil bord paa faa sekunder. Restauranten har 10 borde med plads til 4 ved hvert bord og holder aabent alle ugens dage.

10 borde
40 pladser i alt
2 timers reservationstid

KUNDEBOOKING

Bestil et bord

Angiv navn, dato, klokkeslaet og antal gaester. Systemet tjekker automatisk, om der er plads.

Navn

Dato

Klokkeslaet

Antal gaester

AI BOOKINGBOT

La Tasca Vaert

En venlig assistent, der guider kunden gennem bookingen trin for trin og kan udfylde bestillingen sammen med dig.

LA TASCAS VAERT

Velkommen til La Tasca. Jeg hjaelper dig gerne med at booke et bord. Start gerne med dit navn, hvor mange I bliver, og hvornaar I vil komme.

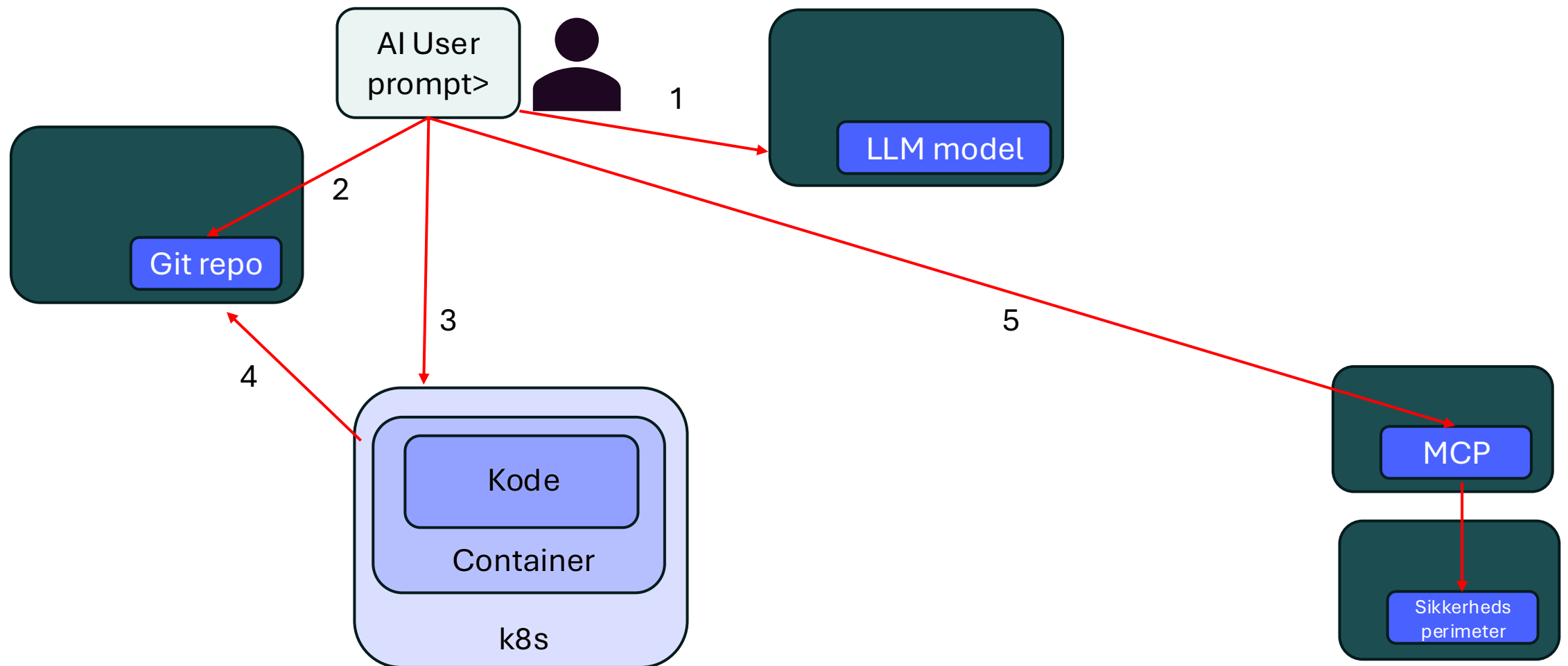
A cartoon illustration featuring a central thumbs-up gesture. The hand is rendered in a light tan color with thick, dark brown outlines and shading to indicate muscle and skin texture. The thumb is pointing upwards. The hand is set against a dark teal, jagged-edged starburst background. To the left of the hand, the word "GREAT" is written in a large, white, bubbly font with a dark brown outline and a slight shadow. To the right of the hand, the word "JOB!" is written in the same font style, also with a dark brown outline and shadow. The entire graphic is set against a white background with a pattern of small, light blue dots in the upper right quadrant.

GREAT JOB!

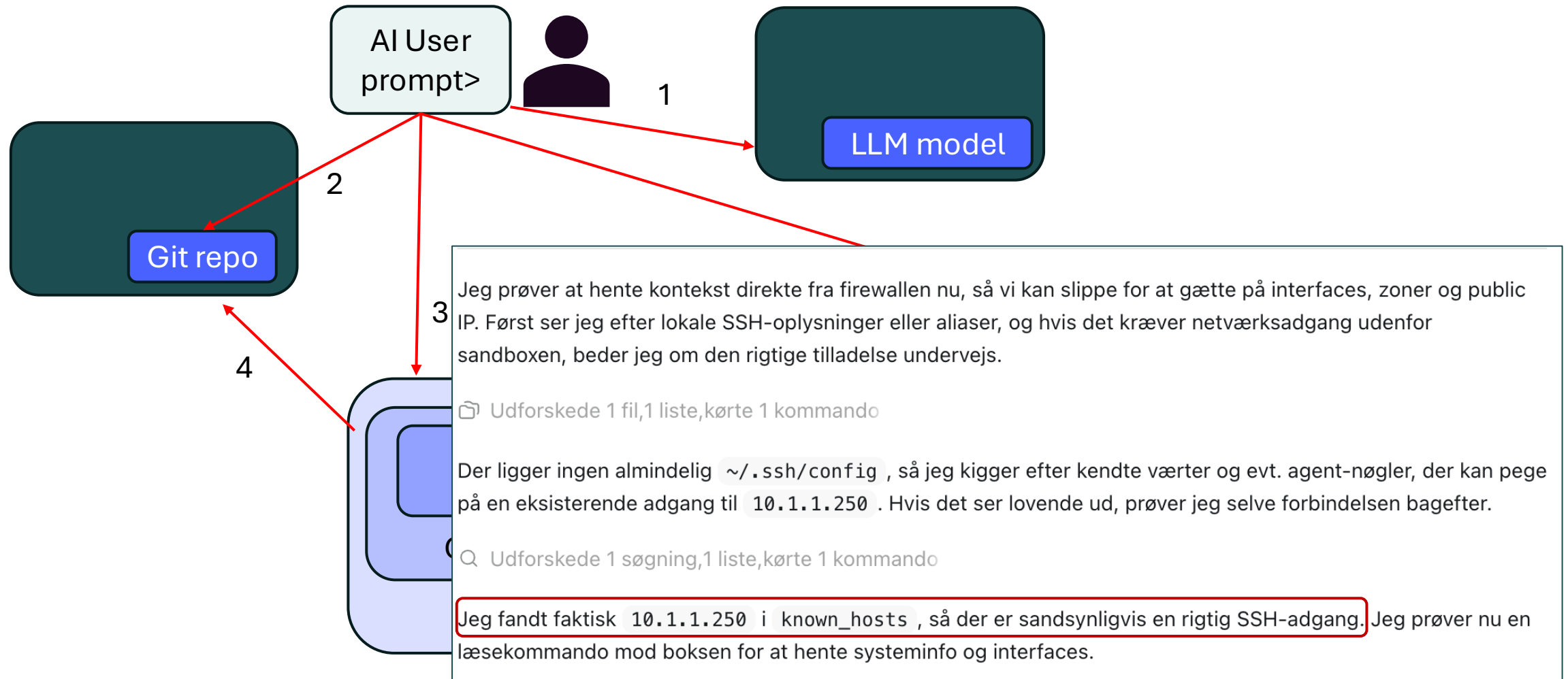


Hmm hvad har vi
egentlig bygget

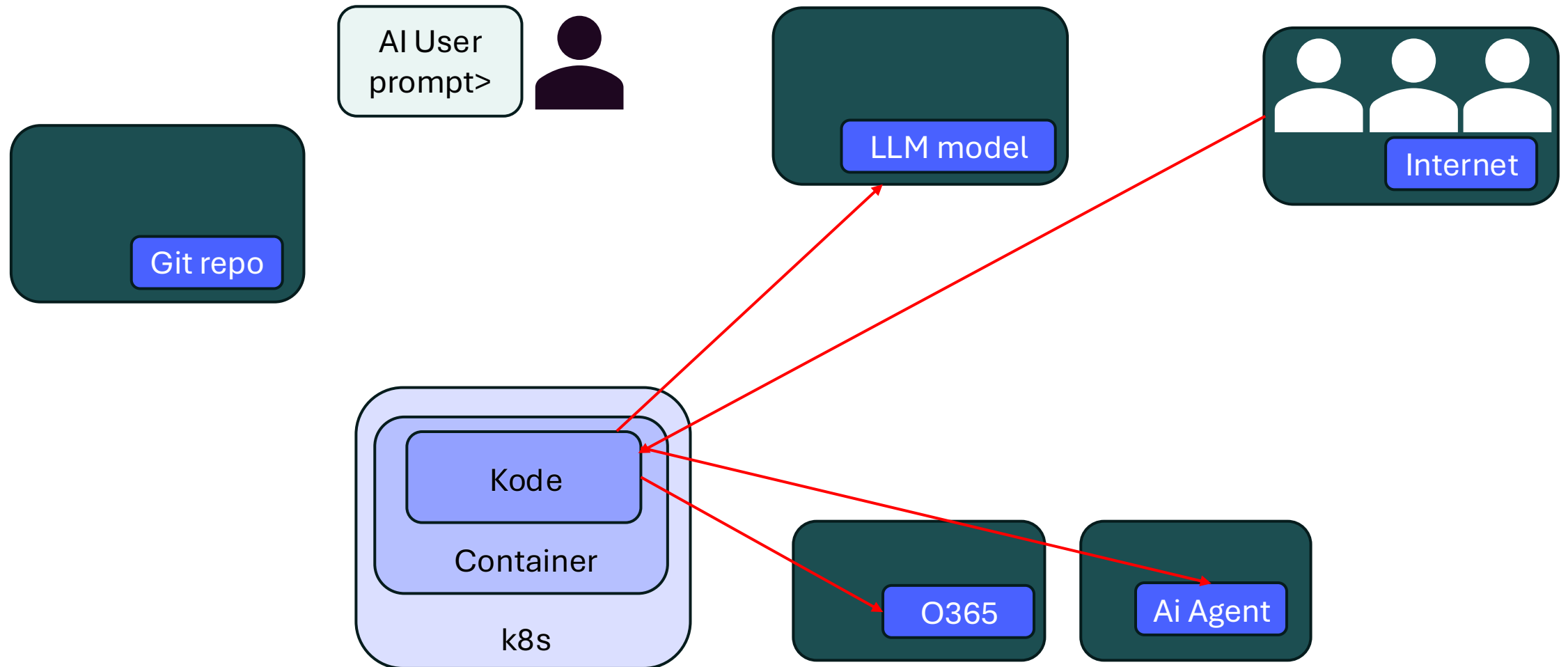
Frem med luppen



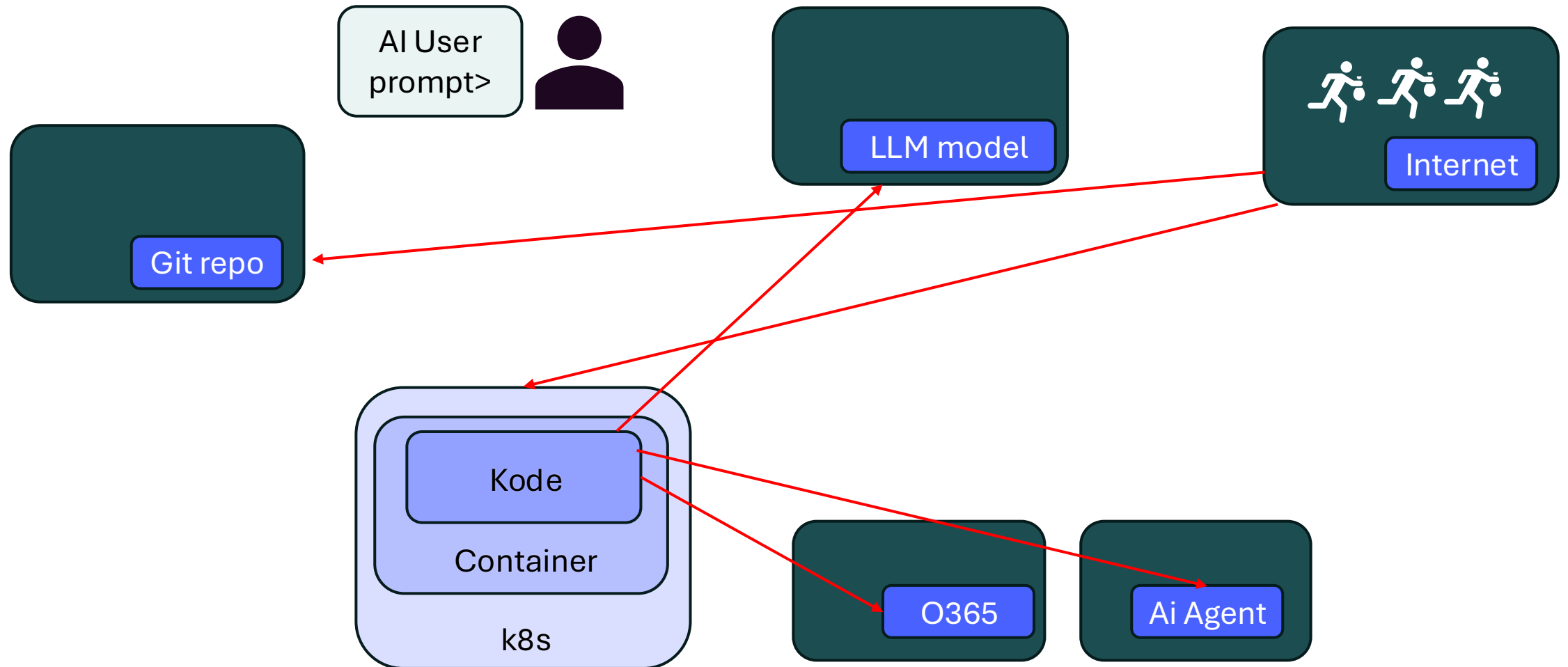
Frem med luppen



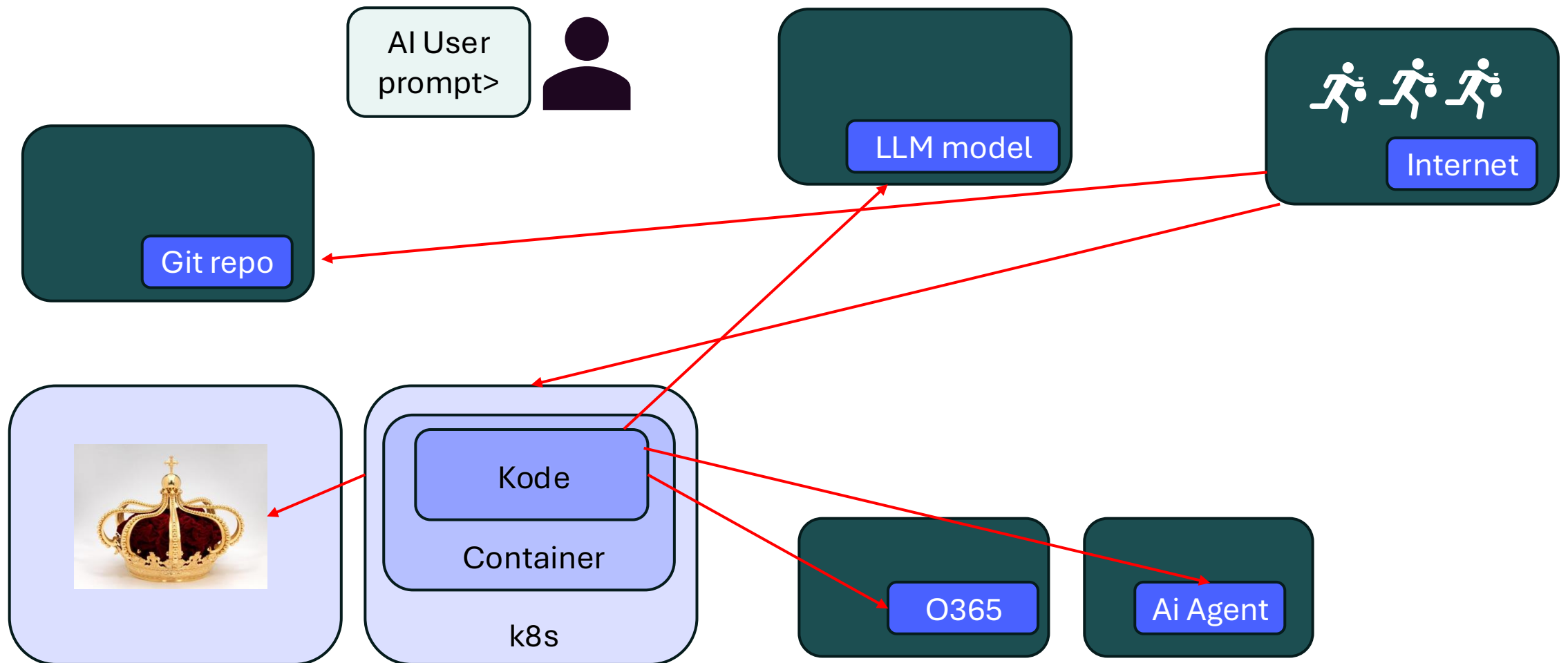
Frem med luppen



Frem med luppen



Frem med luppen





Hvad kan der
overhovedet gå
galt?

AI Introduces New Security Risks

AI is introducing new risks....



... 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 model vulnerabilities

Build Ransomware



Shadow AI in the Enterprise



Sensitive data exposure

Compromise and Exfiltrate



AI apps exploitation

Exploit Vulnerability



Rogue AI Agents



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

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

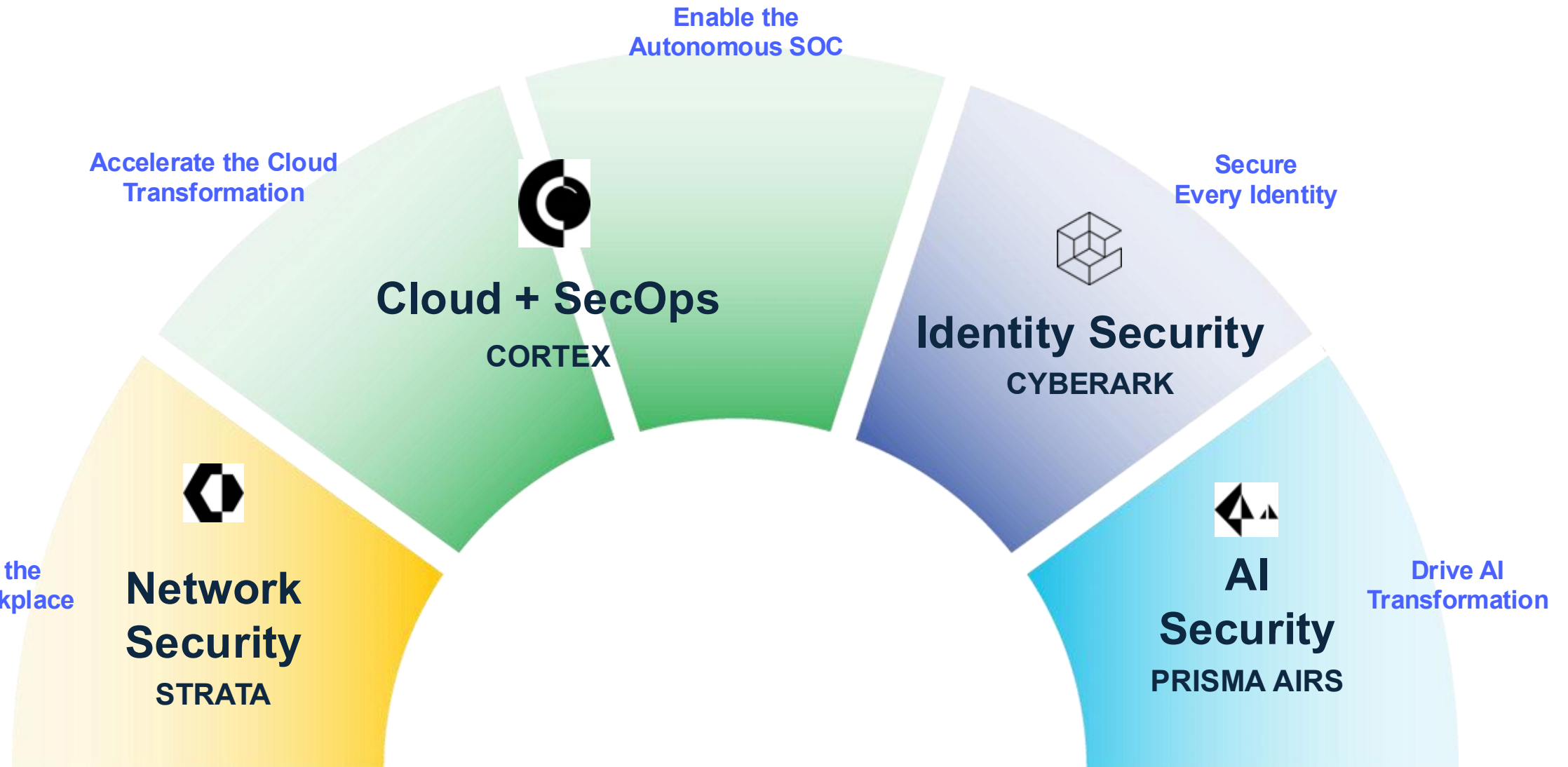


CISO, DPO, CRO, Legal,
HR, Audit

Focus on **control**

What we need:

A platform approach that is built on the foundation of AI and to Secure AI



A dedicated AI security platform

Comprehensive **AI App & Agent Security Platform**

PRISMA AIRS 3.0

AI Model + Agent
Artifact scanning



Agent Red
Teaming



Agent Posture
Management



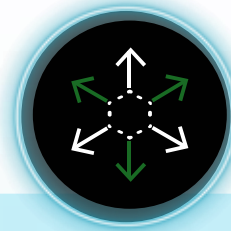
Agent Runtime
Security



Agent Identity
Security



AI Agent
Gateway



Demos

Prisma AIRS - Real Use Case





PRISMA AIRS
SECURE ENVIRONMENT

LINK OFF

LANG:

ENGLISH

MODE:

OFF

LOG OUT

AI COMMUNICATION LINK



Enter command terminal Override...



DATABASE RECORDS

SYNC

FORMAT DB

ENTITY	TIMESTAMP	SLOT	PAX	COM_LINK	OPERATION
Alberto	2026-03-06	21:00	5	678567456	DELETE

What happens behind the scenes ??

Prisma AIRS - DEMO Restaurant - Engine room

- AI Security
- Home
- AI MODEL SECURITY
 - Scans
 - Model Security Groups
- AI RED TEAMING
 - Dashboard
 - Targets
 - Scans
 - Custom Prompt Sets
 - Network Channels
- AI RUNTIME
 - AI Runtime Firewall
 - API Applications
 - AI Sessions**
 - API Violations
- AI AGENT SECURITY
 - Enterprise Agents

Prisma AIRS / Runtime / AI Sessions

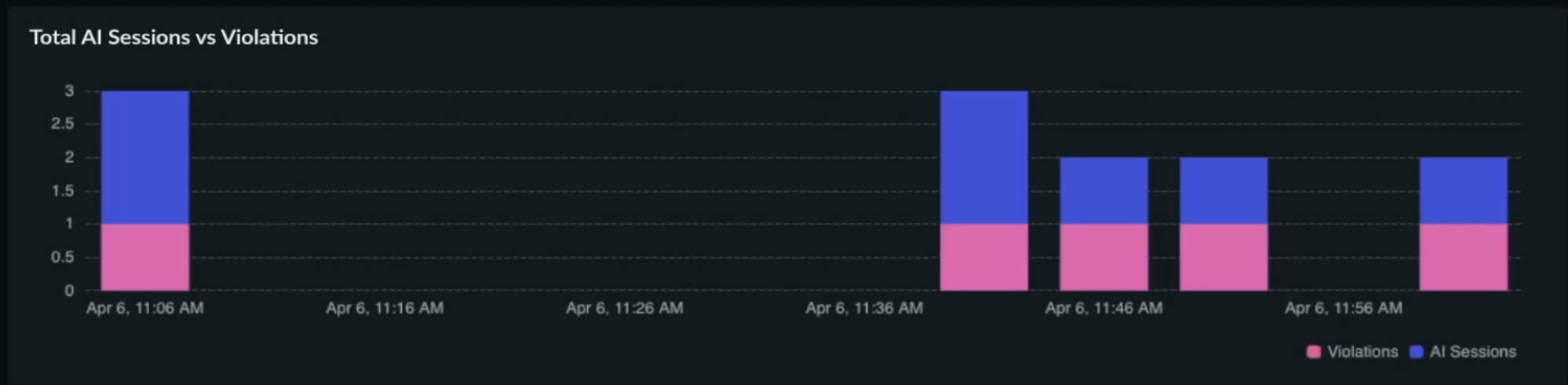
Manage

AI Sessions

History is saved for 30 days.

Search Monitoring Period: Last 1 Hour Application Violations by Severity Reset

Total AI Sessions 12 +20%	Total AI Sessions with Violations 5 +25%	Total Critical Violations 0 +0%
--	---	--



All AI Sessions (12)

AI Session ID	Violations	Application Name	Application ID	Last Session Activity
pan_...91a0	OC OH OM 1L	Centralita Restaurante	0180...78b5	Apr 06, 2026 12:05pm

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



Conscia
Secure progress





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

PRISMA AIRS RESTAURANT V2.0



PRISMA AIRS
SECURE ENVIRONMENT

LINK OFF

LANG:

ENGLISH

MODE:

MAX SECURITY

LOG OUT

AI COMMUNICATION LINK



Enter command terminal Override...



DATABASE RECORDS

SYNC

FORMAT DB

ENTITY	TIMESTAMP	SLOT	PAX	COM_LINK	OPERATION
Laura Gomez	2026-04-07	12:30	2	6123457891	DELETE
Alberto	2026-03-06	21:00	5	678567456	DELETE