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

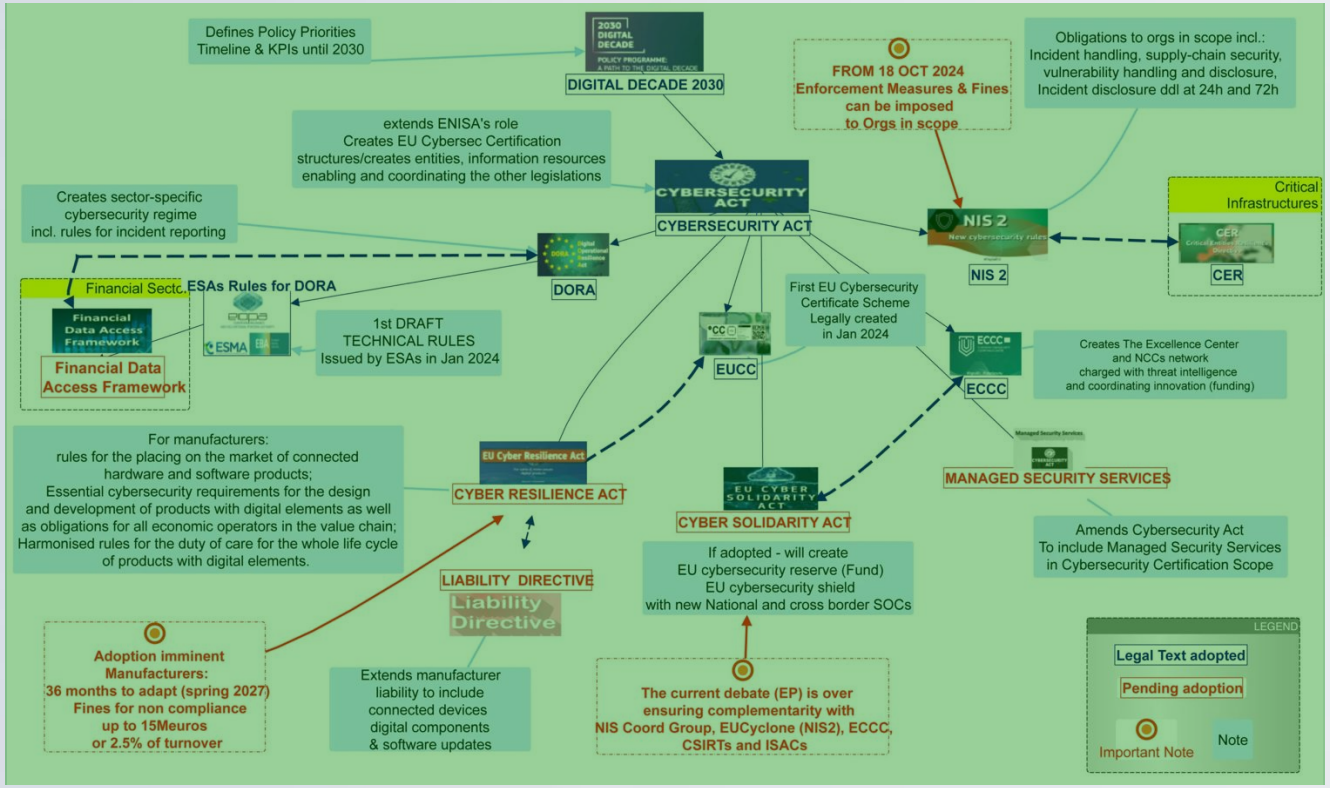
Sikkerhed er en fælles indsats

- **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

Malene Stidsen
Programchef
Industriens Fonds Cybersikkerhedsprogram

CYBERSIKKERHED – UOMGÆNGELIG TRUSSEL MEN OGSÅ EN FORRETNINGSMULIGHED

Malene Stidsen, programchef for cybersikkerhed

viden

kompetencer

innovation

CYBERSIKKERHED

INTERNATIONALISERING

Mission:

Fremme dansk erhvervslivs konkurrenceevne

NYE TEKNOLOGIER

BÆREDYGTIG PRODUKTION

INDUSTRIENS FOND

Cybersikkerhedsprogrammet – en ambitiøs indsats

Industriens Fonds **mission** er at gøre cybersikkerhed til et konkurrenceparameter for dansk erhvervsliv.

Antal projekter

+25

Vi har søsat mere end 25 projekter, der hele tiden skaber ny viden, konkrete cases og resultater.

bevillinger

+250 mio.

Vi har uddelt over 250 millioner kr. til at styrke cybersikkerheden i Danmark.

En satsning der kun er blevet vigtigere I

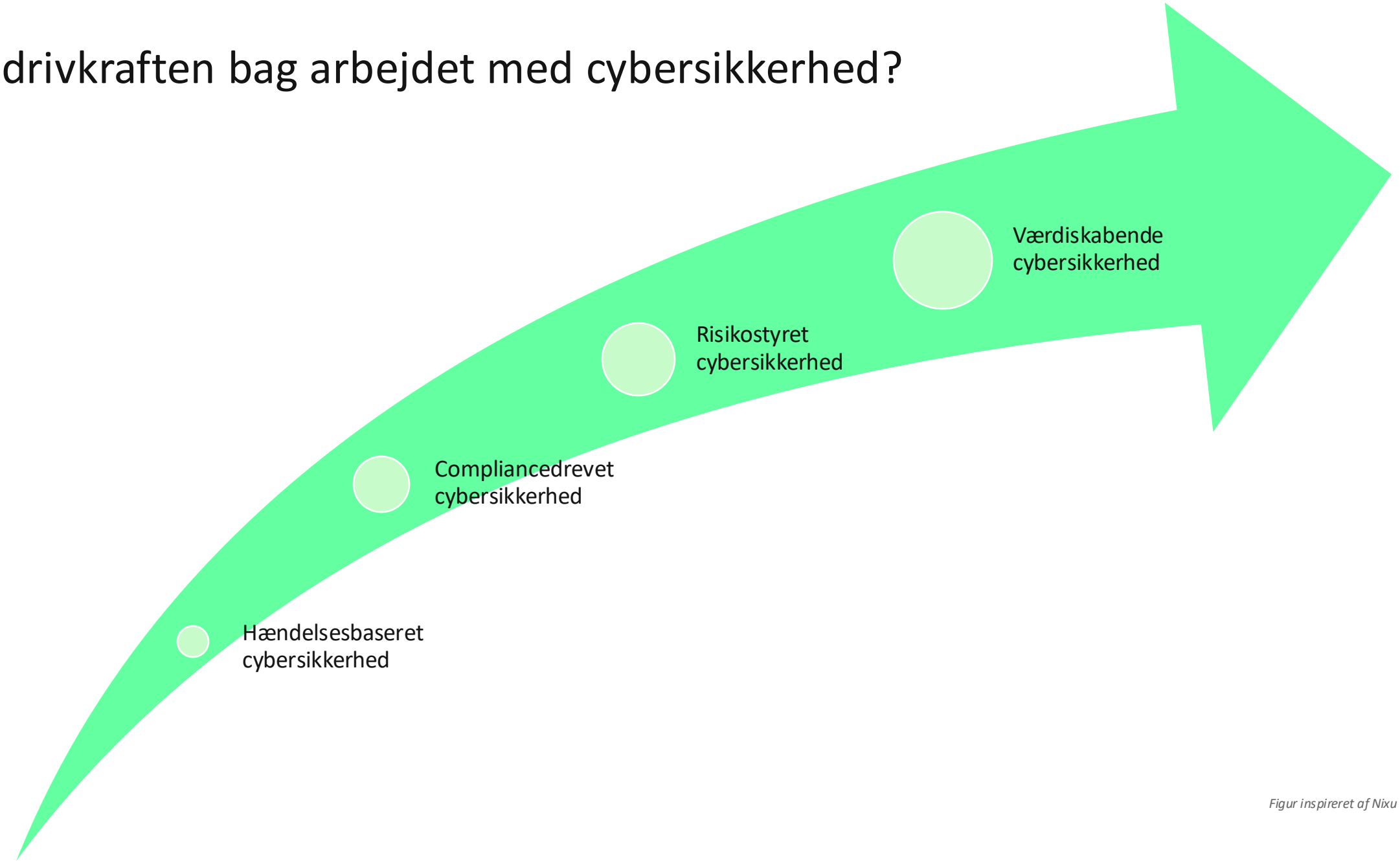
- Danmark vinder digitaliseringsmedaljen, men glemmer ofte bagsiden
- En hyperudvikling i forhold til nye teknologier

INDUSTRIENS FOND

En satsning der kun er blevet vigtigere II

- Ny geopolitisk virkelighed
- Regulering fra EU: løftestang eller byrde?

Hvad er drivkraften bag arbejdet med cybersikkerhed?



Figur inspireret af Nixu

Cyberbarometer.dk

Cyberbarometeret viser sammenhængen mellem investeringer i cybersikkerhed og konkurrencefordele.

Baseret på årlig spørgeundersøgelse blandt CEOs i danske SMV'er.

Undersøger hvilke konkrete cybersikkerhedstiltag virksomhederne har gennemført inden for 3 kategorier: Teknik, forankring & styring og rutiner & træning.

Og om de oplever konkurrencefordele inden for kategorierne Effektivitet & nytænkning, Tillid og Bundlinje.

INDUSTRIENS FOND

Hovedresultater

1 Lille stigning i SMV'ernes cybersikkerhedstiltag

Gennem Cyberbarometerets målinger i 2022, 2023 og 2024 ses en positiv udvikling i antallet af implementerede cybersikkerhedstiltag blandt SMV'er. Bundniveauet er hævet, hvilket betyder, at færre virksomheder slet ikke har implementeret tiltag i 2024. Samtidig er andelen af virksomheder med et stærkt cyberforsvar steget.

I 2024 fokuserer Cyberbarometeret på SMV'ernes rejse mod et robust cyberforsvar. Interviews peger på, at særligt medarbejdertræning og tydelig kommunikation kan være nøgleelementer i at opbygge et solidt forsvar.

2 Det er stadig to ud af tre SMV'er, der oplever konkurrencefordele

Tidligere målinger af Cyberbarometeret har vist, at cybersikkerhed og konkurrencefordele går hånd i hånd. I 2024 er der stadig en tydelig sammenhæng mellem SMV'ernes implementering af tiltag og deres oplevelse af konkurrencefordele.

Fra 2022 til 2023 steg andelen af virksomheder, der oplevede konkurrence-fordele, fra 56 pct. til 72 pct. I 2024 er denne udvikling stagneret, og 69 pct. af virksomhederne rapporterer nu om konkurrencefordele ved deres cybersikkerhedstiltag.

3 Konkurrencefordele handler om mere end antallet af tiltag

Det er ikke kun antallet af cybersikkerhedstiltag, der gør en forskel. Virksomheder opnår konkurrencefordele, når cybersikkerhed betragtes som en helhed, der både omfatter tekniske, organisatoriske og forankrende tiltag.

Årets Cyberbarometer viser desuden, at særligt tillid kan styrkes gennem solid forankring i organisationen og ved tydelig kommunikation til omverdenen.

4 Krav fra omverdenen påvirker SMV'ernes cyberstrategi

SMV'ernes cyberstrategi sker ikke i et vakuum, men påvirkes i høj grad af virksomhedernes omverden.

Hver femte SMV oplever, at deres kunder stiller krav til virksomhedens cybersikkerhed, og hver fjerde oplever krav til, at deres underleverandører skal have et højt niveau af cybersikkerhed. Der er en markant sammenhæng mellem at opleve forventninger udefra, og at sikre sin egen cybersikkerhed og sin værdikæde.

3 former for konkurrencefordele

Effektivitet & nytænkning

- At virksomheden er blevet bedre til at implementere og bruge nye teknologier
- At virksomheden har styrket sin nytænkning og innovation
- At arbejdsgange i virksomheden er blevet simplere eller mere effektive

Tillid

- At tilliden fra bestyrelsen til virksomhedens ledelse er øget
- At tilliden fra investorer og aktionærer til virksomhedens ledelse er øget
- At virksomheden har styrket relationen til eksisterende kunder
- At tilliden er øget fra virksomhedens samarbejdspartnere (herunder underleverandører)

Bundlinje

- At virksomheden har kunnet differentiere sig fra konkurrenter
- At virksomheden har kunnet tiltrække nye kunder
- At virksomheden har kunnet tiltrække nye kompetente medarbejdere
- At virksomheden har kunnet hæve prisen på de produkter virksomheden sælger

Benchmarkværktøj

- Få overblik
- Få anbefalinger
- Få sammenligninger til andre virksomheder
- www.cyberbenchmark.dk

FRA CYBERSIKKERHED TIL KONKURRENCEFORDELE

På baggrund af dine besvarelser anbefaler vi, at I sætter ind overfor nedestående tiltag:

1 Løbende opdateringer af virksomhedens software

Hvordan kommer jeg igang?

2 Udarbejdelse eller opdatering af it-beredskabsplan

Hvordan kommer jeg igang?

3 Opkvalificering af den øverste ledelse i it-sikkerhed eller ansvarlig dataanvendelse

Hvordan kommer jeg igang?

INDUSTRIENS FOND

Hvordan bliver stærk cybersikkerhed til en forretningsmæssig styrke?

- Afgørende med ledelsesfokus
- Træk din værdikæde med ind i cybersikkerhedsarbejdet
- Synliggør din cybersikkerhedsindsats

Styrkelse af Strategiske Cyberkompetencer

Projektejer
Bestyrelsesforeningen på CBS

:INDUSTRIENS FOND

Formål

Projektet har fokus på at øge opmærksomhed og kompetencer inden for håndtering af cyberkriminalitet i danske bestyrelser og direktioner.

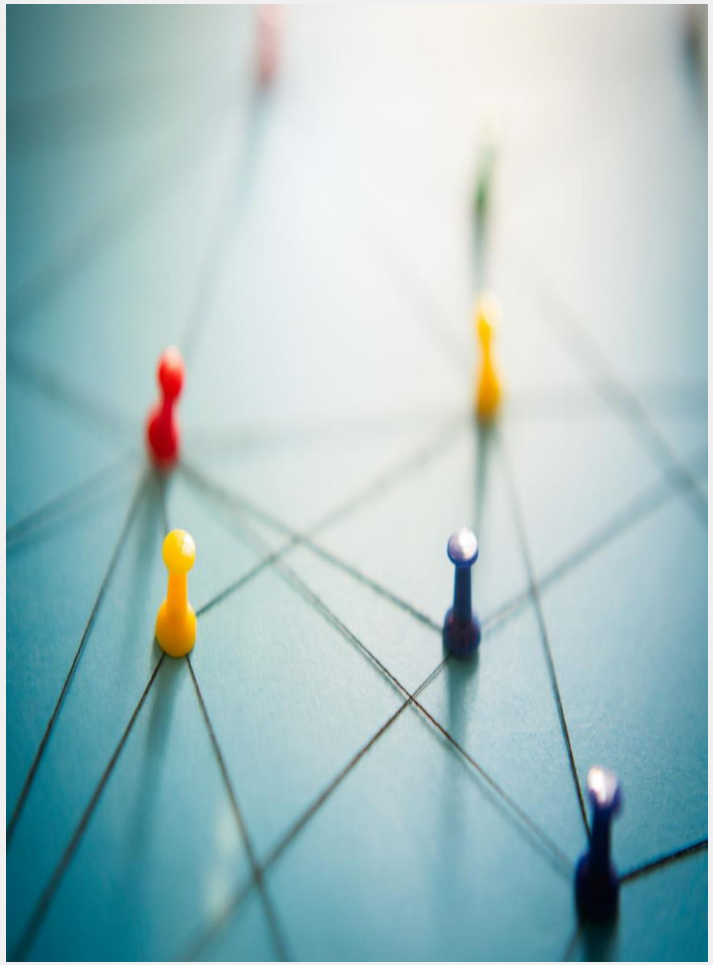
Hvordan hjælper projektet SMV'er?

- Viden og vejledning
- Cybersimulator med fokus på hændelseshåndtering

- https://bcfc.dk/

Cybersikkerhed i værdikæden

- Stigning i supply chain angreb
- Skaber øget kompleksitet i cybersikkerhedsarbejdet
- SMV'erne kan blive de store tabere
- Ændret dialog virksomheder imellem
- Mærker og standarder til at skabe transparens



D-mærket:

D-mærket er en mærkningsordning for it-sikkerhed og ansvarlig dataanvendelse, som både hæver sikkerhedsniveauet og konkurrenceevnen

www.d-maerket.dk/

01 Start med selvevalueringen

Den gratis selvevaluering af din eksisterende dataanvendelse og it-sikkerhed er det første skridt på vejen til at blive D-mærket. Her måles din besvarelse mod D-mærkets standarder for din type af virksomhed, så du opnår en rapport med konkrete anvisninger, der hjælper dig videre i processen hen imod en mulig tildeling.

02 Indsend din ansøgning

Når du har besvaret spørgsmålene i selvevalueringen, er du klar til at indsende din ansøgning om at blive D-mærket. Her har du brug for at kunne indsende dokumentation, der viser, hvordan din virksomhed lever op til de relevante krav og kriterier, der gælder for jer. Det er først i dette trin, at I vil blive opkrævet betaling.

03 Tilsyn og kontrol

Når du har indsendt ansøgningen, vil én af D-mærkets eksperter starte arbejdet med tilsyn og kontrol. Her vil I som virksomhed kunne opleve at få yderligere spørgsmål om jeres dokumentation for, hvordan I lever op til netop jeres kriterier.

04 Tildeling af D-mærket

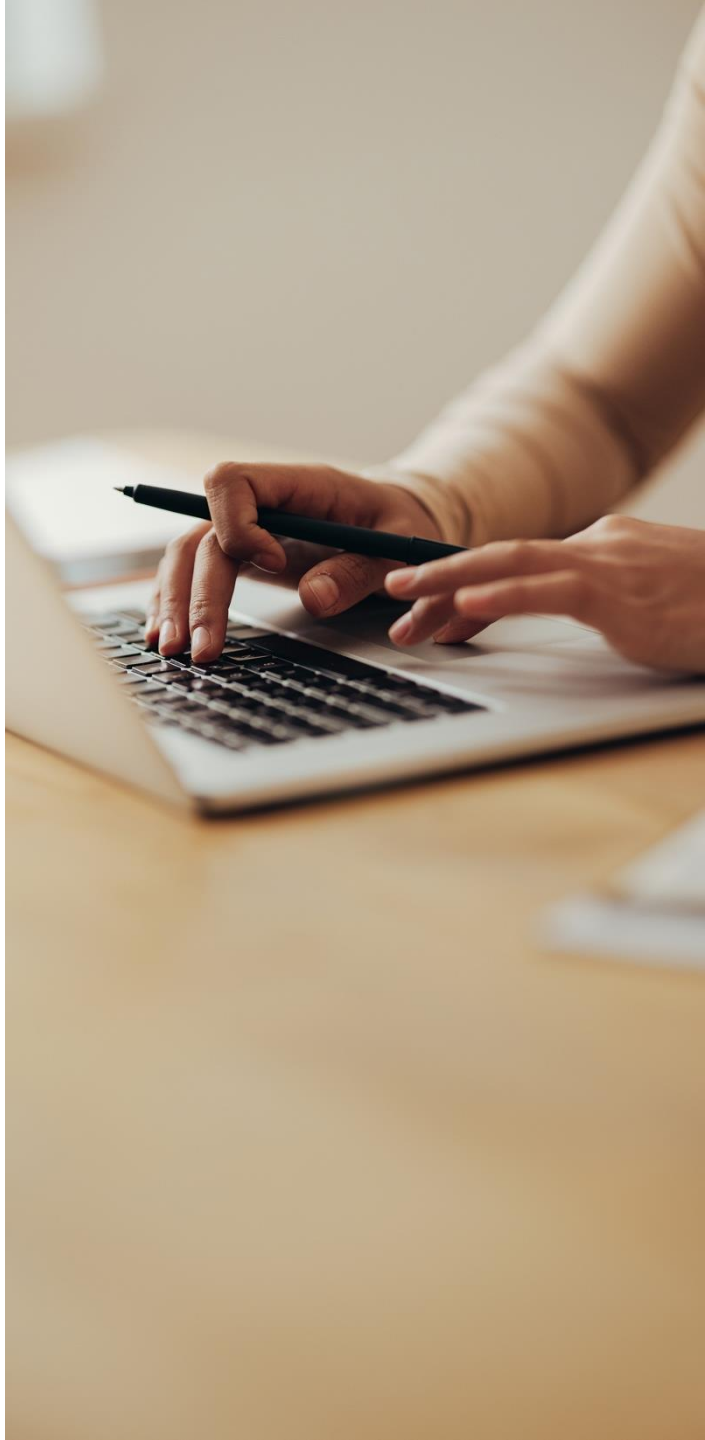
Når jeres ansøgning og dokumentation er gennemgået og godkendt, vil I som virksomhed modtage jeres velfortjente D-mærke - et symbol, der skaber tillid og viser jeres ansvarlighed og forpligtelse på sikkerhed overfor både kunder, kolleger og samfund.

1 KRITERIE 1 Styring og forankring i ledelsen →	2 KRITERIE 2 Awareness og sikker adfærd →
3 KRITERIE 3 Teknisk it-sikkerhed →	4 KRITERIE 4 Krav til leverandørers it-sikkerhed og ansvarlig dataanvendelse →
5 KRITERIE 5 Transparens & kontrol med data →	6 Privacy & security by design and default →
7 KRITERIE 7 Pålidelige algoritmer og AI →	8 KRITERIE 8 Dataetik

digital tryghed

Hvis I vil vide mere… :

https://industriensfond.dk/vores-fokusomrader/cybersikkerhed/



INDUSTRIENS FOND

TAK

www.industriensfond.dk

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.

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.

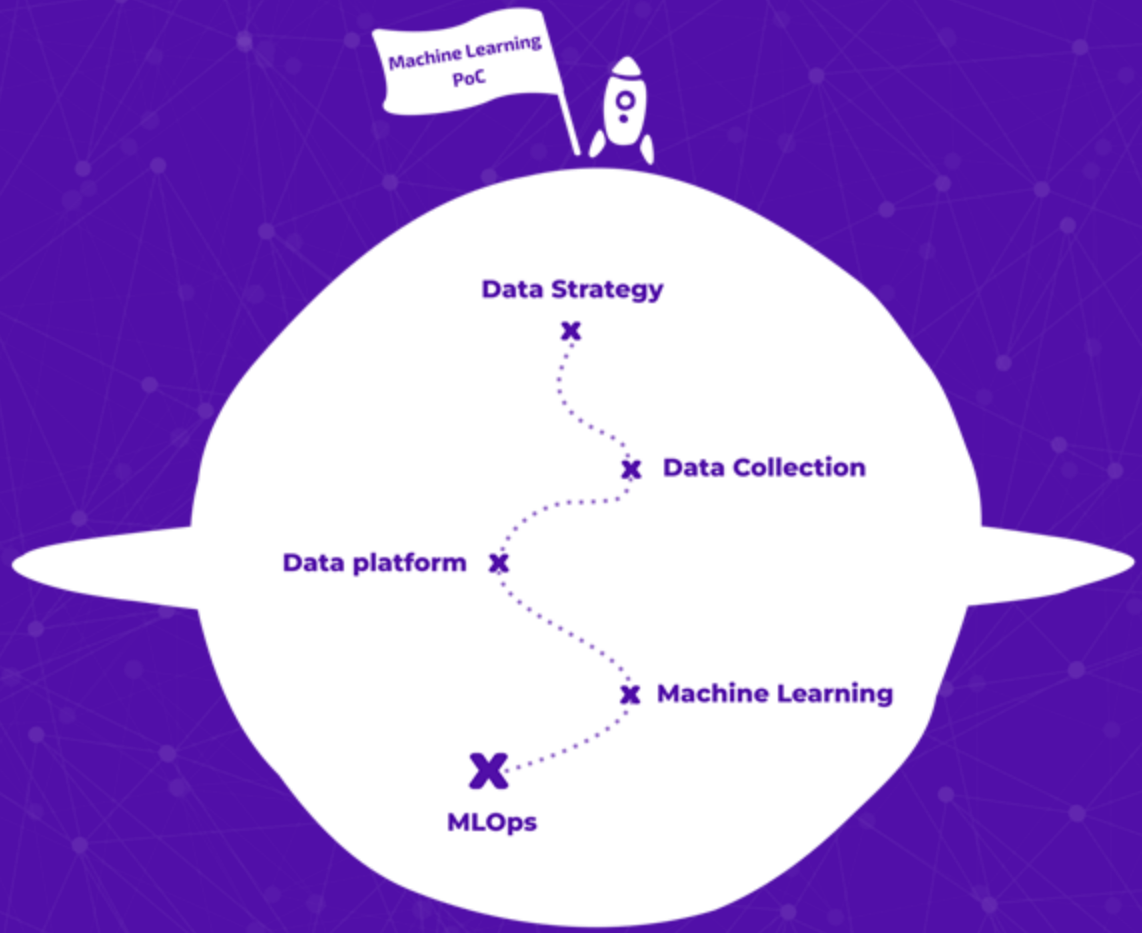
Rasmus Steiniche

CEO

@ **Neurospace**

Linkedin: *steiniche*

Solutions that fit your data journey



neuro space

Selected Customers

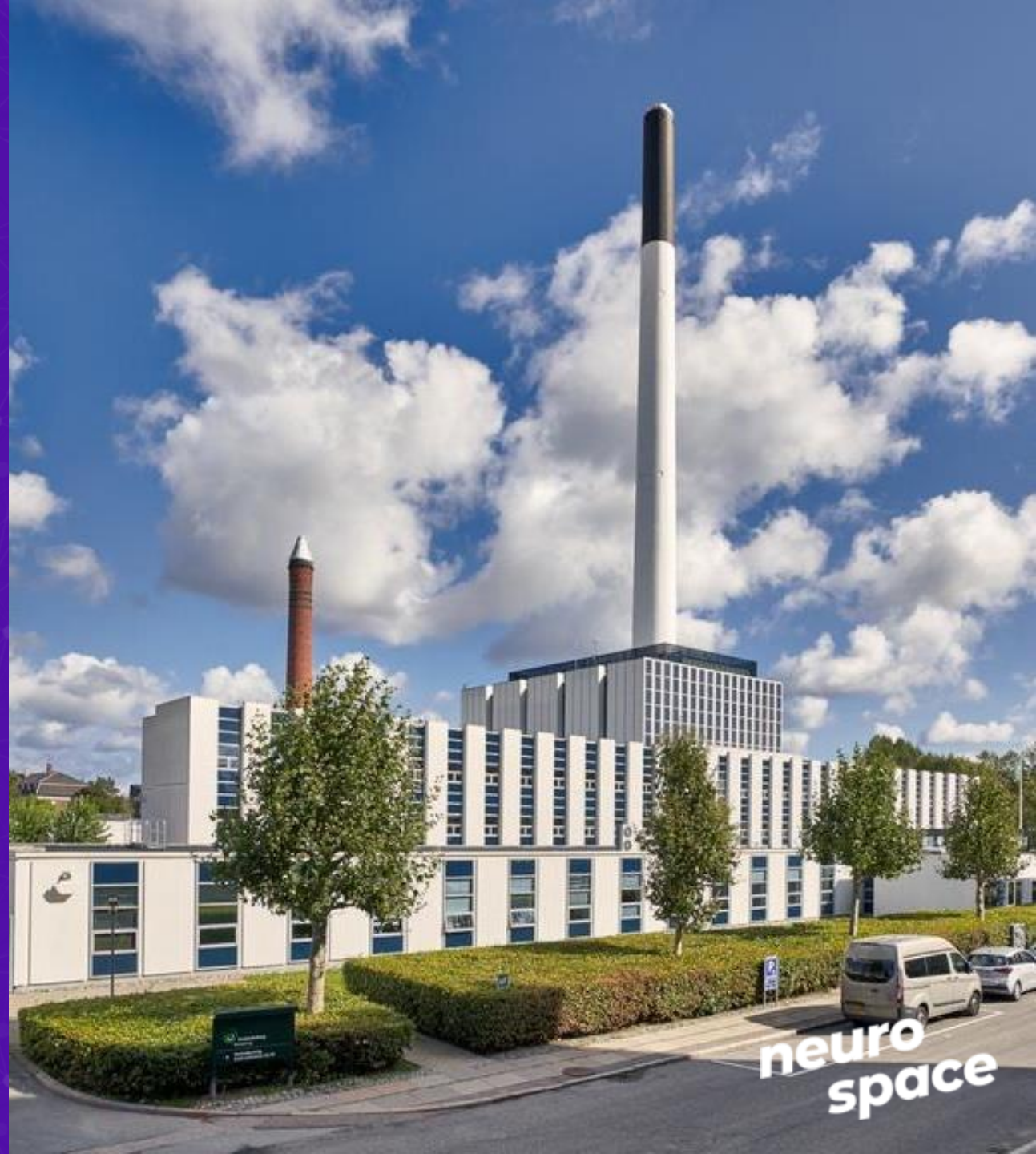
Partners

neuro space

Principle: **10 x Security**

Project LAVA

Predicting Optimal Temperature in the Transmission System



C | T | R

Predictive Maintenance

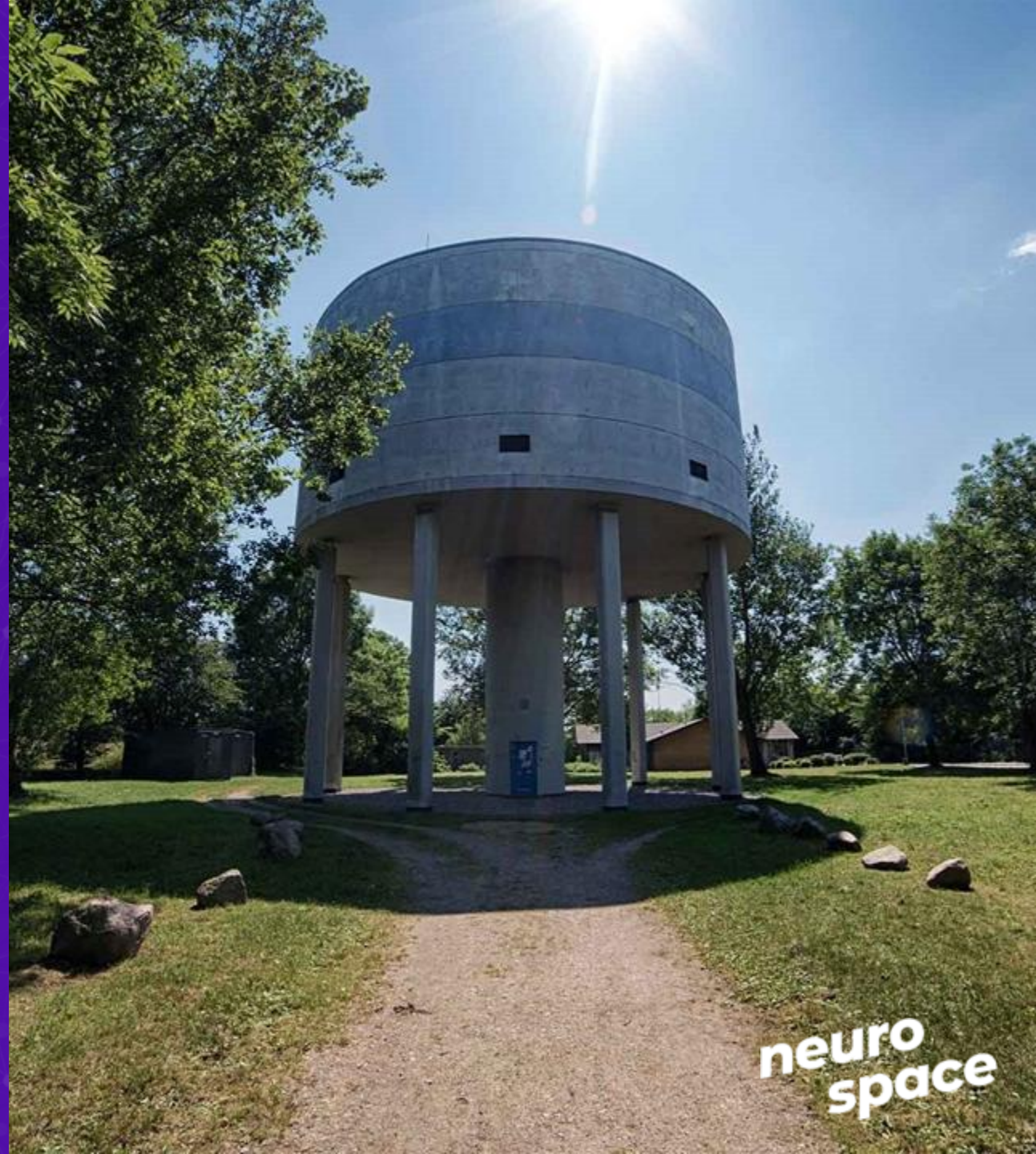
Semiconductor Switches

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

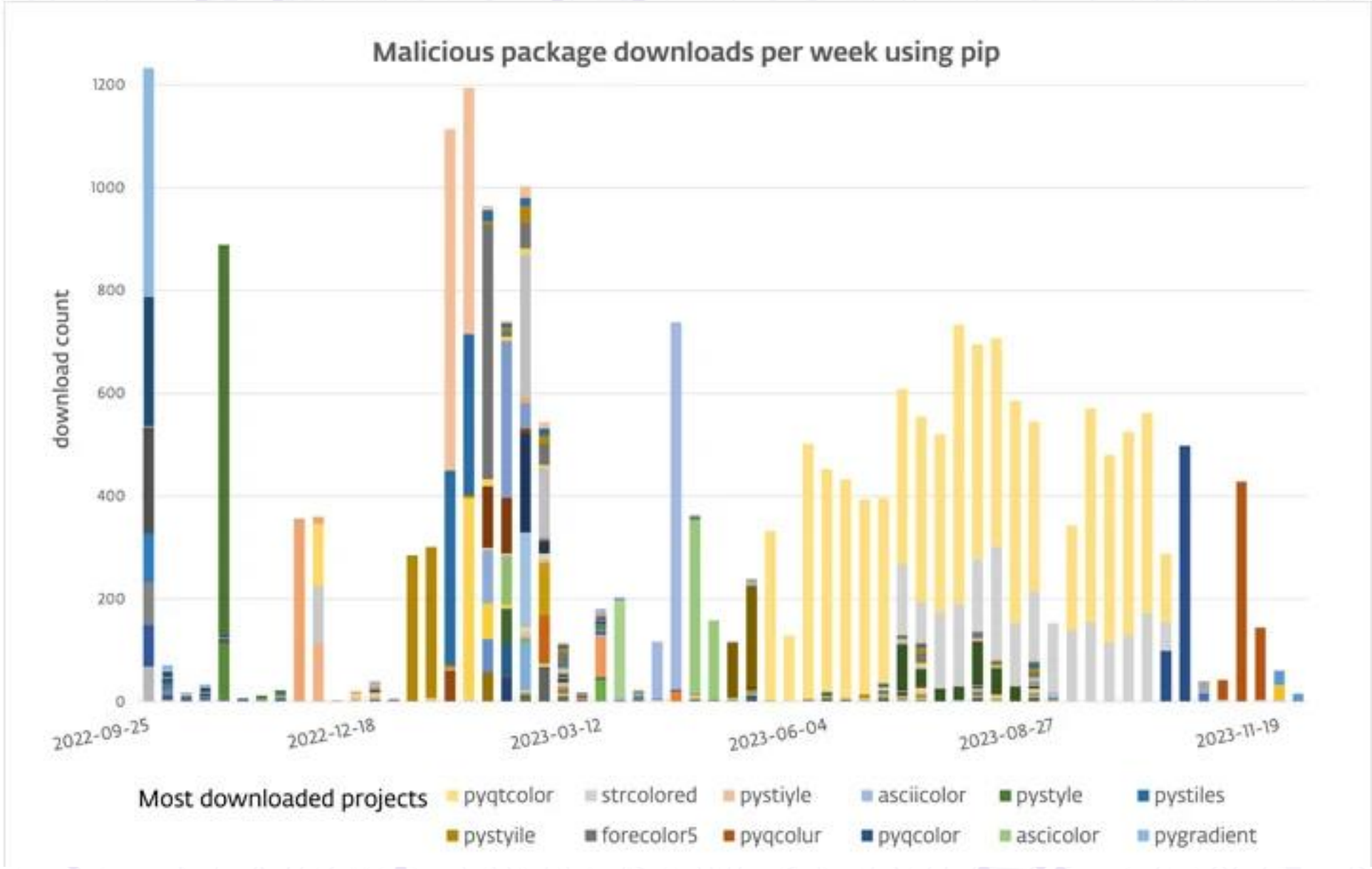
ML Algorithm

+

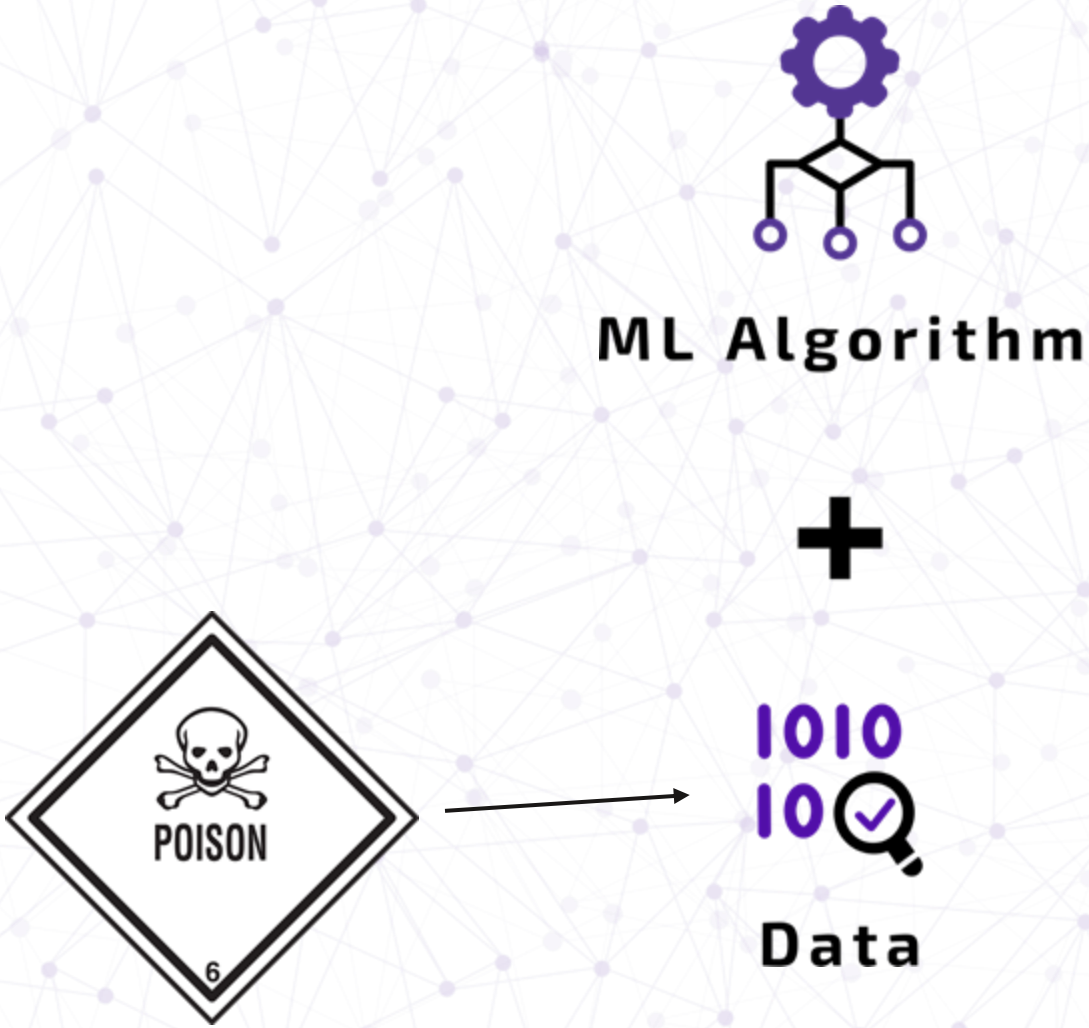
Data

116 Malware Packages on PyPI Repository Infecting Windows and Linux

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

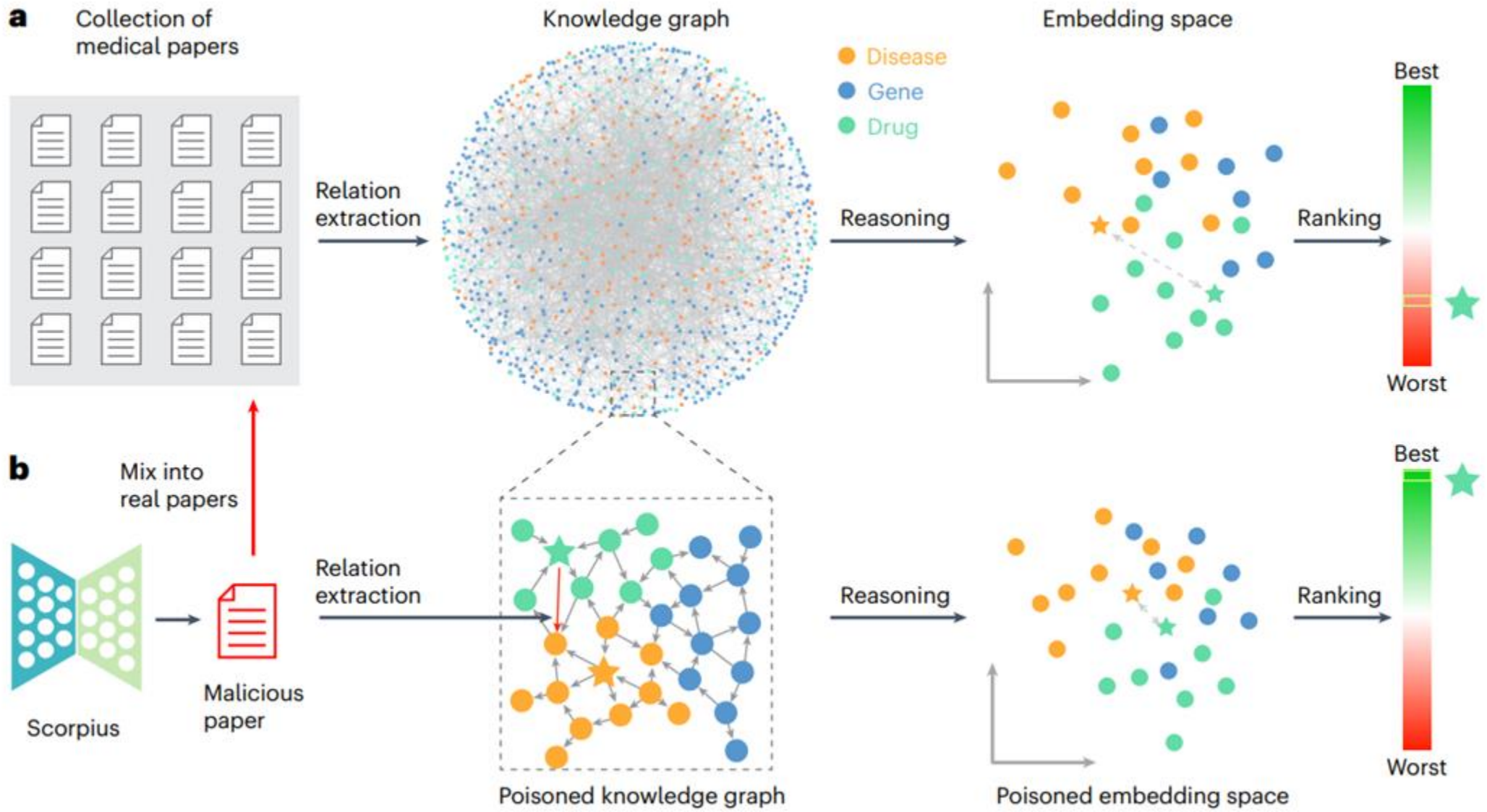


Poison Traning Data



Poisoning medical knowledge using large language models

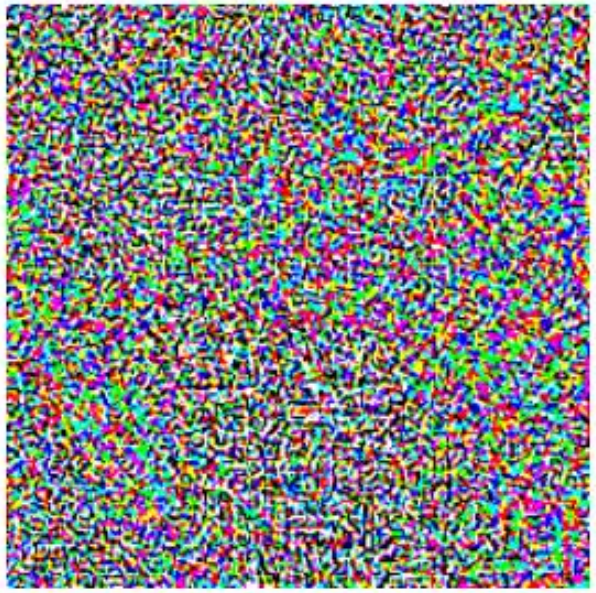
https://juweipku.github.io/files/NMI24.pdf



Poison Model Input

Explaining and Harnessing Adversarial Examples

$+ .007 \times$



$=$

$\boldsymbol{x}$

"panda"
57.7% confidence

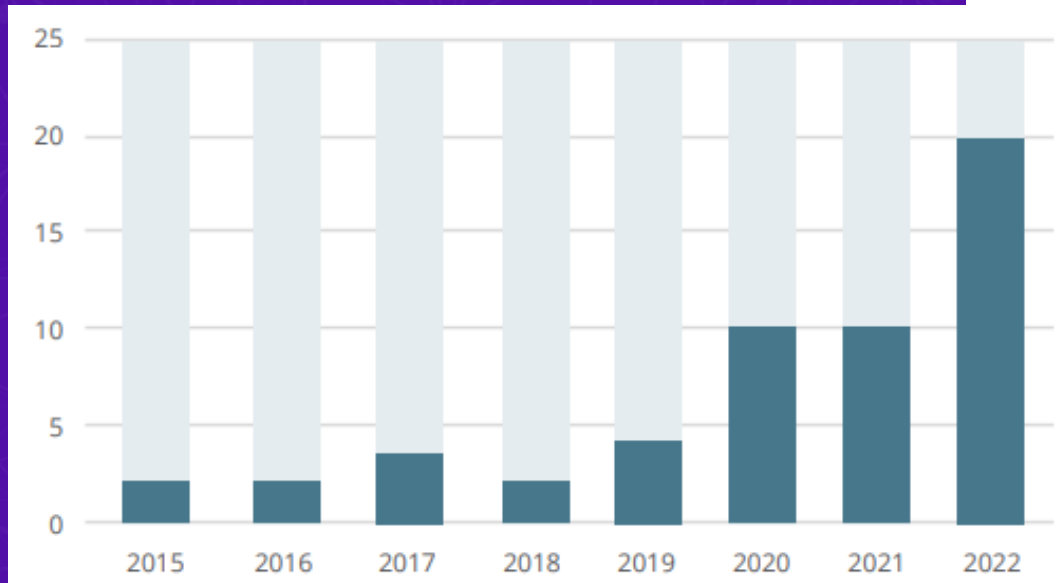
$\text{sign}(\nabla_{\boldsymbol{x}} J(\boldsymbol{\theta}, \boldsymbol{x}, y))$

"nematode"
8.2% confidence

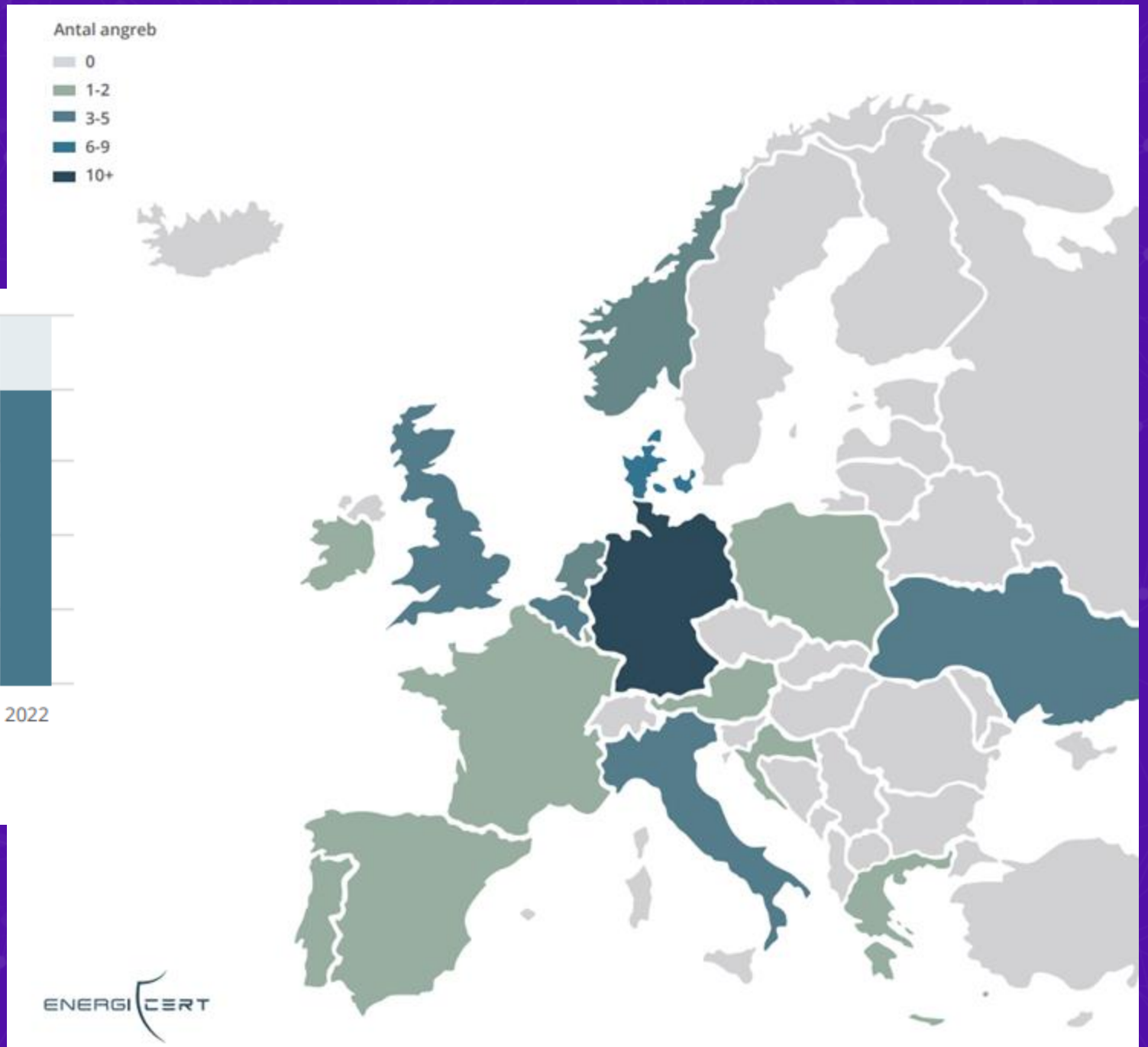
$\boldsymbol{x} +$
$\epsilon \text{sign}(\nabla_{\boldsymbol{x}} J(\boldsymbol{\theta}, \boldsymbol{x}, y))$
"gibbon"
99.3 % confidence

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

Benjamin Rasmussen
Cybersecurity Specialist
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

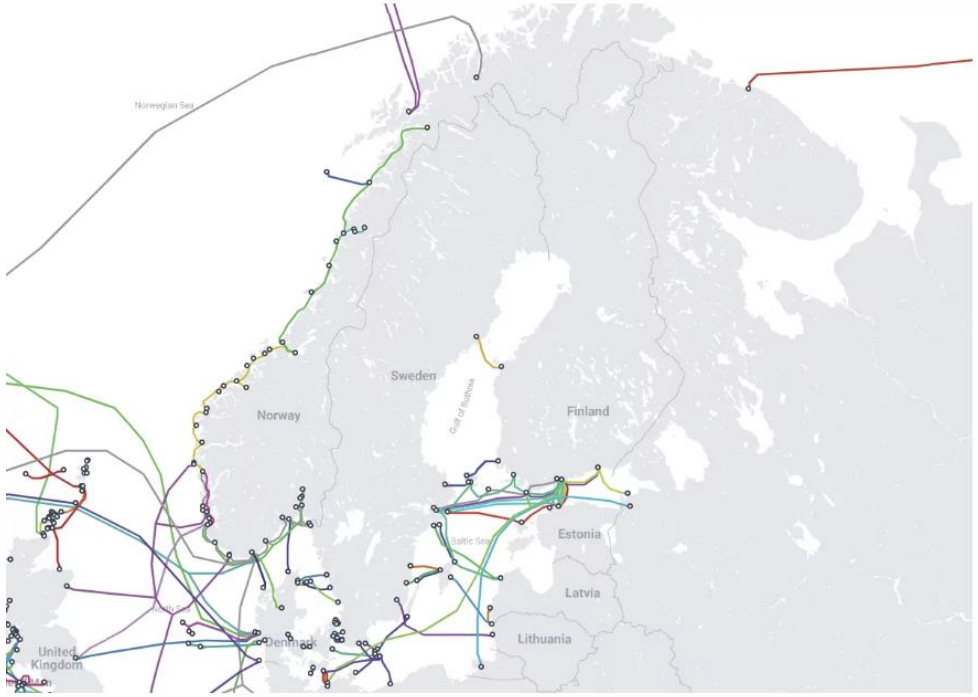
En verdensorden baseret på rå magt

Fra Jalta til Riyadh

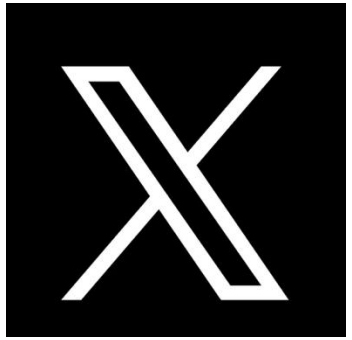
Grønlands-affæren

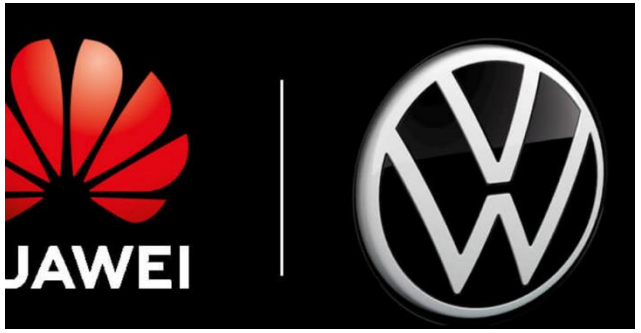
Skyggekrig mod Europa fortsætter

- 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!