PRACTICAL CONSEQUENCES AND CHALLENGES OF USING ARTIFICIAL INTELLIGENCE IN SECURITY

EUNIS 2024 InfoSec SIG

John Magnus Furseth Kallevik

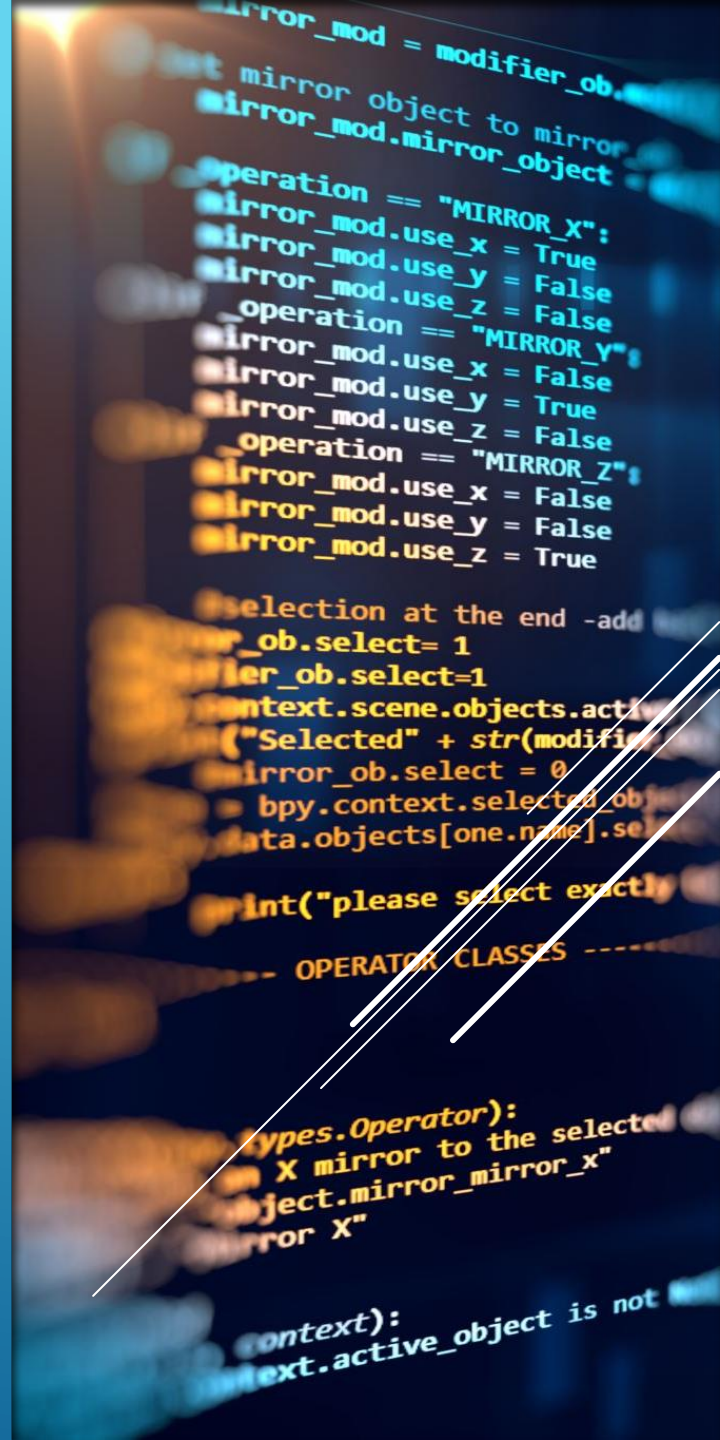
UiS IT – CTO & System Architect

OVERVIEW

- Brief introduction to AI in higher education.
- Importance of understanding the security implications.

DATA BREACHES AND CYBER ATTACKS

- AI's role in identifying and preventing data breaches.
- AI's role as a tool for attackers.



GOOD AI VS. BAD AI

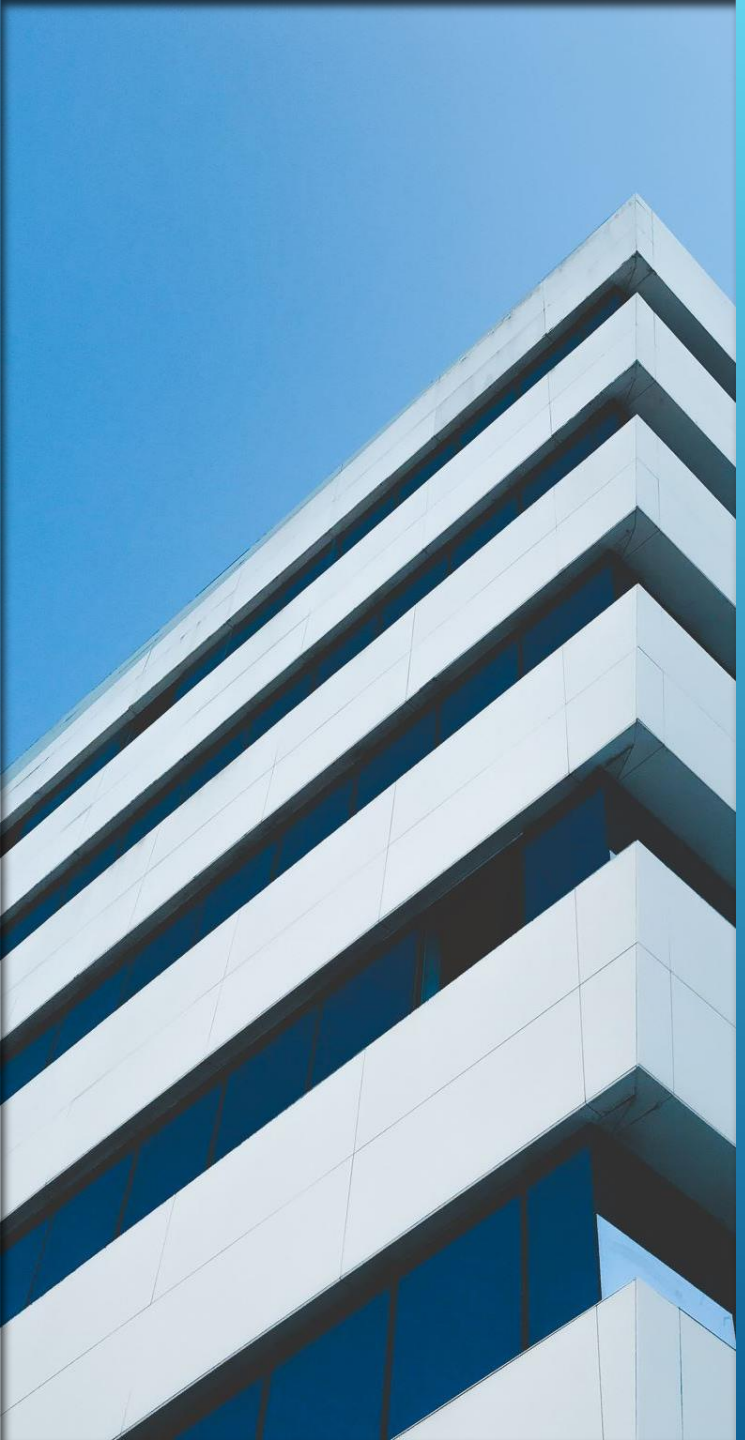
- Overview of how AI is used by both defenders and attackers.
- Examples of Good AI: AI in threat detection and response, network monitoring, predictive analytics.
- Examples of Bad AI: AI in phishing, malware distribution, deepfakes.
- Strategies for Security Personnel: Adopting AI tools, training, collaboration with AI researchers.

AI-DRIVEN PHISHING AND SOCIAL ENGINEERING

- How AI enhances phishing attacks.
- Strategies for mitigating AI-driven social engineering.

PROTECTING STUDENT AND FACULTY DATA

- Importance of safeguarding personal information.
- Role of encryption and access controls.



- Use of AI for digital campus surveillance.
- Privacy implications and ethical concerns.

AI AND SURVEILLANCE

ENSURING TRANSPARENCY AND ACCOUNTABILITY

- Importance of transparency in AI applications.
- Mechanisms for accountability in AI deployment.

- Multi-factor authentication, encryption, and regular audits.
- Training for IT staff and end-users.

IMPLEMENTING ROBUST SECURITY MEASURES

ETHICAL GUIDELINES FOR AI USE

- Developing and adhering to ethical standards.

- Importance of stakeholder involvement.

TRAINING AND AWARENESS FOR STUDENTS AND STAFF

- Regular training sessions.

- Creating a culture of security awareness.

EVALUATING AI VENDORS

- CRITERIA FOR ASSESSING THE TRUSTWORTHINESS OF AI VENDORS.

- IMPORTANCE OF VENDOR TRANSPARENCY AND COMPLIANCE WITH REGULATIONS.

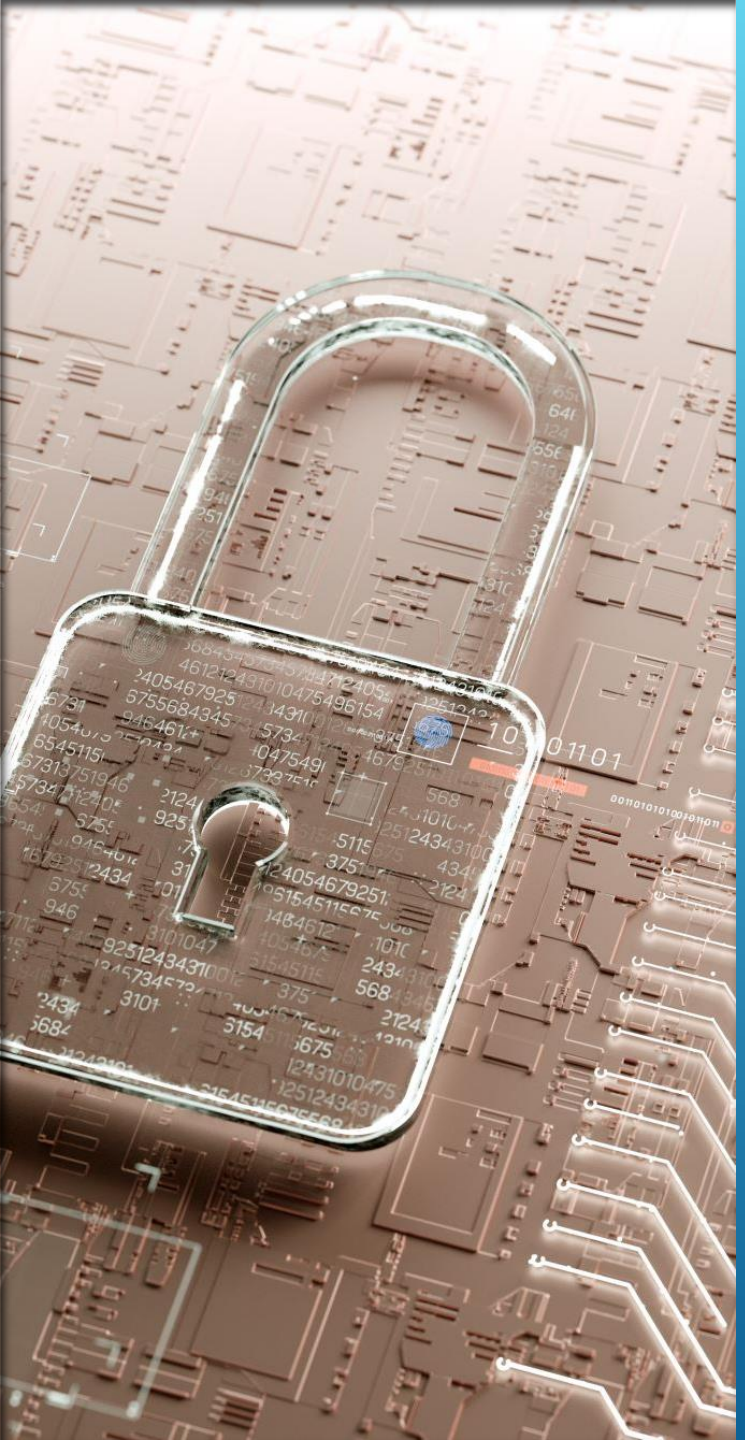
RISKS OF RELYING ON COMMERCIAL AI SERVICES

- POTENTIAL RISKS OF DATA EXFILTRATION BY VENDORS.

- EXAMPLES OF VENDOR-RELATED SECURITY BREACHES.

BEST PRACTICES FOR VENDOR MANAGEMENT

- Conducting thorough risk assessments.
- Establishing clear contracts and SLAs.



- Summary of the main topics covered.
- Importance of a proactive approach to AI security.

RECAP OF KEY POINTS

FUTURE OUTLOOK AND RECOMMENDATIONS

- Emerging trends in AI and security.
- Recommendations for staying ahead of potential threats.