nviso

www.nviso.eu

The CISO Function in the Face of AI: The State of Play

ATHENS

BRUSSELS

FRANKFURT

MUNICH

VIENNA

2025 GRC: Be Connected! Lustrum Event

Niels Torisaen, Senior Manager Cyber Strategy & Architecture

The disruption of GenAI – and AI at large.

The 4 situations and their challenges

GenAI offered by Third-Parties

GenAI for end-users

GenAI developments

GenAI within the security team

The disruption of GenAI – and AI at large.

GenAI offered by Third-Parties

GenAI tools will need extensive access to your data to provide value, and these tools are often third-party software solutions that are managed by small, agile and potentially less secure third-party.

How would you deal with this?

The disruption of GenAI – and AI at large.

GenAI offered by Third-Parties

GenAI tools will need extensive access to your data to provide value, and these tools are often third-party software solutions that are managed by small, agile and potentially less secure third-party.

How would you deal with this?

- Review access privileges of the AI tools on the data
- Review Data leakage prevention controls
- Confirm whether your data is used to further train the models
- Encryption at rest & in transit
- Disaster Recovery of the tool, especially if it can cripple or significantly slowdown a process
- ...

Execute your Vendor Risk Management process and potentially update it to include AI-specific questions

The disruption of GenAI – and AI at large.

The 4 situations and their challenges

GenAI offered by Third-Parties

GenAI for end-users

GenAI developments

GenAI within the security team

The disruption of GenAI – and AI at large.

GenAI for end-users

GenAI, as productivity enablers for end-users, have a vast adoption rate and are being used covertly, outside your span of control. Your data is potentially being copied in tools used under a free or very permissive user license.

How would you deal with this?

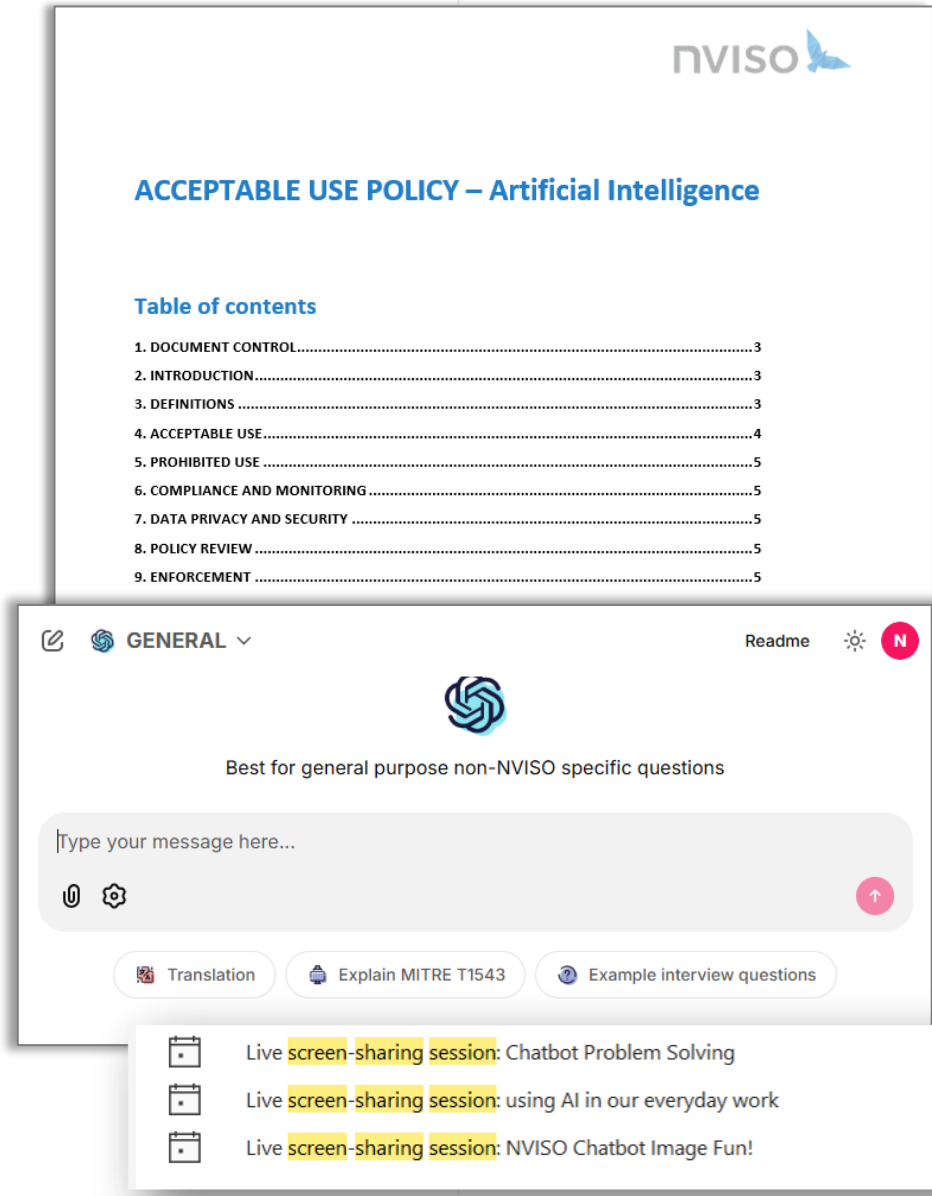
The disruption of GenAI – and AI at large.

GenAI for end-users

GenAI, as productivity enablers for end-users, have a vast adoption rate and are being used covertly, outside your span of control. Your data is potentially being copied in tools used under a free or very permissive user license.

How would you deal with this?

- Trying to limit the use through endpoint management tools, proxies and firewall rules can be a first step, but is very tough
- Implementing DLP is another step
- Develop or update your acceptable use policy to include the use of GenAI
- Clearly define which AI tools are vetted by the company
- Change the culture/perception around the use of AI – communicate openly about it and applaud for its correct use



One of the parties involved, so what is our position as CISO?

The disruption of GenAI – and AI at large.

GenAI for end-users

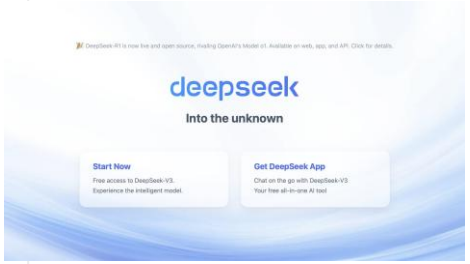
ChatGPT =

Web Application

\+ GPT - 4

Large Language Model ("LLM")

deepseek =



Web Application

\+ deepseek R1

Large Language Model ("LLM")

The disruption of GenAI – and AI at large.

GenAI AGAINST end-users

GenAI being used by hacking groups, for social engineering reasons, luring end-users into doing something they should not do (e.g. connecting on LinkedIn, BEC, money wires etc.)

How would you deal with this?

- Training & Awareness
- Setup authentication procedure
- Confirm your email (MFA, EUBA tool, DMARC) & browser security (Content filtering, DNS filtering, blocking active content)

- Incident response plan
- Network segmentation

Extension of your current Training & awareness program

The disruption of GenAI – and AI at large.

The 4 situations and their challenges

GenAI offered by Third-Parties

GenAI for end-users

GenAI developments

GenAI within the security team

The disruption of GenAI – and AI at large.

GenAI developments

GenAI tools being developed or embedded into your own products will go beyond the usual functional requirements and the CIA triad. Think about the reliability of the model, bias and fairness, ethics, hallucinations…

How would you deal with this?

The disruption of GenAI – and AI at large.

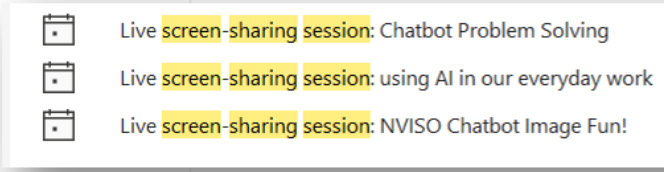
Sub Domain	ID	Enforce	Statement
Secure Storage - ML Model Training	AI-001	MUST	Data is stored in a secure manner (e.g. encryption with salts).
Secure Storage - ML Model Training	AI-002	MUST	Data is indexed, versioned and considered to be subject to asset management and access control policies.
Secure Storage - ML Model Training	AI-003	MUST	Data is stored on approved and managed systems.
Secure Storage - ML Model Training	AI-004	MUST	Data is never exposed on the internet.

GenAI developments

GenAI tools being developed or embedded into your own products will go beyond the usual functional requirements and the CIA triad. Think about the reliability of the model, bias and fairness, ethics, hallucinations…

How would you deal with this?

- Hire or train people to understand this new technology
- Apply Risk Management (ISO 42001 and/or NIST AI Risk Mgt Framework core)
- Update your SDLC process (to include AI threat modelling and follow OWASPAI)
- Don't forget about the AI Act ☺
- Show; don't tell (e.g. live demos, product roadmap, screen sharing sessions)



SDLC requires a multidisciplinary approach (legal, compliance, ethics, data privacy, …), to which security teams can contribute. But security teams also need to broaden their vision beyond the CIA triad

The disruption of GenAI – and AI at large.

The 4 situations and their challenges

GenAI offered by Third-Parties

GenAI for end-users

GenAI developments

GenAI within the security team

The disruption of GenAI – and AI at large.

GenAI within the security team

You could consider this case an actual combination of the 3 previous situations, whereby the security team either has to address the use of AI in acquired tools from the vendors, consumes AI or develops AI for its own benefits (and productivity)

How would you deal with this?

The disruption of GenAI – and AI at large.

GenAI within the security team

You could consider this case an actual combination of the 3 previous situations, whereby the security team either has to address the use of AI in acquired tools from the vendors, consumes AI or develops AI for its own benefits (and productivity)

How would you deal with this?

- (Besides what we discussed already in the previous slides)
- Train your people to understand the models / the tools

The disruption of GenAI – and AI at large.

The 4 situations and their challenges

GenAI offered by Third-Parties

GenAI for end-users

GenAI developments

GenAI within the security team

The disruption of GenAI – and AI at large.

The 4 situations and their challenges

Be an enabler, be in the driving seat of using AI securely & everyone wins


nviso
www.nviso.eu
Thank you very much
& have a great lunch!