

Varslingssystem for digital infrastruktur (VDI)

- Hvorfor er tillit så viktig?

«NSM skal gjøre Norge i stand til å beskytte seg mot spionasje, sabotasje, terror og sammensatte trusler»

NASJONALT CYBERSIKKERHETSSENTER

Utvikling og
tilgjengeliggjøring av
tiltak og anbefalinger.
Rådgiving

Nasjonal
responsfunksjon
med deteksjon og
hendelsehåndtering

Nasjonale tekniske
sikkerhetstjenester

Samlet nasjonal kompetanse der ulike aktører samarbeider basert på felles risikobilde og situasjonsforståelse i felles lokaler og over nett

VDI

- Innhente, prosessere og analysere data, for å avdekke og håndtere cyberoperasjoner
- Eksistert siden slutten av 90-tallet
- Tillitsbasert samarbeid
- 2003 - NSM etablert
- 2006 - NorCERT etablert
- Kontinuerlig under utvikling for å møte dagens trusselbilde

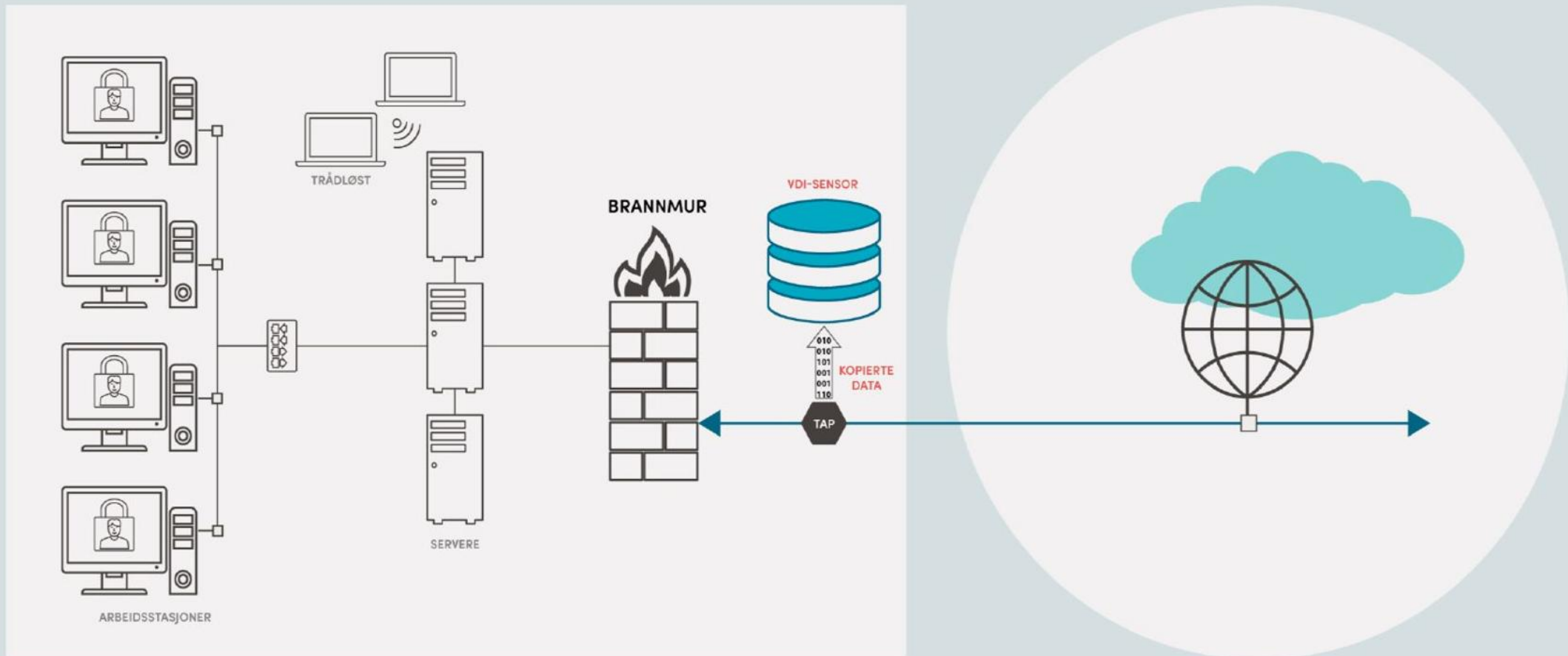


VDI-sensorplassering

DELTAGENDE
VIRKSOMHET

VDI-SENSOR

INTERNETT



Trusselaktører



Operasjonssenteret

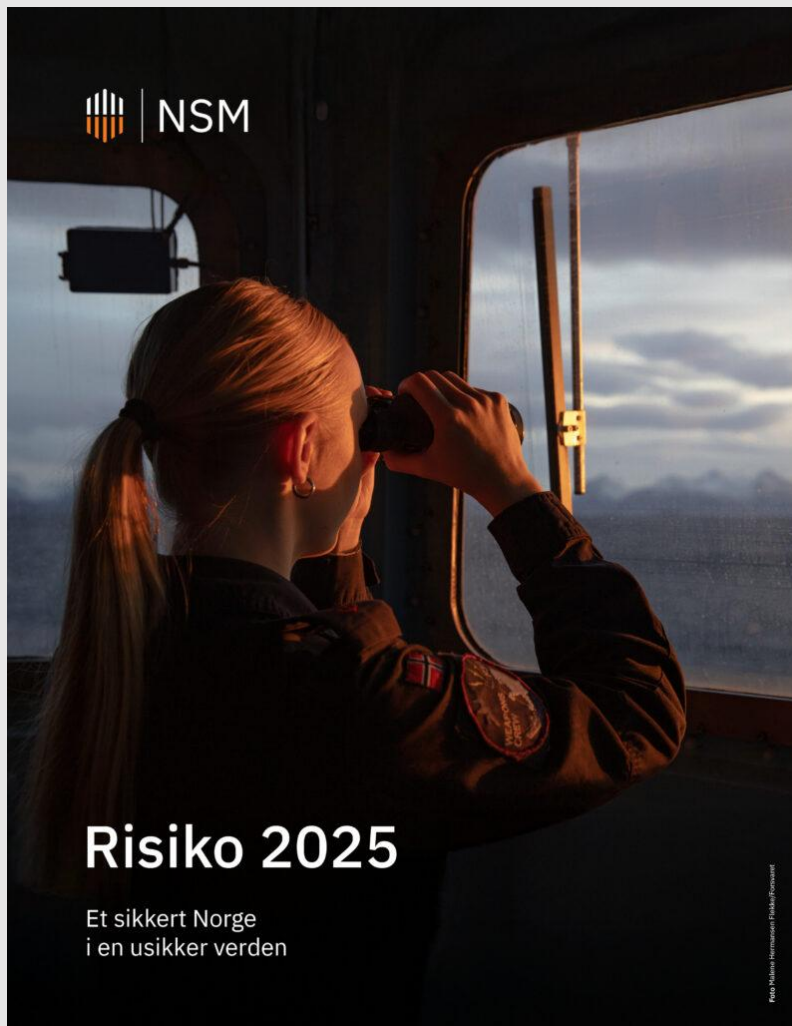
- Den operative delen av NSM
- 24/7 Operasjonssenter på Fornebu
- Detekterer, håndterer og analyserer de mest alvorlige, digitale angrepene og truslene mot norsk infrastruktur og informasjon
- Produserer det nasjonale, digitale **situasjonsbildet**
- Stort fagmiljø med ekspertise innen
 - Forensics
 - Nettverksanalyse
 - Skadevareanalyse
 - Sårbarhetsanalyse
 - Flerkildeanalyse
 - Avanserte sensor og deteksjonsteknologier



Utfordring til dagens nasjonale deteksjonsevne

- Hjemmelsgrunnlag
- Kryptering
- Vanskelig å skille trusslaktøraktivitet fra normal/legitim aktivitet
- Skyløsninger
- Det er mye data som skal analyseres – krever nye analysemetoder
- KI – nye muligheter, men også utfordringer





Sikkerhet gjennom samarbeid