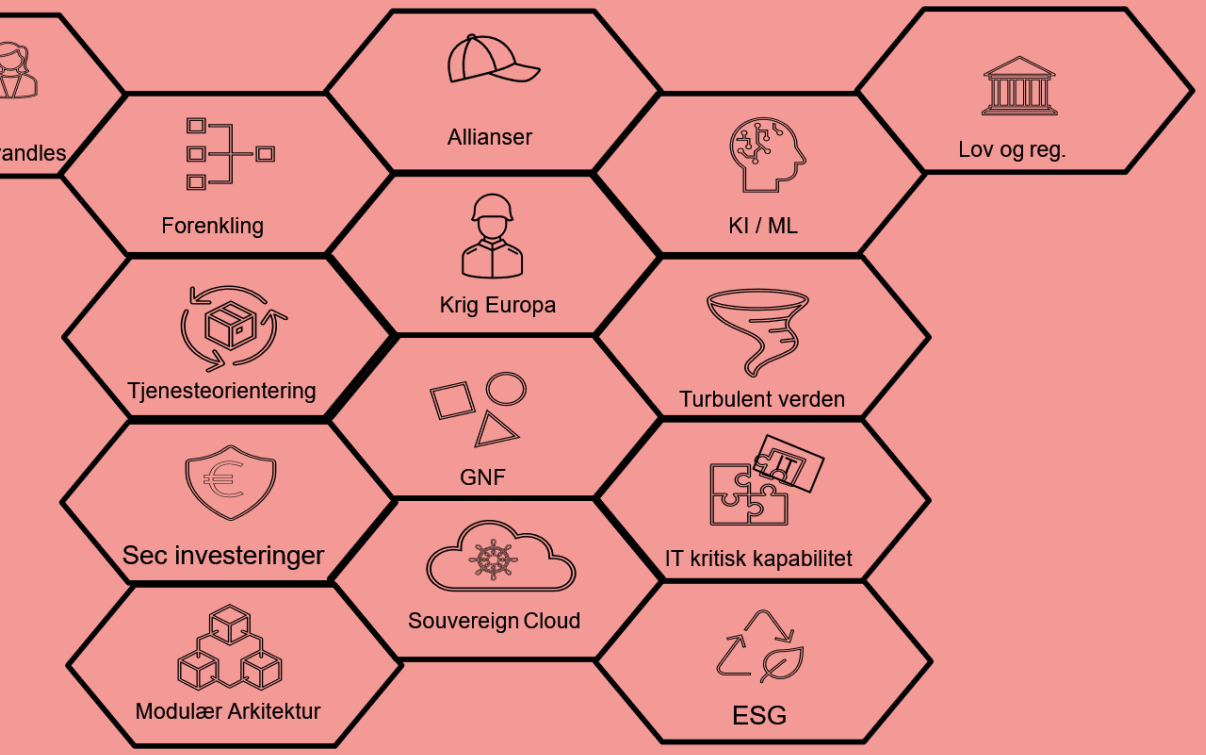
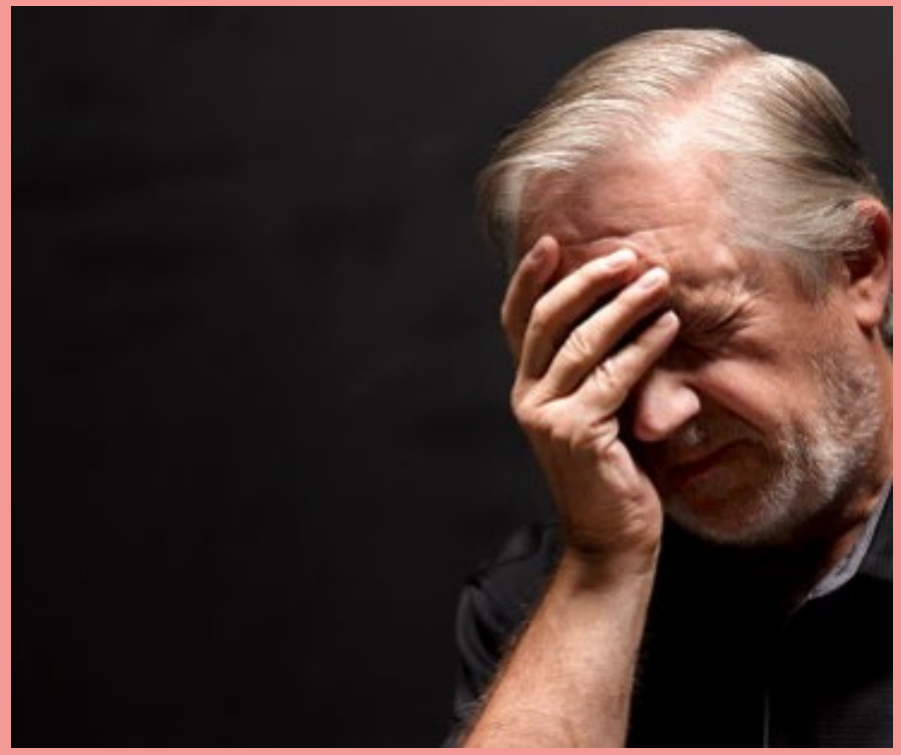


Fra ord til handling. Et arkitektur og sikkerhetsperspektiv.

André Barkhald | Senior Solution Architect
Orange Cyberdefense

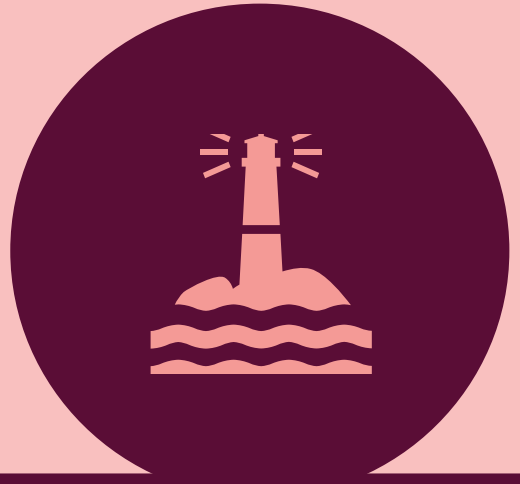
Hvorfor måtte vi få dette på vår vakt!





Det som har fungert til nå, vil ikke fungere i fremtiden!

NOKIOS



Tradisjonelt ble selskaper bygd for å kunne stå imot disrupsjon. De måtte kunne stå støtt når det bølget som mest.



I dag må et selskap kunne ri disse bølgene. Endring er ikke lenger en hendelse, men en tilstand.

Den viktige balansen...

Å gjøre tingene riktig!

X > 0%

Å gjøre de riktige tingene!





Eksempel, mer konkrete mål.



Prioritering av tjenester...

Leveransekjede...

Nye behov...

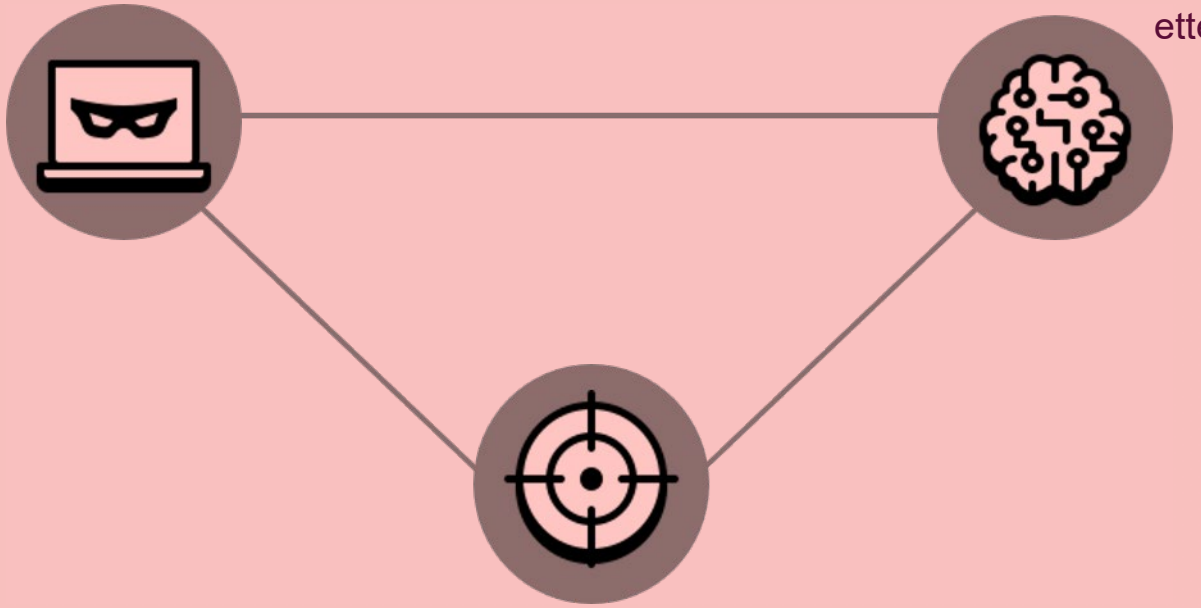
NOKIOS

“We tend to overestimate the effect of a technology in the short run and underestimate the effect in the long run.”

Roy Charles Amara
Researcher, scientist & past president of the Institute for the Future

AI sikkerhet er ikke bare én diskusjon

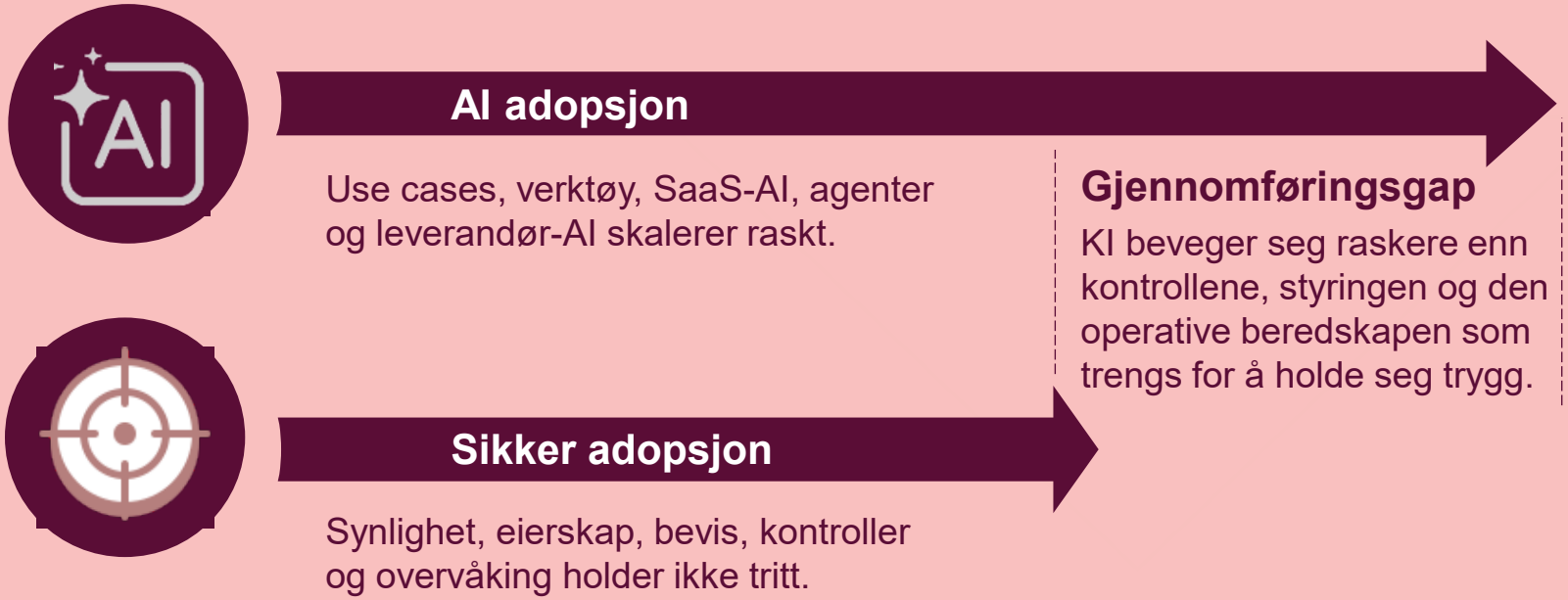
AI-augmenterte trusler
Angripere bruker AI til å skalere phishing, social engineering, rekognosering og rask variasjon.



AI for sikkerhet
Sikkerhetsmiljøene bruker AI til forbedring av triagering, etterforskning, deteksjon og respons.

Sikkerhet for AI
Organisasjoner må sikre egne AI-verktøy, applikasjoner, agenter, data- og arbeidsflyter.

AI-bruken akselerer...
Sikker bruk henger etter...

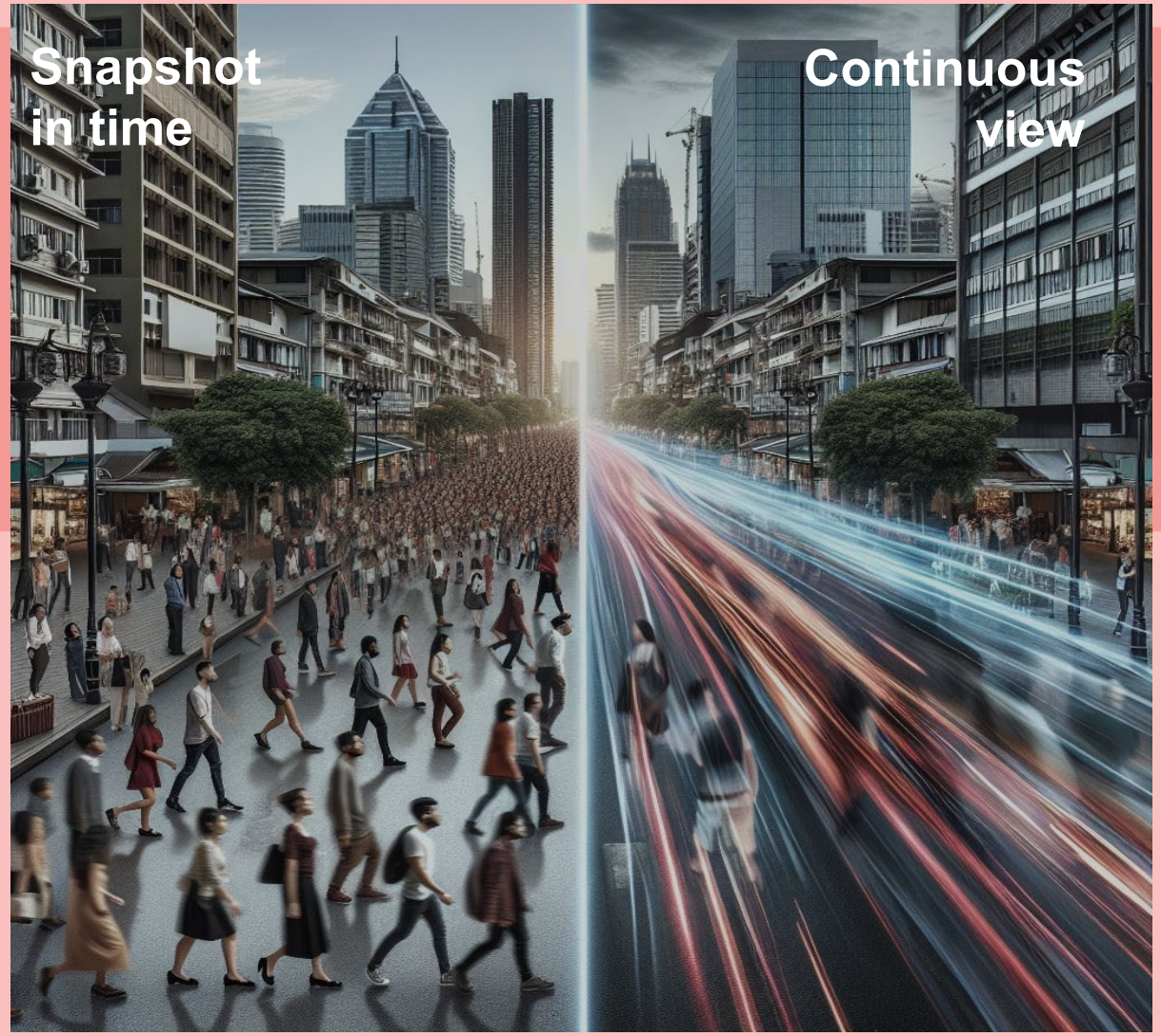


Målet er ikke å bremse AI-adopsjonen, men å muliggjøre det trygt.
Utfordringen er ikke bevissthet; det er gjennomføring.

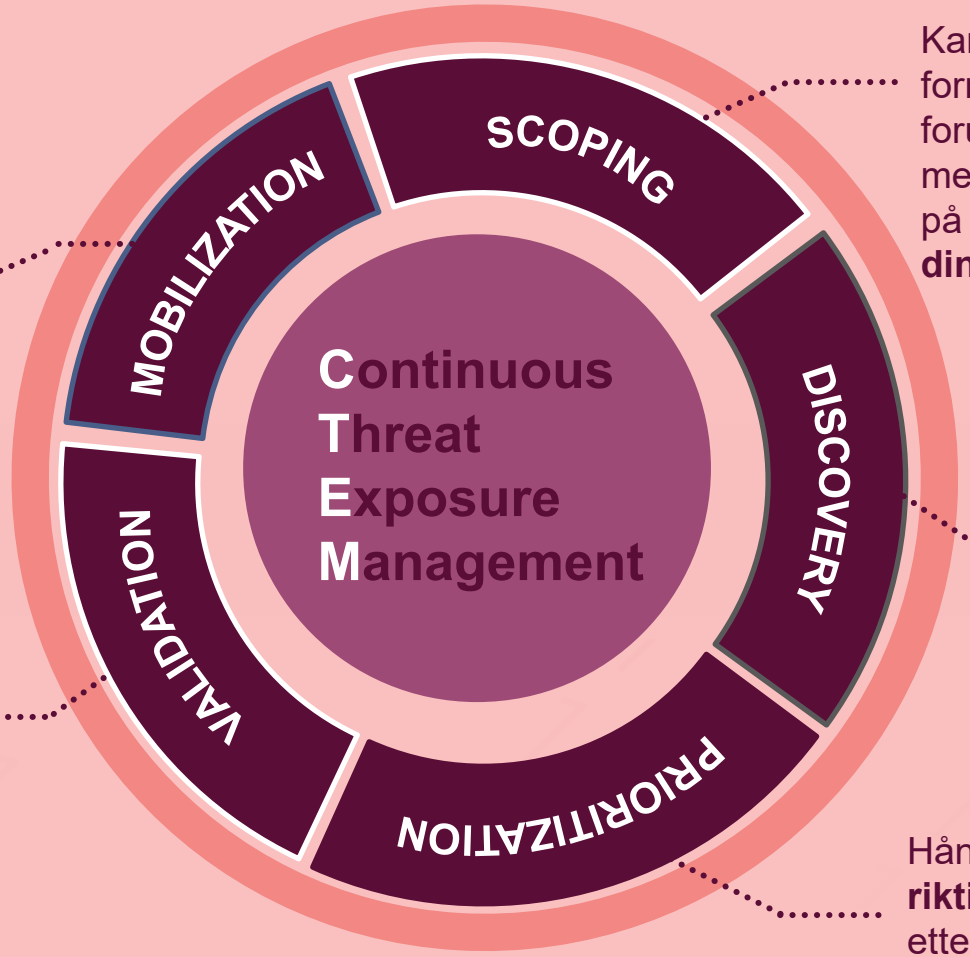
Nytt perspektiv.
Nytt språk.

fra… «en **sårbarhet** er en CVE»

til… «en **eksponering** er en CVE …**og** miskonfigurering, identitet, tilgangsstyring, tredjepartsrisiko, etc.»



NOKIOS



Kartlegg forretningsmessige forutsetninger. Hva er mest relevant å fokusere på for **din virksomhet**?

Kontinuerlig oppdagelse av **interne** og **eksterne** eksponeringer, inkludert verdier på avveie og merkevaresvindel.

Håndtere eksponeringer i **riktig rekkefølge**, basert på etterretning og forretnings-messige målsetninger.

Teste **angrepsstier** – hva kan faktisk utnyttes? Validere effektive sikkerhetskontroller. (volum, fokus, etterlevelse)

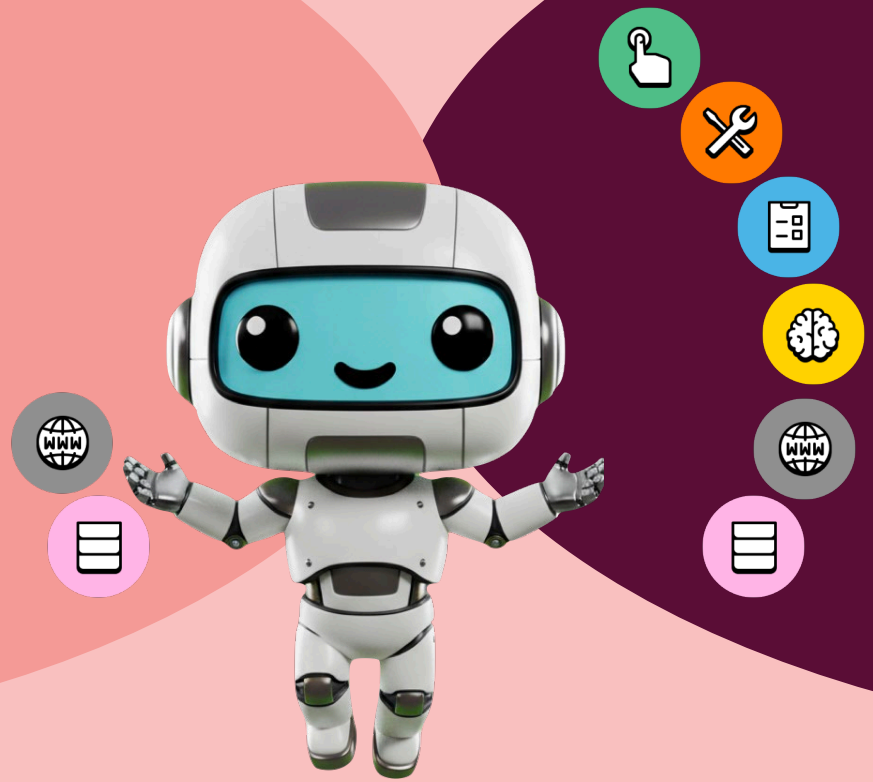
Respons- og håndteringsevne. Minimere angrepsflate og justere sikkerhetsstatus.

Fremveksten av Agentisk AI endrer risikoligningen

NOKIOS

Tradisjonell GenAI

Et reaktivt system som produserer innhold (tekst, bilde, kode, osv.) som svar på en spesifikk forespørsel.



Agentic AI

Et autonomt system som oppfatter sitt miljø, resonerer, planlegger og handler ved hjelp av eksterne verktøy for å oppnå et gitt mål.

orange Cyberdefense

Sikkerhet for AI - en huskeliste å starte med

NOKIOS



Analyser risikoen din



Øk bevissthet i hele virksomheten



Tilpass styring og policy



Sjekk dine sårbarheter



Beskytt AI-apper & infrastruktur

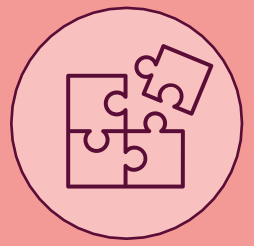


Sikre bruken av GenAI-apper

Oppsummert...



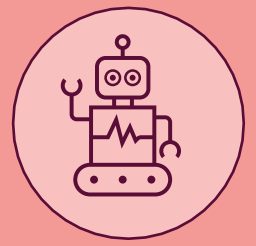
Lær å «surfe»



Tid til de riktige tingene



Lær av «naboen»



AI sikkerhet, ikke bare én diskusjon

Kontaktinformasjon



André Barkhald
Senior Solution Architect, Orange Cyberdefense

Andre.barkhald@orangecyberdefense.com

LinkedIn:
https://www.linkedin.com/in/abarkhald/

NOKIOS

Norsk konferanse for IKT i offentlig sektor