AI in Practice

How should we think about AI and cybersecurity?

Susanna Hellström Gefwert
CatapultAI

Camilla Lundahl
Cyrenity AB

AI is powerful but how can we keep it safe? Here are some answers to common questions!

01

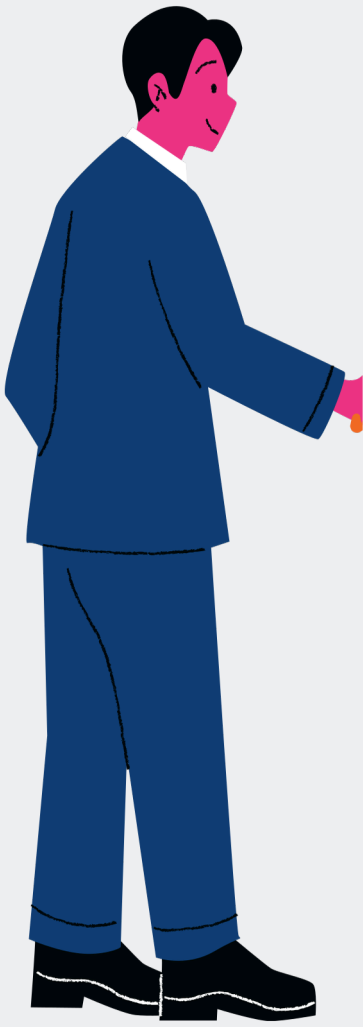
As an employee, what's most important to keep in mind when adopting a new AI product?

- **Follow** the company's rules for third-party and open-source software.
- **Avoid** "Shadow AI" only use AI tools that are approved.
- If the **rules** can't keep up with technological developments, help update them.

02

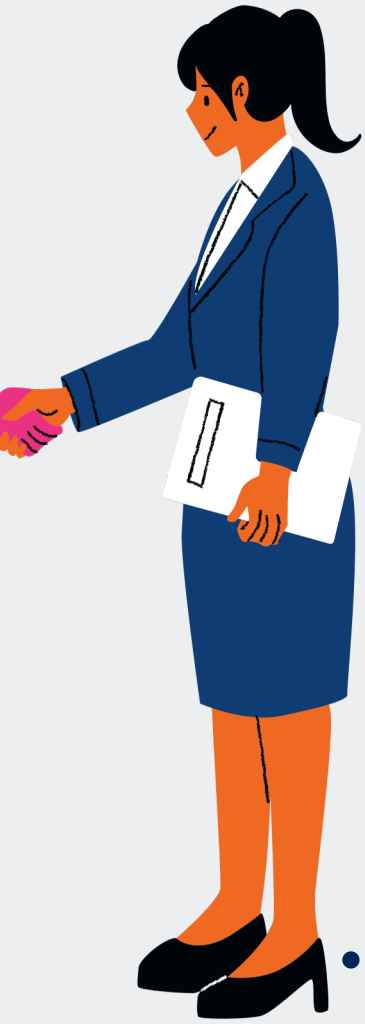
Who decides on AI use in the company?

- The company's leadership needs to set the direction
- Determine who is responsible for AI use.
- Create an AI policy or, even better, include AI in the existing technology policy.
- Ideally, involve the CISO or a similar representative in the process.
- AI is not just an IT matter, it's an organization-wide matter.



What risks do we need to discuss before implementing Gen AI?

- What can go wrong if the **AI** is manipulated or disabled?
- Can the AI **leak** sensitive information?
- How can we protect the AI integration from **cyberattacks**?
- Are there both technical safeguards and human **oversight**?



How can we prevent the AI implementation from creating new security issues?

- Use the company's existing processes such as procurement routines or New Product Approval (NPAP).
- Make security part of AI work from the start.
- Consider how the AI differs from other systems. Review, for example, vulnerability scanning practices and the logs in and around the AI.

05

How can employees contribute to the safe use of AI

- Do not input **sensitive information** into the AI.
- **Evaluate** content before using or publishing it.
- Follow internal and **external security** rules (e.g. your AI policy).
- Be alert to **phishing**, AI can also be used as an attack tool.

06

How can we involve the organization in security efforts?

- Security isn't just about technology, it's about **people**.
- Keep humans in the **loop** to monitor and prevent errors.
- Create **training programs** that makes staff AI-savvy and security-aware.

What if we don't have an AI policy yet?

- Start with a simple **guideline** describing permitted AI use.
- Include AI in **existing policies**, such as your IT or security policy.
- **Engage** the entire organization in discussions about AI and security.

AI is the future, but security is the key.

How does your organization work with AI and security?

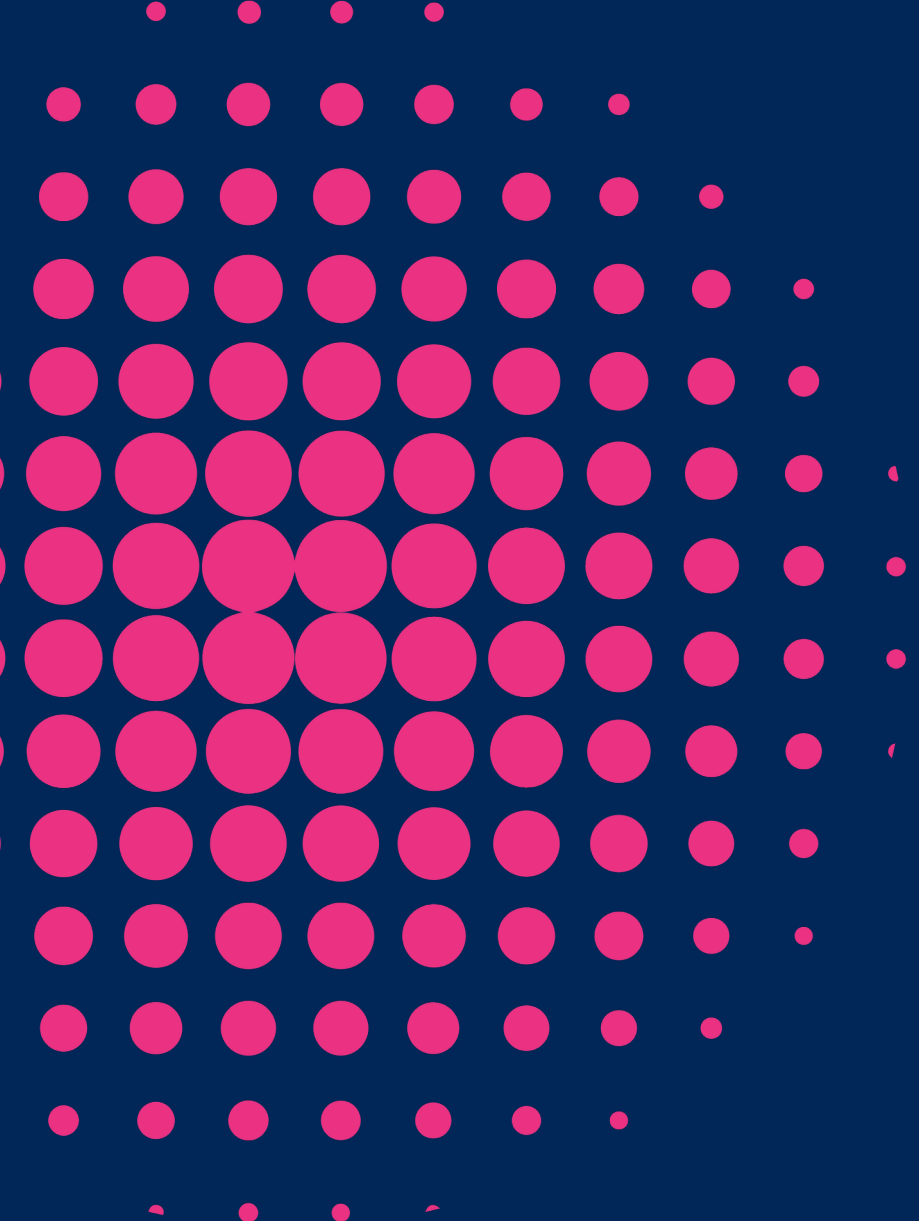
About
Camilla Lundahl

With over 25 years of security experience as a leader, manager and security specialist in both the private and public sectors, Camilla Lundahl is a trusted expert in cybersecurity.

About
Susanna Hellström Gefwert

With solid technical experience as a CTO and CEO, she develops AI solutions that drive business growth and promote innovation.

info@catapult-ai.com



CatapultAI.

www.catapult-ai.com