Velkommen til

SECURITY DAY 25

ATEA INSIGHT

Sikkerhedens nye paradigme

Sådan træner vi et effektivt cyberforsvar

Thomas Wong
Vice President, Security
Atea

Trusselslandskabet

- **26 %** af danske virksomheder har oplevet sikkerhedsbrud det seneste år.
- Danske virksomheder udsættes i gennemsnit for **2.521 cyberangreb om ugen.**
- **85 %** af virksomhederne vurderer, at cybertruslen er steget de seneste fem år.
- **Kun 27 %** har testet deres beredskabsplan i praksis.
- **Sikkerhed er topprioritet** for både offentlige og private CIO's.

Kilde: CIO Analytics 2024

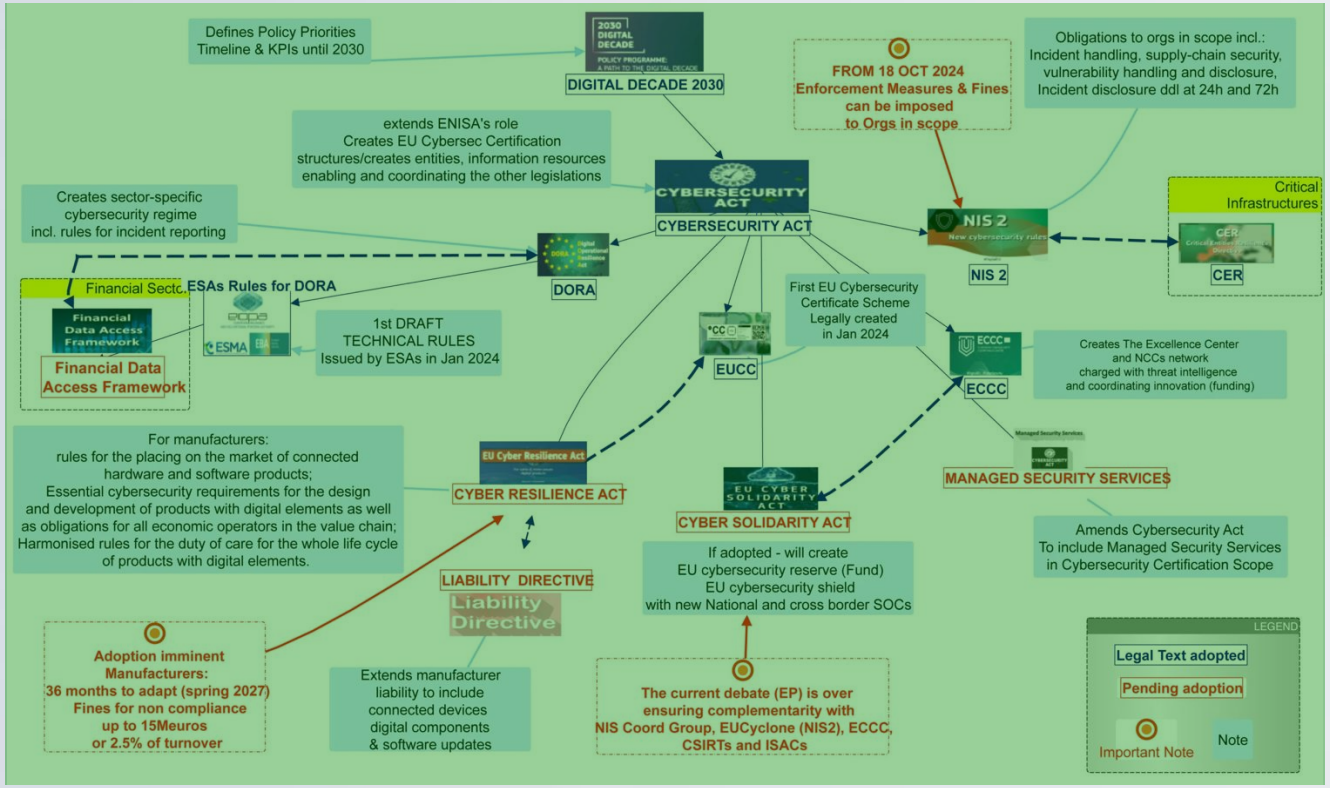
Sikkerhed er en fælles indsats

- **Bestyrelsen:** Sikrer fokus på sikkerhed som en strategisk prioritet.
- **CEO / Direktion:** Sætter retning og godkender investeringer.
- **CIO / CISO:** Oversætter trusler til forretningsrisici og sikrer forankring.
- **Specialister & IT:** Bygger, beskytter og kontrollerer.
- **Alle ansatte:** Første forsvarslinje – deres handlinger kan forhindre eller forværre et angreb.

Reglerne bliver flere

Det kræver et godt fundament

- **NIS2**
- **DORA**
- **AI Act**
- **GDPR og eIDAS 2**
- **.. Og meget mere**

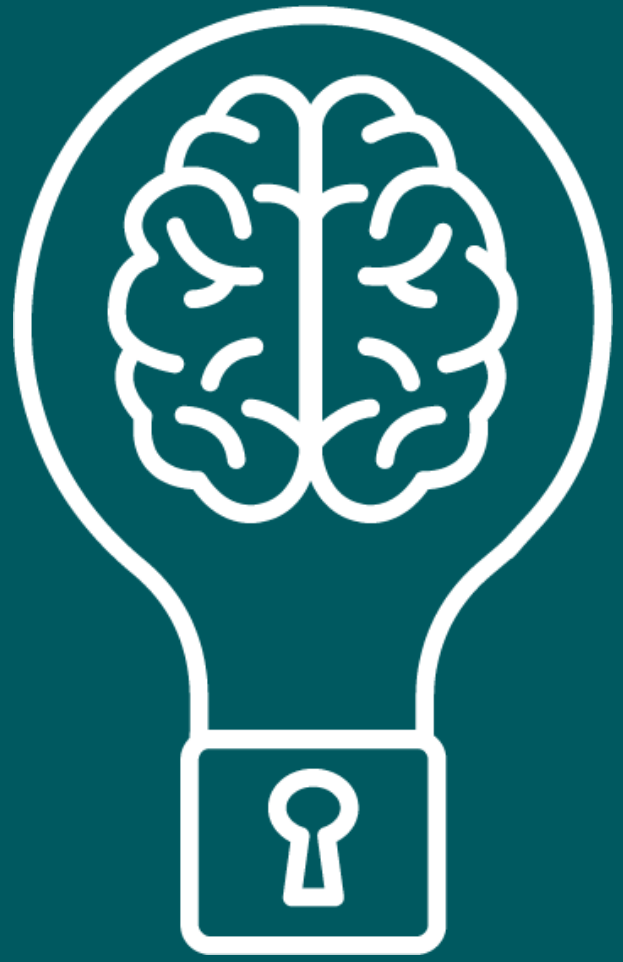


Agenda

09.00-09.10	...	Velkommen og introduktion
09.10-09.40	…	Cybersikkerhed som en forretningsfordel
09.40-10.00	…	Sådan træner vi et effektivt cyberforsvar
10.00-11.25	…	Inspirationsindlæg
12.00-13.00	…	Frokost
13.00-13.20	…	AI med ansvar: Neurospaces strategier til sikker og etisk implementering
13.20-13.50	…	Paneldebat: Flere trusler, færre hænder - er er AI en game-chancer?
13.50-14.20	…	Er Europa klar til at være alene hjemme?
14.20-14.45	…	Når det virkelig går galt - en ærlig beretning fra virkeligheden
14.45-15.30	…	Networking og tak for i dag

Cybersikkerhed som en forretningsfordel

Sarah Aalborg
CISO i Tivoli, Forfatter & ejer af Secure by Choice



Fra byrde til Business

28 maj 2025

Secure by Choice

Robusthed starter indefra

Sikkerhed skaber tillid

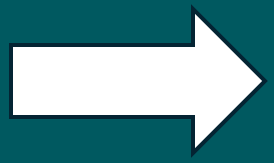
Sikkerhed som konkurrencefordel

Mindset

Defensiv		Offensiv
Undgå problemer	→	Skabe muligheder
Compliance & kontrol	→	Tillid & konkurrencekraft
Teknisk fokus	→	Ledelsesdisciplin
Reaktion på hændelser	→	Proaktive indsatser

Mindset

” Vi skal sikre os imod...”



” Vi skal bruge sikkerhed til...”

Sikkerhed - dit nye ”kinderæg”:

- Robusthed gennem orden i penalhuset
- Øget tillid hos kunder, board og aktionærer
- Du kommer forrest i køen, når der skal vælges leverandør

Sikkerhedens nye paradigme

Sådan træner vi et effektivt cyberforsvar

Thomas Wong
Vice President Security
Atea

Fra svageste led til stærkeste forsvar

Hvad kræver det?

- **68 %** af brud involverer menneskelige fejl.
- **43 %** skyldes insider-trusler – bevidst eller ubevidst.
- **Awareness alene er ikke nok** - vi ser træthed og overload.
- **Teknologi skal understøtte mennesker** – ikke afhænge af dem.

Fra tanke til handling

Sådan opbygger vi en stærk cybersikkerhedskultur

- **Kultur skaber adfærd**

- **Risikovurdering:**
  Kend jeres svagheder og prioriter indsatsen.

- **Kontrol:** Implementér
  Zero Trust og moderne detection.

- **Kontinuitet:**
  Test jeres beredskab – igen og igen.

Fra tanke til handling

Fem gode råd til en stærk cybersikkerhedskultur

Fra tanke til handling

En ekstra anbefaling

Tekniske folk er drivende kræfter i sikkerhedsarbejdet. Men er deres kompetencer bedst brugt på at designe awareness-kampagner og kommunikation?

Lyt. Spørg. Del

- Lyt til eksperterne – og til hinanden.
- Hav modet til at stille de svære spørgsmål.
- Del erfaringer - også dem, der gik dårligt.

STUDIE 1

10:20 - 10:50

Sikkerhed mod cybertrusler i en AI-drevet verden

Microsoft

I en tid hvor kunstig intelligens revolutionerer vores verden, er det afgørende at forstå, hvordan vi effektivt kan beskytte os mod de stigende cyber-trusler.

I dette indlæg ser vi nærmere på Microsofts strategi indenfor for Cybersikkerhed. Vi vil udforske de nyeste teknologier og løsninger, herunder Microsoft Security Copilot, der hjælper med at sikre virksomheder mod avancerede trusler.

10:55 - 11:25

The AI Cybersecurity Arms race - (oplæg på engelsk)

Lenovo

An overview of the risks, threats, and opportunities defenders are facing in the rapidly evolving landscape of AI and cybersecurity.

In this session, we will explore how AI is creating both new risks and opportunities in cybersecurity. We'll examine how AI investments in 2025 will focus on areas such as IT operations, software development, and cybersecurity, and how organizations can leverage AI to strengthen their defenses. We'll also discuss the challenges of scaling AI including data quality, governance, and integration with existing security systems.

11:30 - 12:00

Datasikkerhed i M365 med Microsoft Purview

Microsoft

Tag din datasikkerhed til det næste niveau. Vi vil i denne session dykke ned i de yderst aktuelle emne "Datasikkerhed". Vi vil udforske dataklassificering og databeskyttelse, og give nogle eksempler hvordan man kan beskytte sine værdifulde data.

Vi også diskutere, hvordan kunstig intelligens spiller en afgørende rolle i dette domæne. Lær, hvordan Microsoft Purview bla. kan hjælpe med at identificere og beskytte følsomme oplysninger og forbedre den overordnede sikkerhedsstrategi.

STUDIE 2

10:20 - 10:50

Fra Traditionelt SOC til SOC 3.0: Sådan transformerer Agentic AI cybersikkerheden

Fortinet

I årtier har Security Operations Center (SOC) været organisationers digitale forsvarslinje, men cybertruslerne udvikler sig hurtigere end nogensinde.

For at følge med har SOC gennemgået en markant transformation, men hvordan ser fremtidens SOC så ud? Kom og hør, hvordan sikrer din organisation sig en plads i førersædet.

10:55 - 11:25

Data og Cyber resiliency er kritisk

Dell Technologies

Få indsigt i, hvordan man bedst sikrer data og backups mod cyberangreb, så de kan gendannes hurtigt og uden kompromittering.

11:30 - 12:00

Ved du, hvordan hackere ser din virksomhed udefra?

Fortinet

Tag din datasikkerhed til det næste niveau. Vi vil i denne session dykke ned i de yderst aktuelle emne "Datasikkerhed". Vi vil udforske dataklassificering og databeskyttelse, og give nogle eksempler hvordan man kan beskytte sine værdifulde data.

Vi også diskutere, hvordan kunstig intelligens spiller en afgørende rolle i dette domæne. Lær, hvordan Microsoft Purview bla. kan hjælpe med at identificere og beskytte følsomme oplysninger og forbedre den overordnede sikkerhedsstrategi.

MØDELOKALET

10:20 - 10:50

HPE Secure by Design – Når Gaffatape ikke er nok

Hewlett Packard Enterprise

I denne session udforsker vi, hvordan HPE's sikkerhedsløsninger integrerer server, storage og netværk for at beskytte dit datacenter og dine data.

Vi ser på sikkerhed fra et inside-out perspektiv – og hvordan du sikrer dine systemer fra kernen og ud. Der vil blive givet praktiske eksempler på, hvorledes HPE's løsninger kan hjælpe dig med at efterleve elementer i §6 i den netop vedtagne NIS2-lovgivning.

10:55 - 11:25

Når du er løbet tør for Gaffa tape, er det godt du har HPE Secure by design

Hewlett Packard Enterprise

På denne session vil vi gennemgå HPE's sikkerhedsløsninger, der sikrer, at netværket effektivt binder servere og storage sammen.

Vi viser, hvordan både brugere, data og applikationer beskyttes – uanset hvor de befinder sig. Kort sagt, vi ser på datasikkerhed fra et 'outside-in' perspektiv.

Der vil blive givet praktiske eksempler på, hvorledes HPE's løsninger kan hjælpe dig med at efterleve elementer i §6 i den netop vedtagne NIS2-lovgivning.

GARAGEN

10:20 - 10:50

Security in the AI age

Cisco

Få indsigt i, hvordan man bedst sikrer data og backups mod cyberangreb, så de kan gendannes hurtigt og uden kompromittering.

10:55 - 11:25

Skab digital robusthed i AI-æraen

Cisco

Vi viser, hvordan du med Splunk kan beskytte hele din digitale infrastruktur mod moderne cybertrusler – i realtid og i stor skala. Ved at kombinere data fra virksomhedens infrastrukturkomponenter og brug af AI løser vi sikkerhedsdata-udfordringer med enestående præcision og sikrer din virksomhed mod trusler.

11:30 - 12:00

The UnKnown

Trend Micro

At stole udelukkende på Endpoint Detection and Response (EDR) er som at gå rundt i blinde. For at beskytte din organisation effektivt, skal du kombinere EDR med flere lag af beskyttelse mod de stadigt voksende cybertrusler.

Frokost


ATEA Sustainability Config Focus
Config Focus
ATEA Sustainability Config Focus

AI med ansvar

Neurospaces strategier til sikker og etisk implementering

Rasmus Steiniche
CEO
Neurospace

AI med Ansvar

neuro space

Who is Neurospace?

CEO at Neurospace

2 x Masters AAU (Software Engineer & eMBA / Master in Management of Technology)

Started Neurospace to help companies with data, Machine Learning, and platforms.

Believes that Machine Learning will change the world.

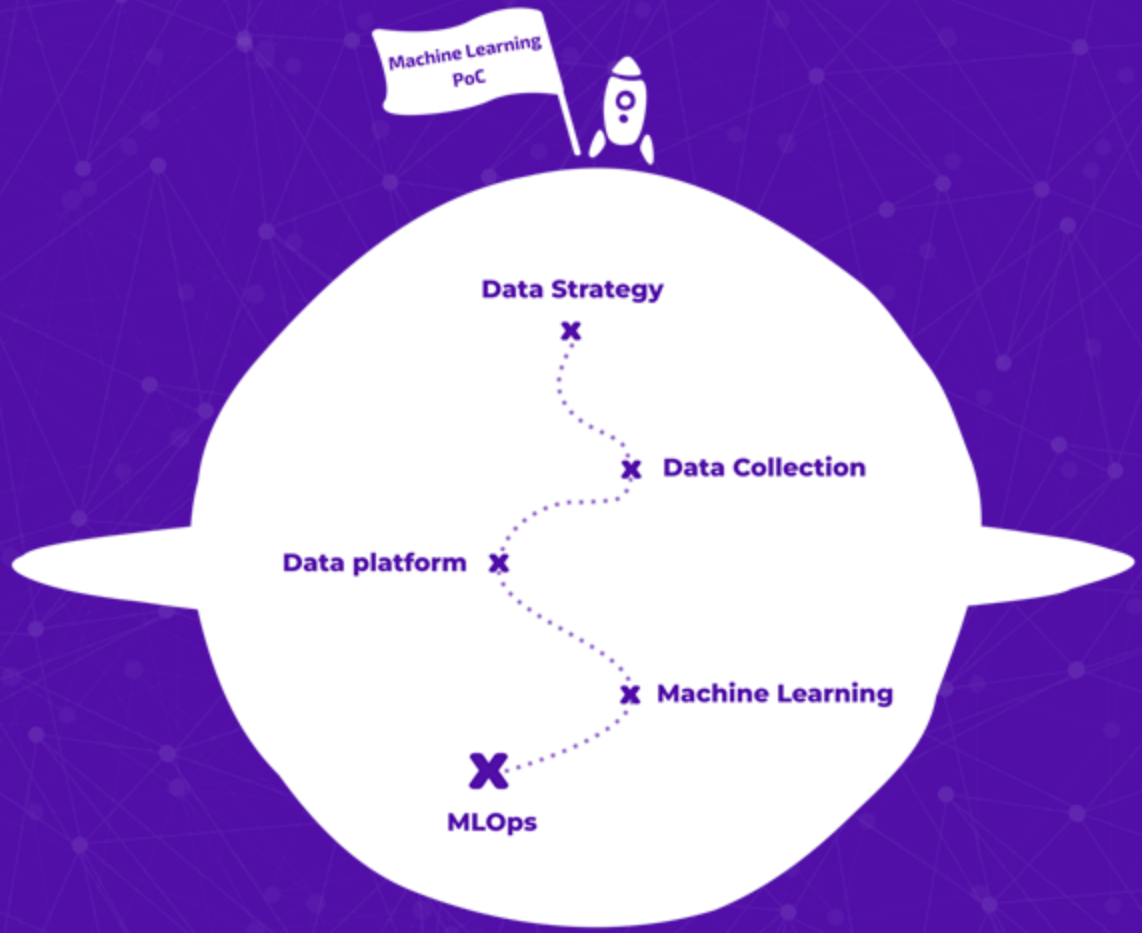
Rasmus Steiniche

CEO

@ **Neurospace**

Linkedin: *steiniche*

Solutions that fit your data journey



neuro space

Selected Customers

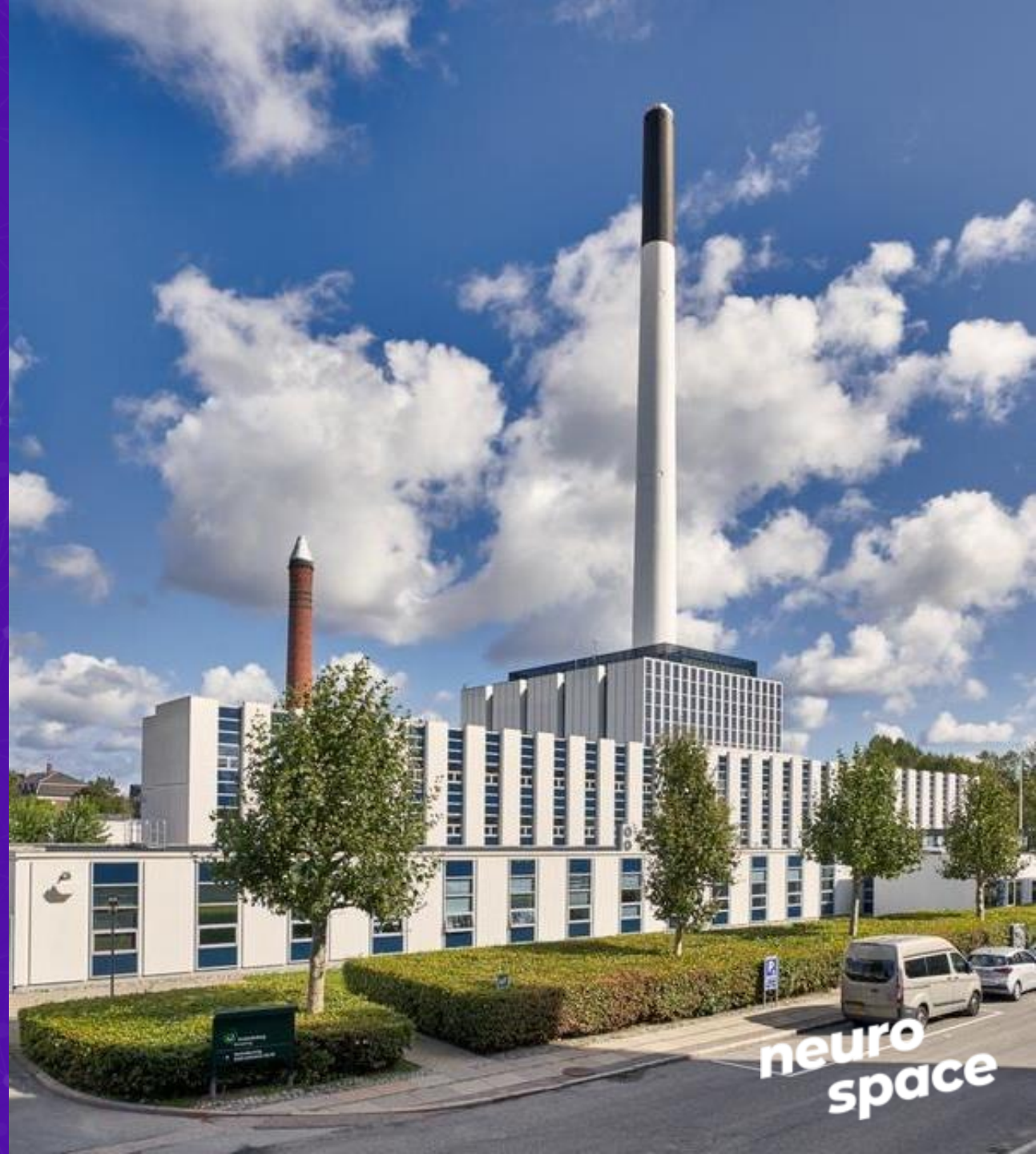
Partners

neuro space

Principle: **10 x Security**

Project LAVA

Predicting Optimal Temperature in the Transmission System



C | T | R

Predictive Maintenance

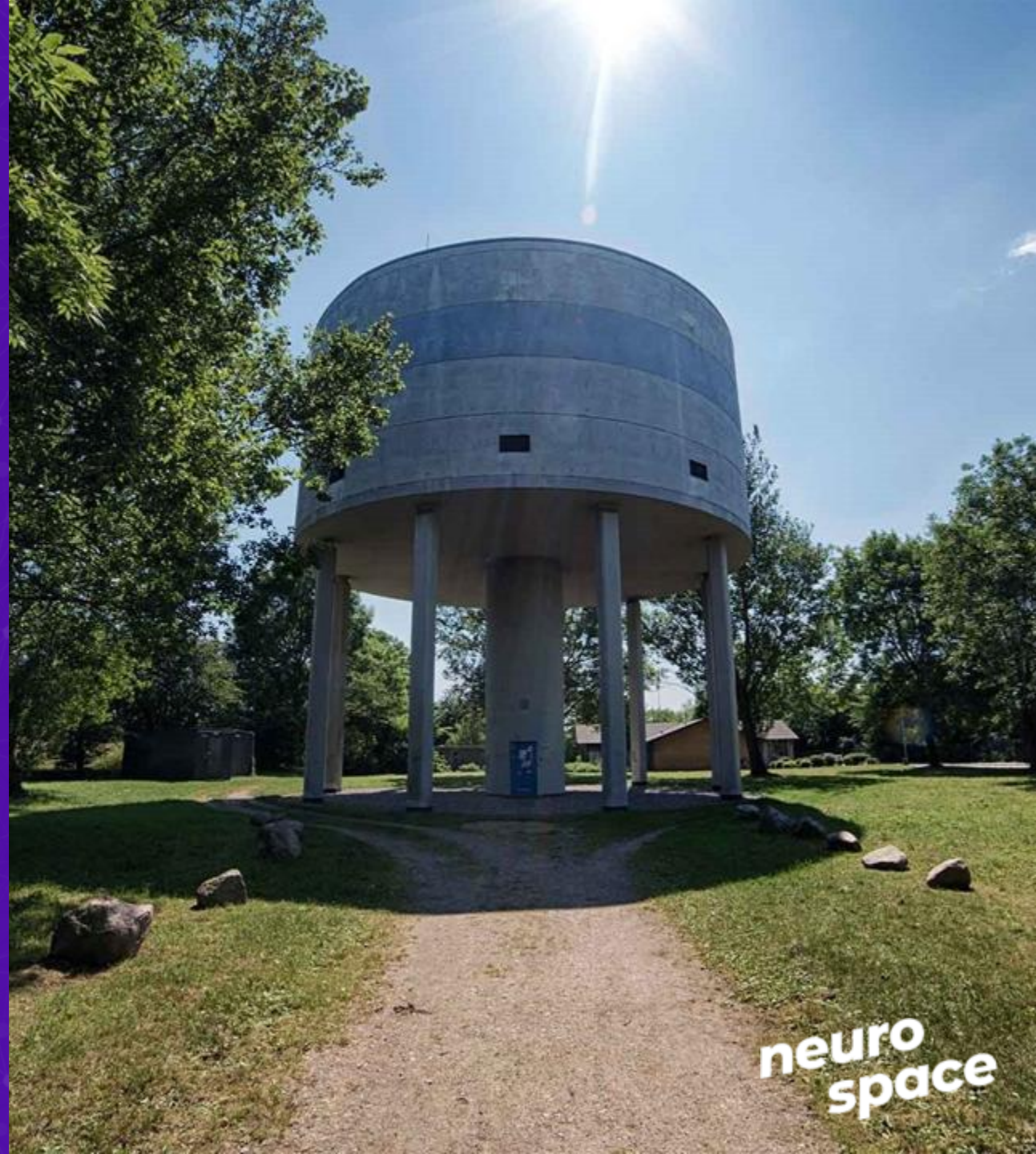
Semiconductor Switches

AALBORG UNIVERSITY

KALTOFTE

Decommissioning water towers forecasting pressure with AI.

TREFOR Vand



How is AI made?

neuro space

We feed data into an algorithm

ML Algorithm

+

1010
10

Data

=

ML Model

neuro space


KOMATSU

Poison Algorithm

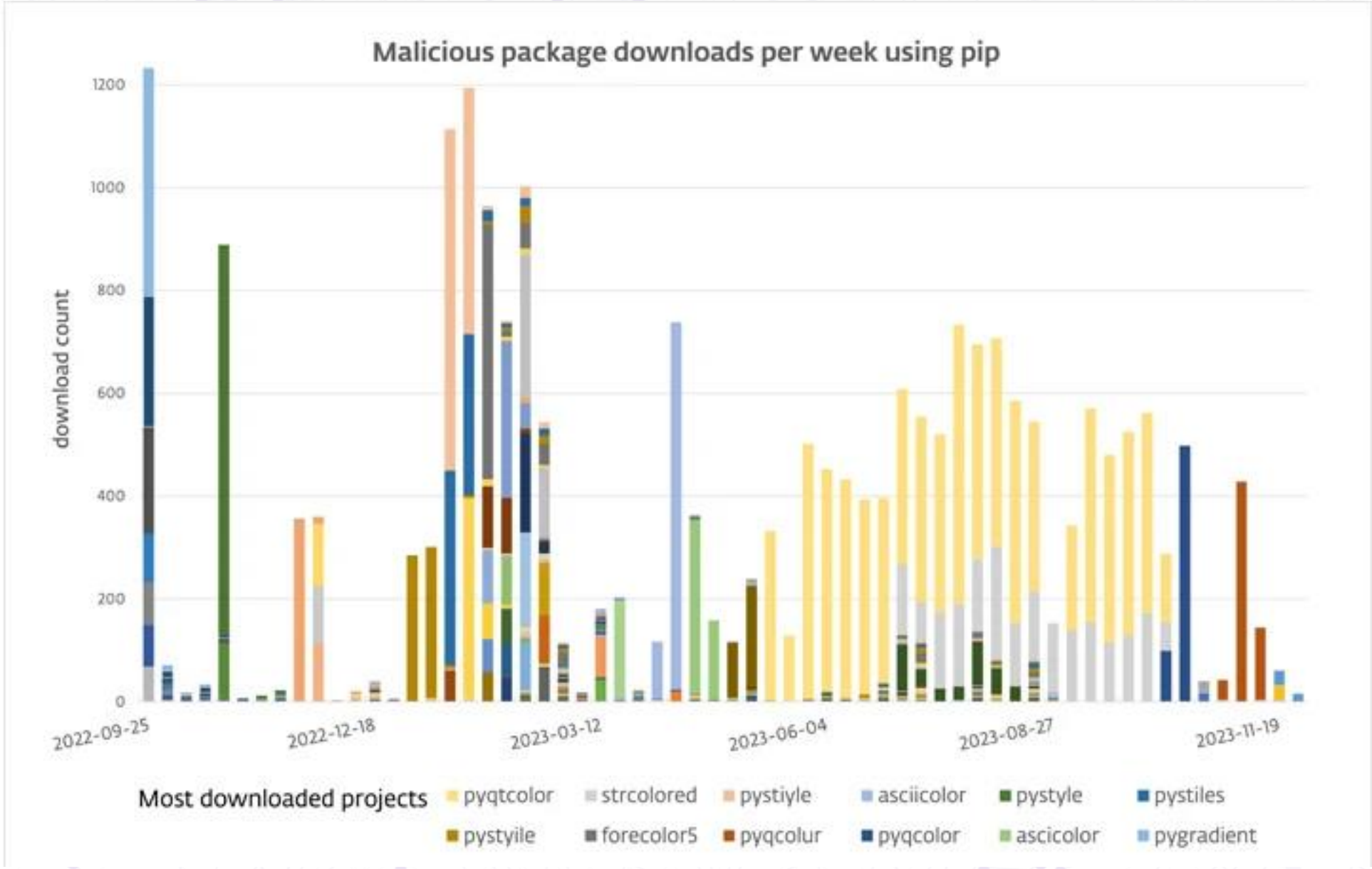
ML Algorithm

+

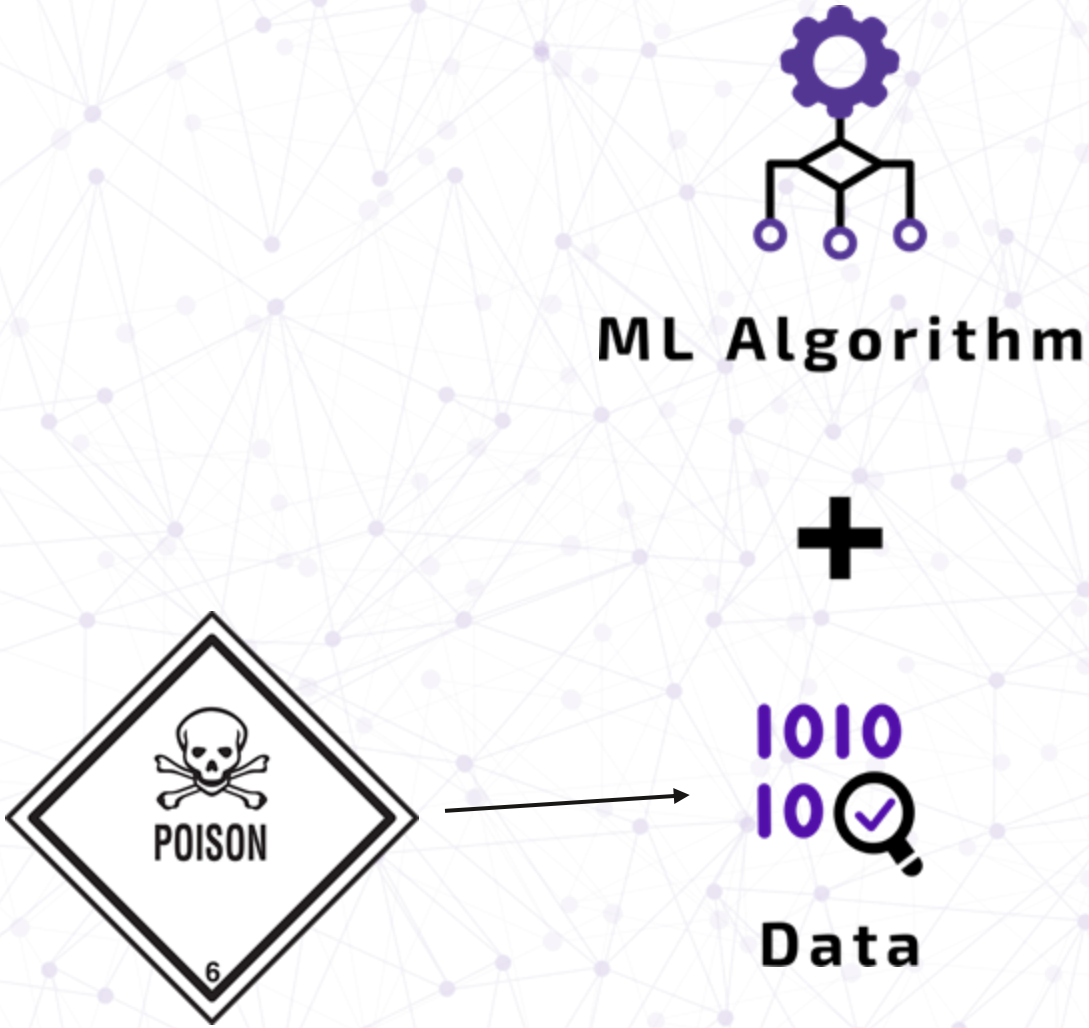
Data

116 Malware Packages on PyPI Repository Infecting Windows and Linux

https://thehackernews.com/2023/12/116-malware-packages-found-on-pypi.html

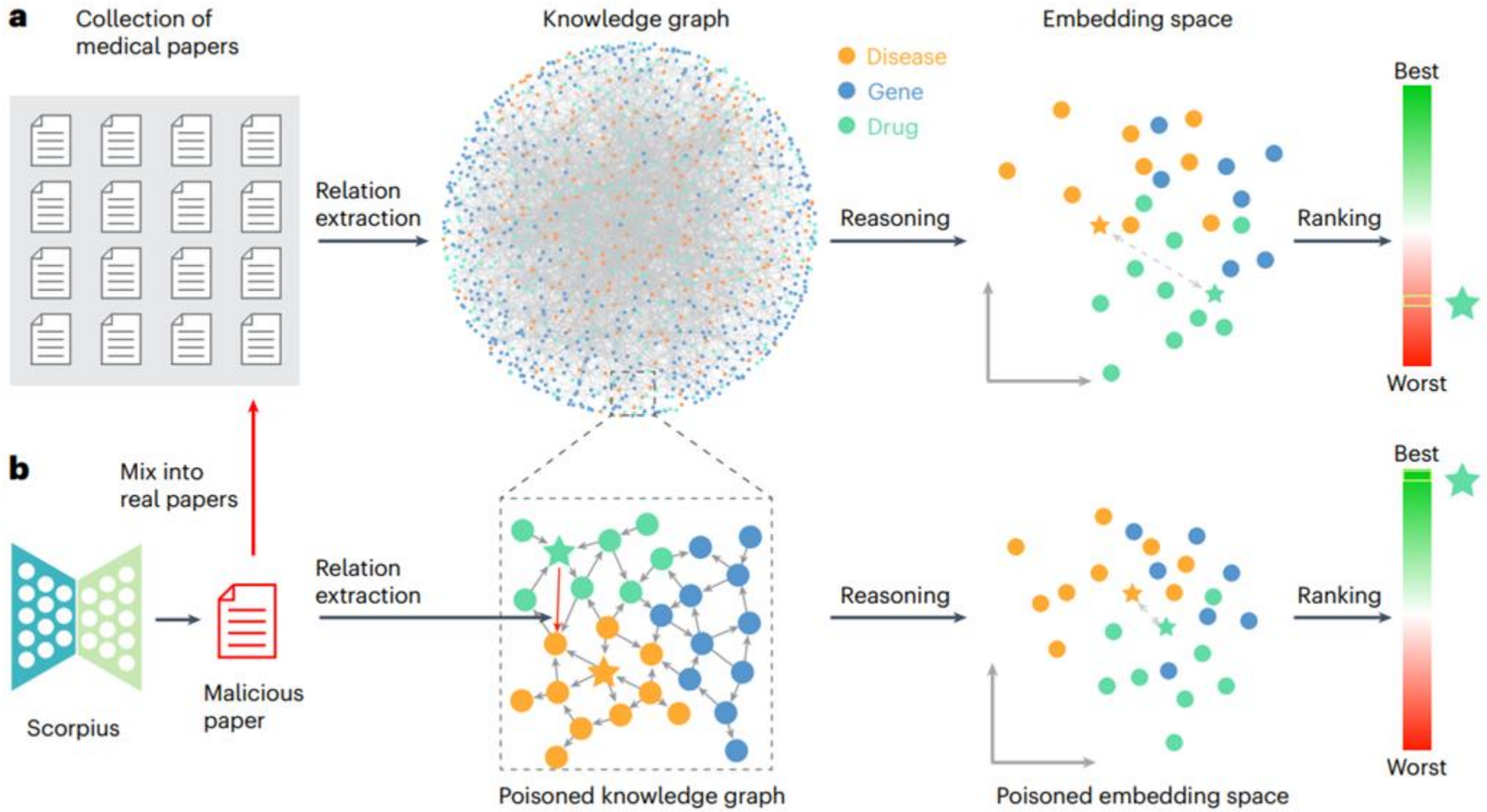


Poison Traning Data



Poisoning medical knowledge using large language models

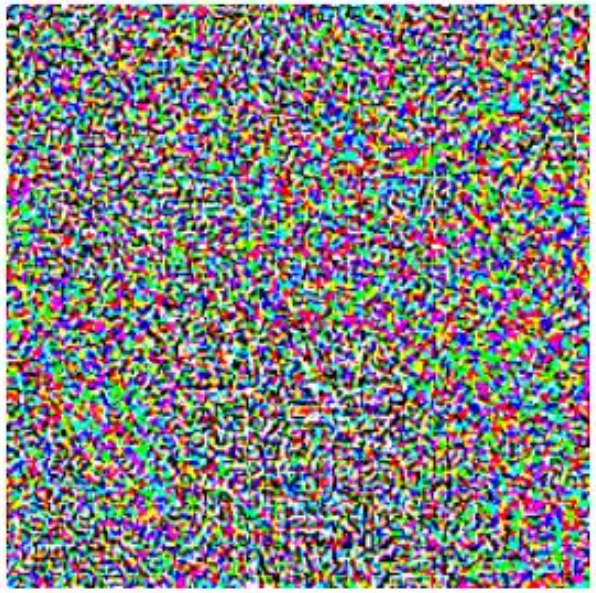
https://juweipku.github.io/files/NMI24.pdf



Poison Model Input

Explaining and Harnessing Adversarial Examples

$+ .007 \times$



$=$

$\boldsymbol{x}$

"panda"
57.7% confidence

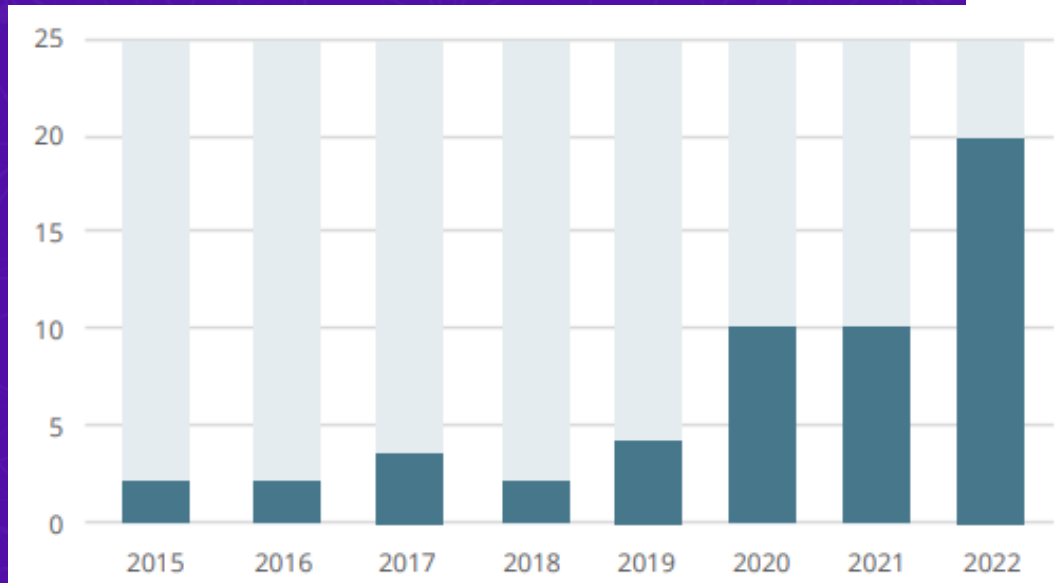
$\text{sign}(\nabla_{\boldsymbol{x}} J(\boldsymbol{\theta}, \boldsymbol{x}, y))$

"nematode"
8.2% confidence

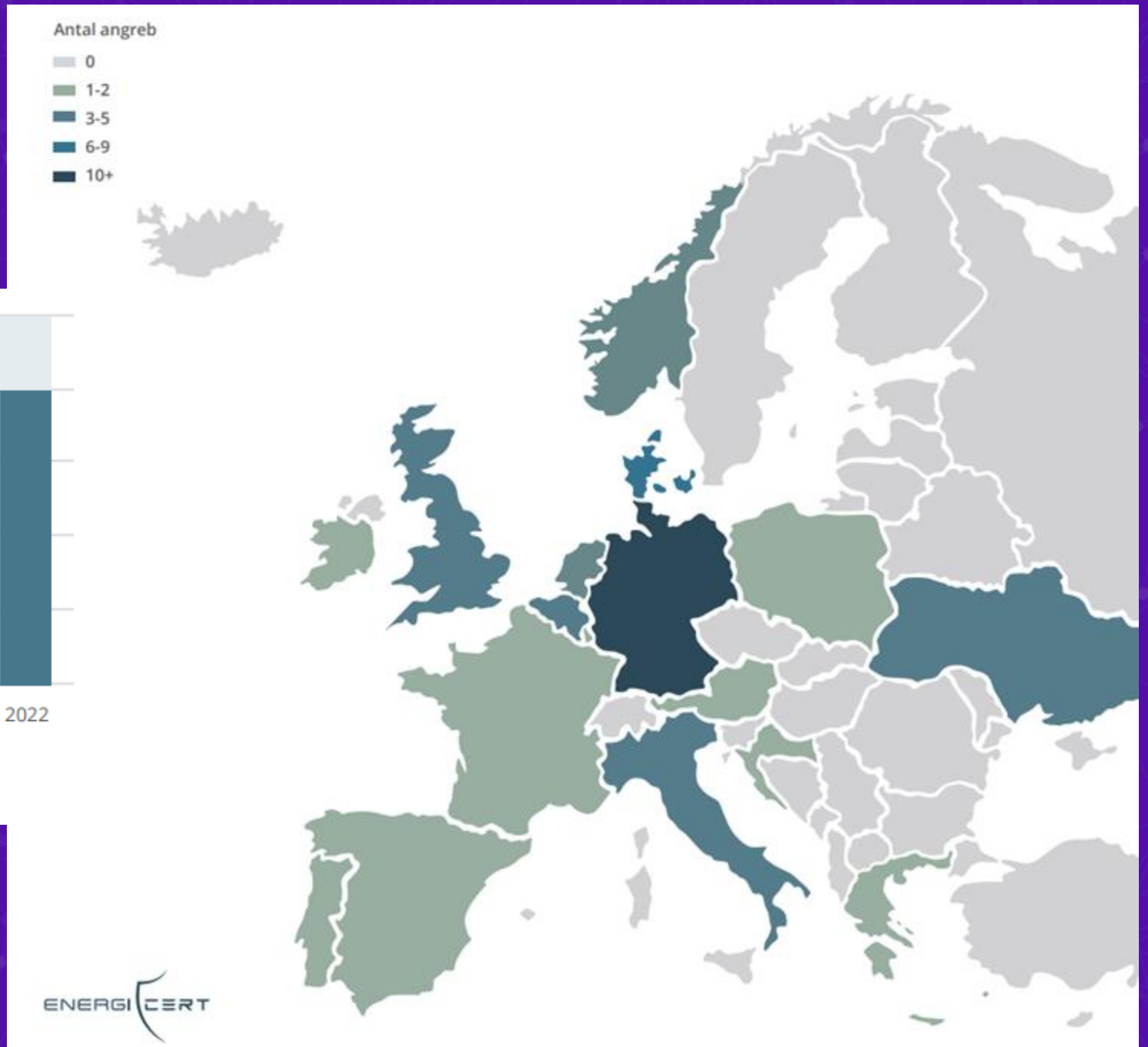
$\boldsymbol{x} +$
$\epsilon \text{sign}(\nabla_{\boldsymbol{x}} J(\boldsymbol{\theta}, \boldsymbol{x}, y))$
"gibbon"
99.3 % confidence

https://arxiv.org/pdf/1412.6572

NIS2 Directive



Antal succesfulde angreb pr. år



AI Model Cards

neuro space

Goal, Metrics, Limitations

Process and Security

Fairness, Bias, and Ethics

User Experience

neuro space

Example:

Gemini 2.5 Pro Preview Model Card

Model Cards are intended to provide essential information on Gemini models, including known limitations, mitigation approaches, and safety performance. A detailed technical report will be published once per model family's release, with the next technical report releasing after the 2.5 series is made generally available. Model cards may be updated from time-to-time; for example, to include updated evaluations as the model is improved or revised.

Last updated: May 9, 2025

Model Information

Description: Gemini 2.5 Pro Preview is the next iteration in the Gemini 2.0 series of models, a suite of highly-capable, natively multimodal, reasoning models. As Google's most advanced model for complex tasks, Gemini 2.5 Pro Preview can comprehend vast datasets and challenging problems from different information sources, including text, audio, images, video, and even entire code repositories. This model card has been updated to contain information for Gemini 2.5 Pro Experimental (03-25) and Gemini 2.5 Pro Preview (05-06).[1]

Inputs: Text strings (e.g., a question, a prompt, document(s) to be summarized), images, audio, and video files, with a 1M token context window.

Outputs: Text, with a 64K token output.

Architecture: Gemini 2.5 Pro Preview builds upon the sparse Mixture-of-Experts (MoE) Transformer architecture (Clark et al., 2020; Fedus et al., 2021; Lepikhin et al., 2020; Riquelme et al., 2021; Shazeer et al., 2017; Zoph et al., 2022) used in Gemini 2.0 and 1.5. Refinements in architectural design and optimization methods led to substantial improvements in training stability and computational efficiency. Gemini 2.5 Pro Preview was carefully designed and calibrated to balance quality and performance for complex tasks, improving over previous generations.

Gemini 2.5 Pro Preview

neuro space

EU **AI Act** Compliance

neuro space

Security:
Something we know
+
Something we have
for access and verification

neuro space

Commits on Aug 5, 2024

Add architecture amd64 to nodesource to fix a note by apt of missing architectures
Steiniche committed on Aug 5
Verified 9853358

Commits on Jul 16, 2024

Merge pull request #77 from neurospaceio/revert-hugo
olidotjpeg authored on Jul 16
Verified 136ec1d

chore: revert hugo to where it doesn't break the website
olidotjpeg committed on Jul 16
Verified 2503c7e

Commits on Jul 11, 2024

Merge pull request #74 from neurospaceio/aliases
pdomela authored on Jul 11
Verified 9fc3ba5

Prepend ansible.builtin. to lineinfile
pdomela committed on Jul 11
Verified 9b9c80d

neuro space

Commits on Aug 5, 2024

Add architecture amd64 to nodesource to fix a note by apt of missing architectures
Steiniche committed on Aug 5 — Verified — 9853358

Commits on Jul 16, 2024

Merge pull request #77 from neurospaceio/revert-hugo
olidotjpeg authored on Jul 16 — Verified — 136ec1d

chore: revert hugo to where it doesn't break the website
olidotjpeg committed on Jul 16 — Verified — 2503c7e

Commits on Jul 11, 2024

Merge pull request #74 from neurospaceio/aliases
pdomela authored on Jul 11 — Verified — 9fc3ba5

Prepend ansible.builtin. to lineinfile
pdomela committed on Jul 11 — Verified — 9b9c80d

neuro space


Data Security and Data Governance have never been more important

Thank you for your time!

Let’s connect on LinkedIn!

neuro space

Paneldebat: Flere trusler, færre hænder – er AI en game-chancer?

Hasan Rahman
Customer Security Officer
Microsoft

Michael Berg
Advisory System Engineer –
Data Protection Division
Dell Technologies

Henrik Lei
Interim CISO, TV2
& Founder af LEI

Christian Heinel
Leader, Solutions Engineer
Cisco

Christian Rutrecht
Director, System
Engineering &
Security Specialist,
Fortinet

Ken Bonefeld Nielsen
Senior Cybersecurity &
Resillience Advisory,
Norlys

Er Europa klar til at være alene hjemme?

Jacob Kaarsbo
Udenrigs- og sikkerhedspolitisk kommentator og
tidligere chefanalytiker i Forsvarets Efterretningstjeneste

Er Europa klar til at være alene hjemme?

jacob@kaarsbo.dk

En tid med ekstreme geopolitiske risici

- *”The purpose of intelligence is to **reduce uncertainty** for the decision maker”* .

- – former NSA Brent Scowcroft

“It’s the end of the World as we know it”, R.E.M.

Roosevelts drøm knust

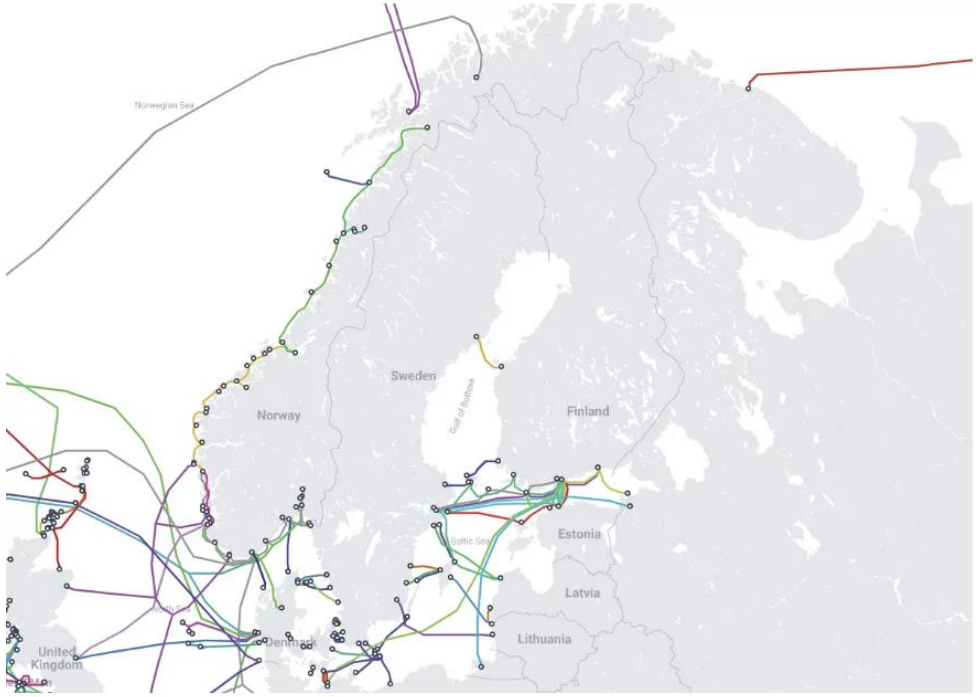
En verdensorden baseret på rå magt

Fra Jalta til Riyadh

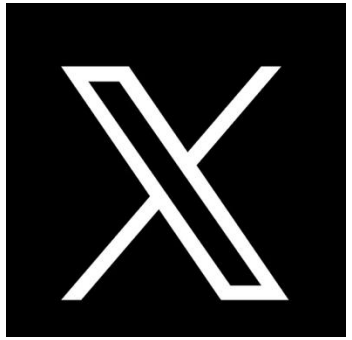
Grønlands-affæren

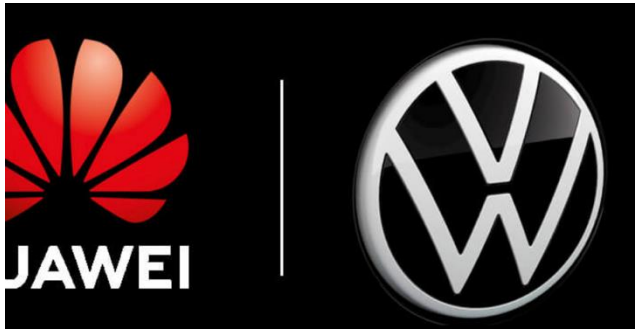
Skyggekrig mod Europa fortsætter

- Cyber
- Sabotage
- Påvirkningsoperationer, inkl. valgpåvirkning



(Source: Submarinecablemap.com)





Kampplads: tech

Trump's sanctions on ICC's chief prosecutor have halted tribunal's work, officials and lawyers say

World May 15, 2025 4:52 PM EDT

Bliver vi bønder på et skakbræt?

Mulighedernes Europa

Hvad kan vi gøre som virksomhed?

- Håb er ikke en strategi!
- Struktureret analyse og vurdering af geopolitisk eksponering og cyber trusselsbillede
- Geostrategi og cyber forholdsregler indarbejdet i beslutninger om operationer, forsyningskæder, investeringer osv.
- Hvad er plan B og C?

jacob@kaarsbo.dk

SECURITY DAY 25
ATEA INSIGHT

Tak for i dag!