AI I Praktiken

Hur ska man tänka kring AI och cybersäkerhet?

Susanna Hellström Gefwert
CatapultAI

Camilla Lundahl
Cyrenity AB

AI är kraftfullt, men hur håller vi det säkert? Här är svaren på några vanliga frågor!

01

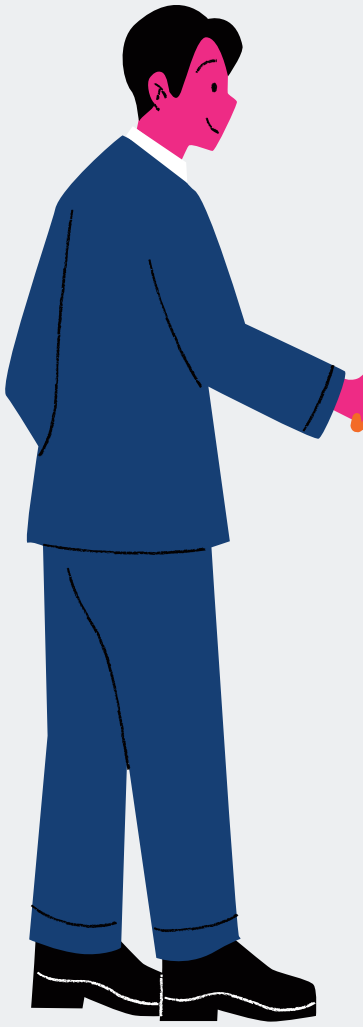
Vad är det viktigaste för dig som medarbetare att tänka på när du tar in en ny AI-produkt?

- **Följ** företagets regler för tredjepart och öppen källkod.
- **Undvik** Shadow AI – använd bara AI-verktyg som är godkända.
- Om **reglerna** inte håller jämna steg med teknikutvecklingen, bidra till att uppdatera dem.

02

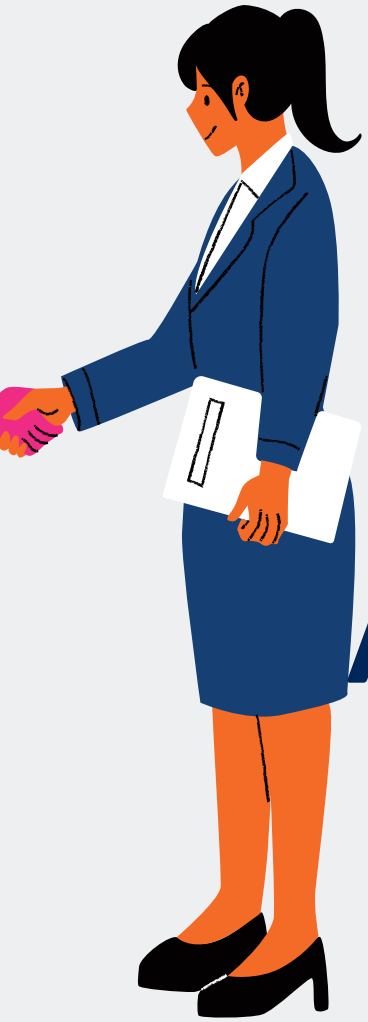
Vem bestämmer över AI-användning i företaget?

- **Företagsledningen** behöver sätta riktningen.
- Bestäm vem som ansvarar för AI-användningen.
- Skapa en **AI-policy** eller allra helst, inkludera AI i befintlig teknisk policy.
- Involvera gärna **CISO** eller liknande representant i processen
- AI är inte bara en IT-fråga – det är en fråga för **hela organisationen**.



Vilka risker behöver vi diskutera innan vi implementerar Gen AI?

- Vad kan gå fel om **AI:n** manipuleras eller slås ut?
- Kan AI:n **läcka** känslig information?
- Hur skyddar vi AI-integrationen från **cyberattacker**?
- Finns det både tekniska skydd och mänsklig **övervakning**?



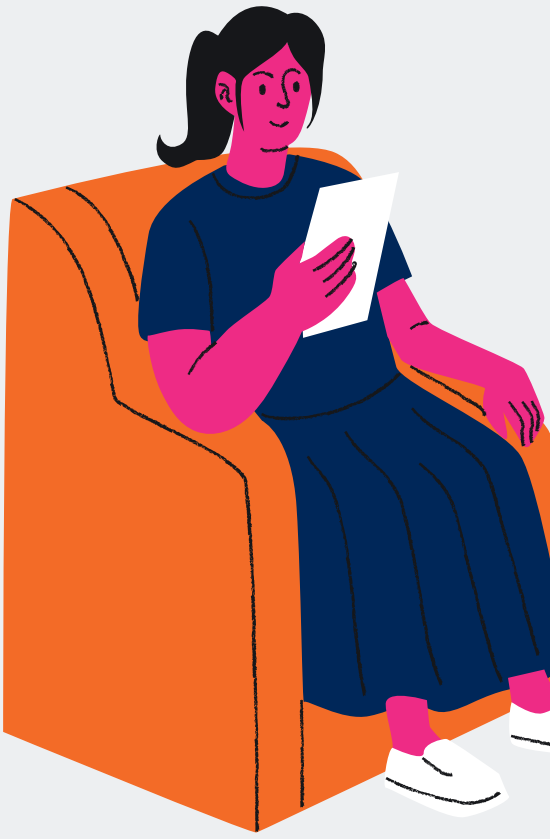
Hur undviker vi att AI-implementationen skapar nya säkerhetsproblem?

- Använd företagets befintliga **processer**, som inköpsrutiner eller new product approval (NPAP).
- Gör säkerhet som en del av AI-arbetet från början.
- Fundera över hur AI:n är annorlunda. Se över t.ex. arbetet med sårbarhetsscanningar samt loggar i och kring AI:n.

05

Hur kan vi som personal bidra till säker AI-användning?

- Mata inte AI:n med **känslig information.**
- **Utvärdera** innehåll innan användning eller publicering.
- Följ interna och externa **säkerhetsregler** (t.ex. er AI-policy).
- Var vaksam på **phishing** – även AI kan användas som attackverktyg.



06

Hur involverar vi organisationen i säkerhetsarbetet?

- Säkerhet handlar inte bara om teknik – det **handlar om människor**.
- Håll människan i **loopen** för att övervaka och förhindra fel.
- Skapa **utbildningar** som gör personalen AI-smart och säkerhetsmedveten.

Vad gör vi om vi inte har en AI-policy ännu?

- Börja med en enkel **riktlinje** som beskriver tillåten AI-användning.
- Inkludera AI i **befintliga** policys, som IT- eller säkerhetspolicyn.
- **Engagera** hela organisationen i diskussioner om AI och säkerhet.

AI är framtiden, men säkerhet är nyckeln.

Hur arbetar ni med AI och säkerhet i er organisation?

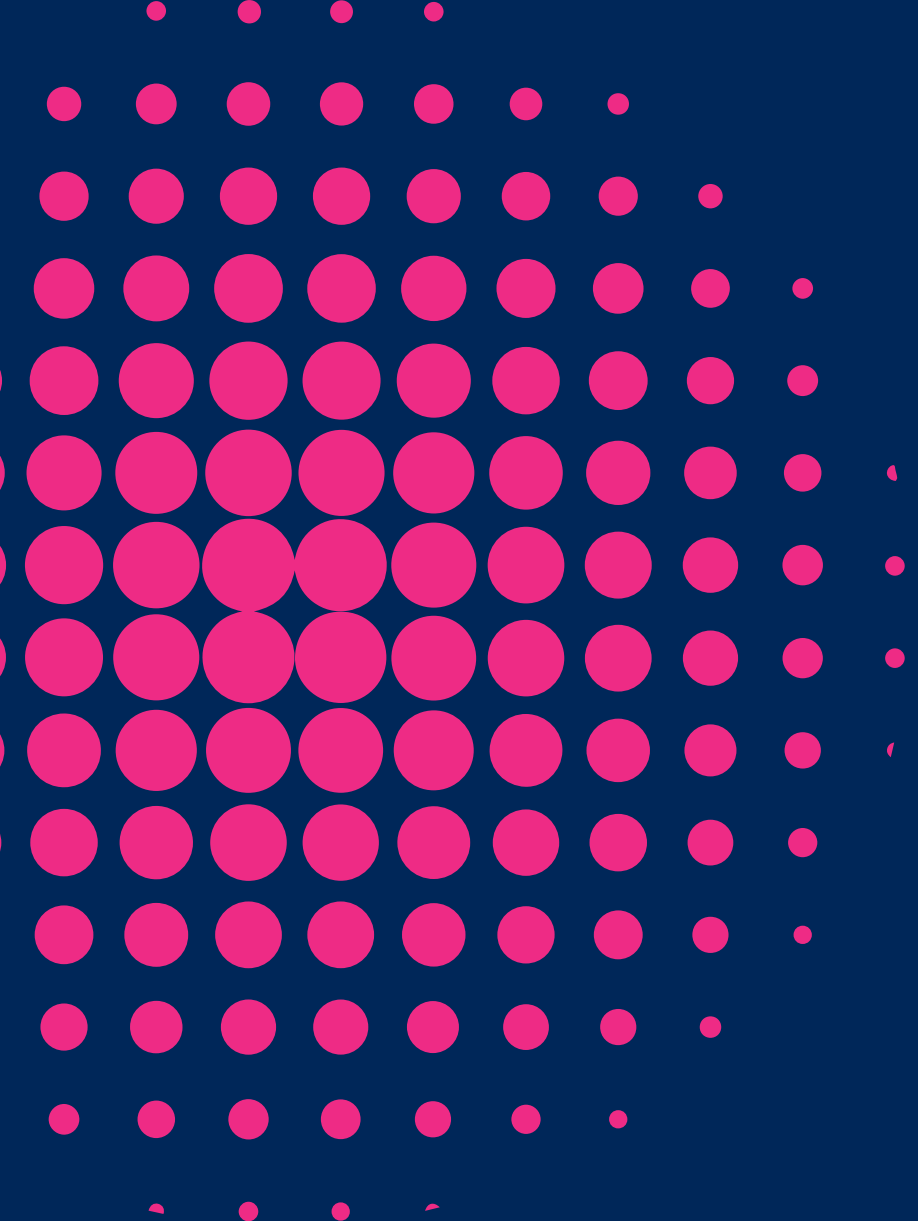
Om
Camilla Lundahl

Med +25 års säkerhetserfarenhet både som ledare, chef och säkerhetsspecialist inom privat och offentlig sektor är Camilla Lundahl en betrodd expert inom cybersäkerhet.

Om
Susanna Hellström Gefwert

Med gedigen teknisk erfarenhet som CTO och CEO skapar hon AI-lösningar som driver företagens tillväxt och främjar innovation.

info@catapult-ai.com



CatapultAI.

www.catapult-ai.com