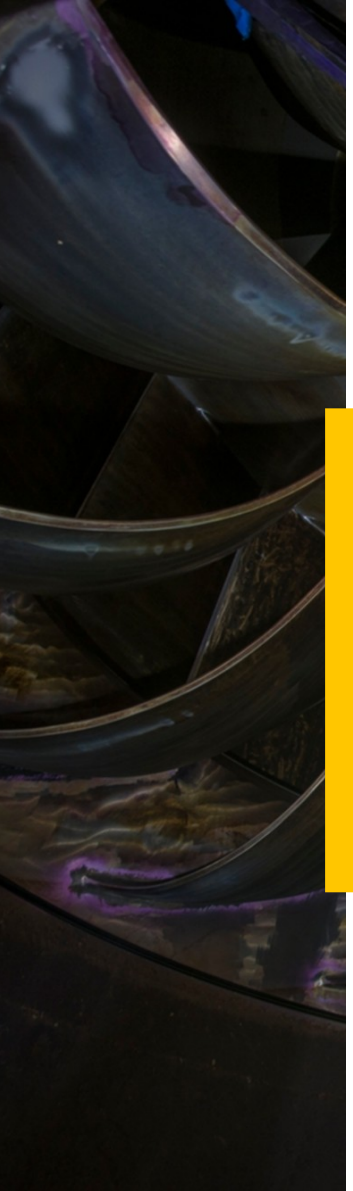
Sektorperspektiv på nasjonalt trusselbilde

Espen Nodeland, KraftCERT/InfraCERT

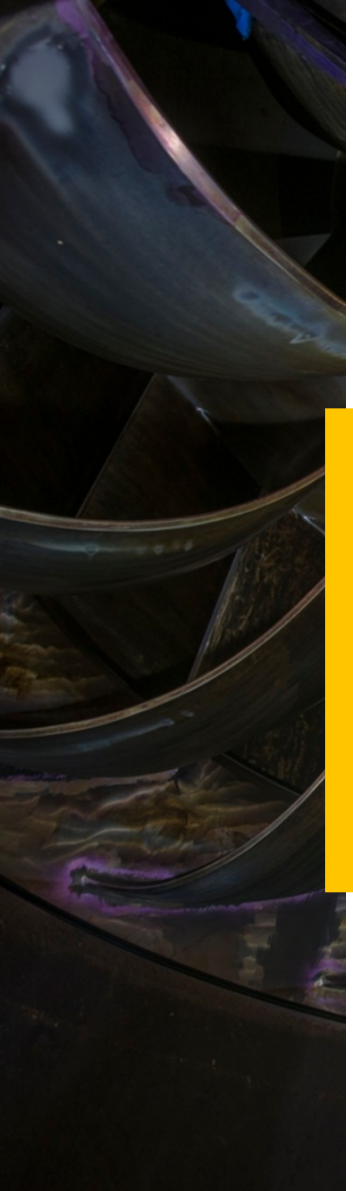
kraftCERT

infraCERT



InfraCERT/ KraftCERT

- Non-profit
- PTIL og NVE SRM
- Årlig trusselvurdering
- Kontinuerlig innhenting og analyse

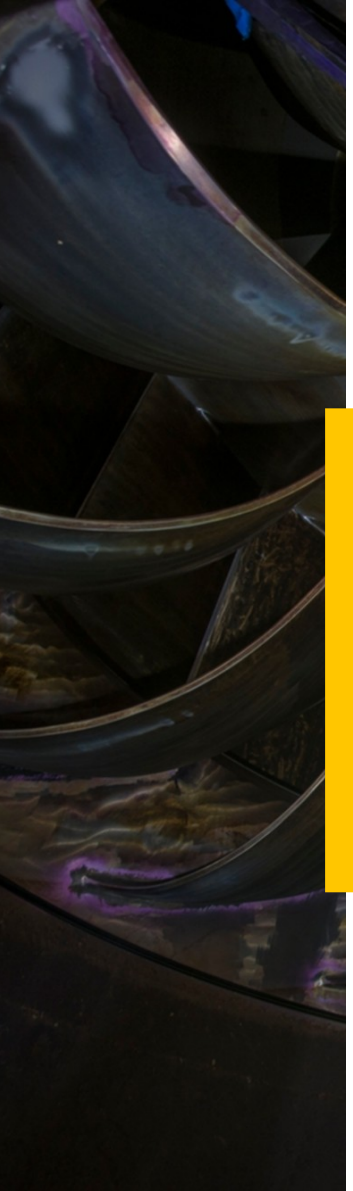


Bottom line

Nasjonale vurderinger kan ikke stå alene eller være primærgrunnlaget for trusselforståelse på sektor eller bedriftsnivå.

Sektorvist trusselbilde må bygges i sektoren.

Bedriftens trusselbilde må bygges lokalt.



Nasjonalt trusselbilde

ETJ – Fokus

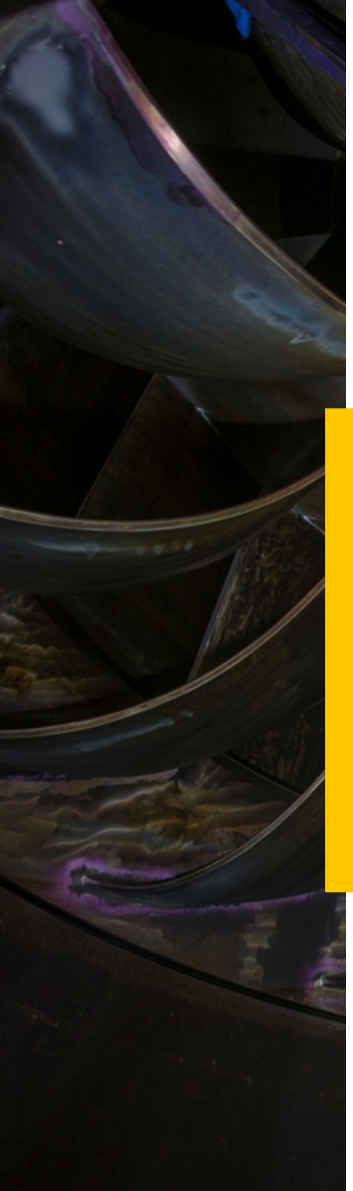
PST – Nasjonal trusselvurdering

NSM – Nasjonalt digitalt risikobilde/ Risiko 20XX

Andre:

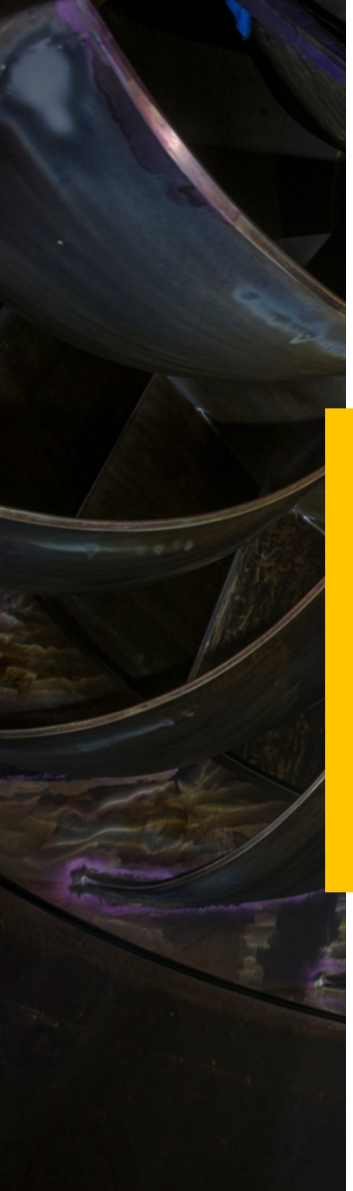
Kripos

NorSIS (Norsk senter for informasjonssikring)



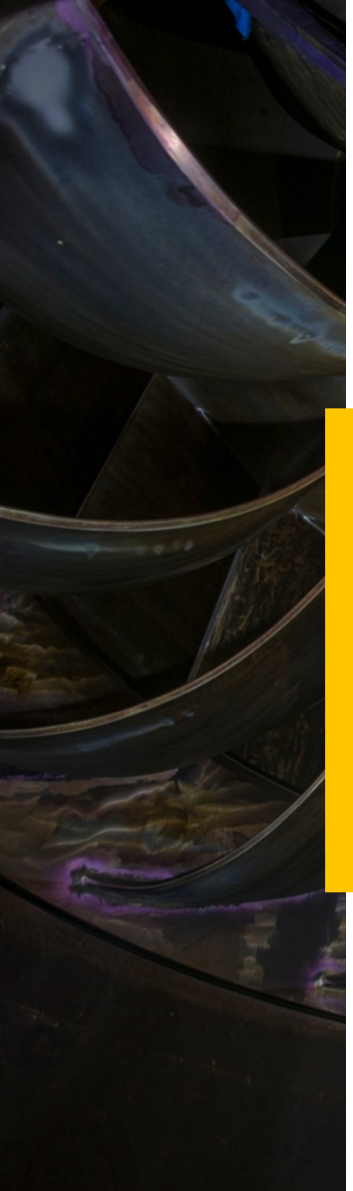
Sektorvist trusselbilde?

- Vi jobber ut fra egne definerte etterretningsbehov og spørsmål.
- Egen analyse, og holder denne opp mot relevante utdrag av nasjonale vurderinger.



Utfordringer

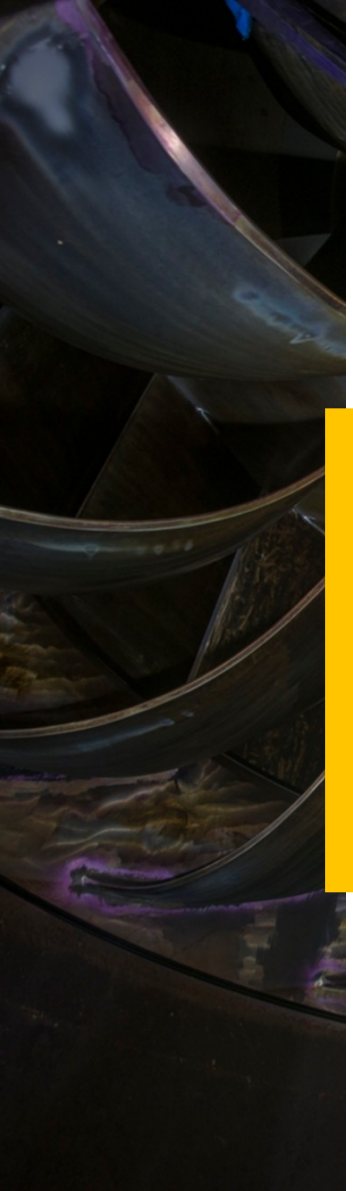
- Mottagere og målsettinger
- Begreper og språk
- Temarotasjon vs kontinuerlig bilde
- Skjult kilde og informasjonsgrunnlag
- Revir og markeringer



Eksempel 1 - språk

«NSM har stadig sett utnyttelse av menneskelige, teknologiske og organisatoriske sårbarheter for å understøtte ondsinnede cyberoperasjoner mot flere norske virksomheter.»

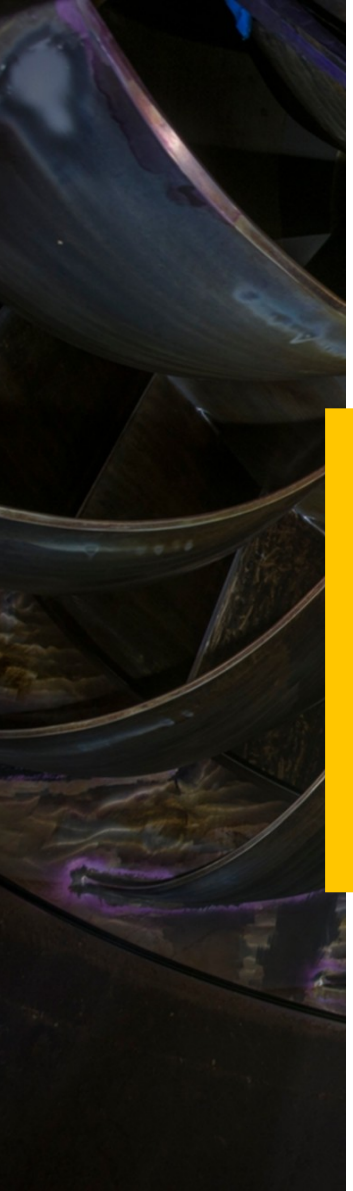
NSM Risiko 2023, s. 18



Eksempel 1 - språk

«NSM har stadig sett utnyttelse av menneskelige, teknologiske og organisatoriske sårbarheter for å understøtte ondsinnede cyberoperasjoner mot flere norske virksomheter.»

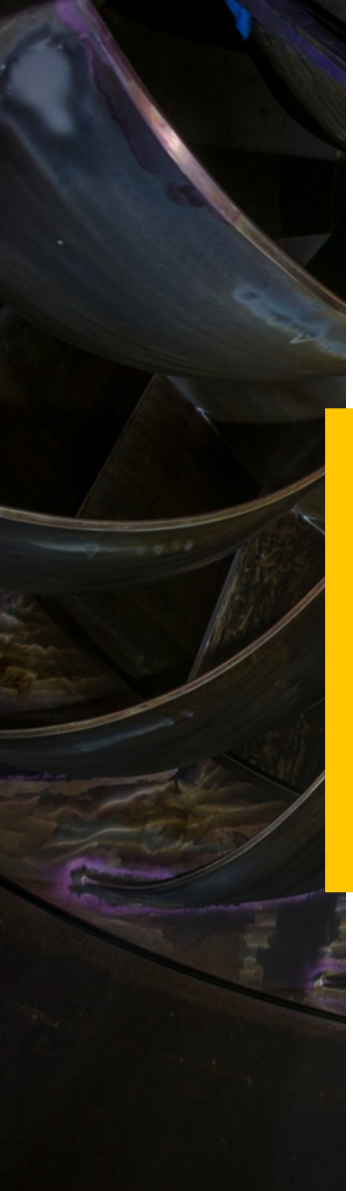
NSM Risiko 2023, s. 18



Eksempel 2 - volum

"I Norge har vi fra 2019 til 2021 sett en tredobling i alvorlige cyberoperasjoner mot norske myndigheter og virksomheter. Antallet alvorlige og svært alvorlige hendelser har i 2022 holdt seg på et tilsvarende nivå som i 2021."

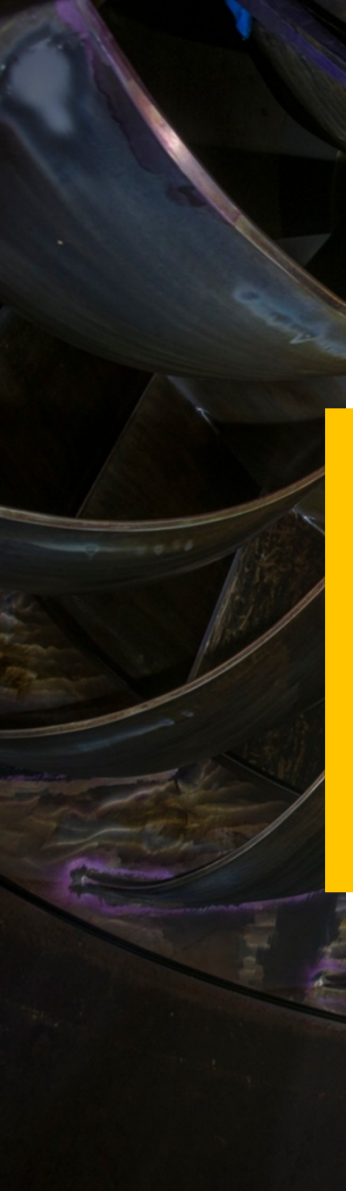
NSM Risiko 2023, s. 18



Eksempel 2 - volum

"De vanligste angrepene var distribuerte tjenestenektangrep, phishing og kartleggingsaktivitet."

NSM Risiko 2023, s. 18

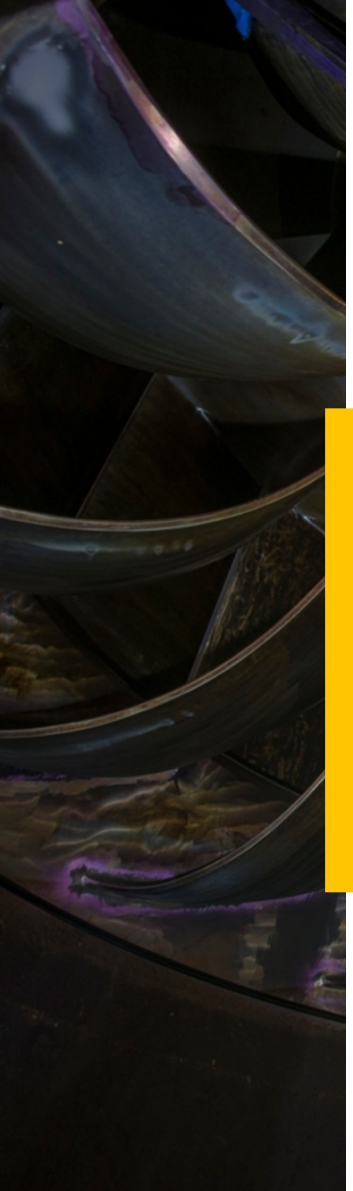


Sektorvist trusselbilde

Hva er en sektor?

Hva er et sektorangrep?

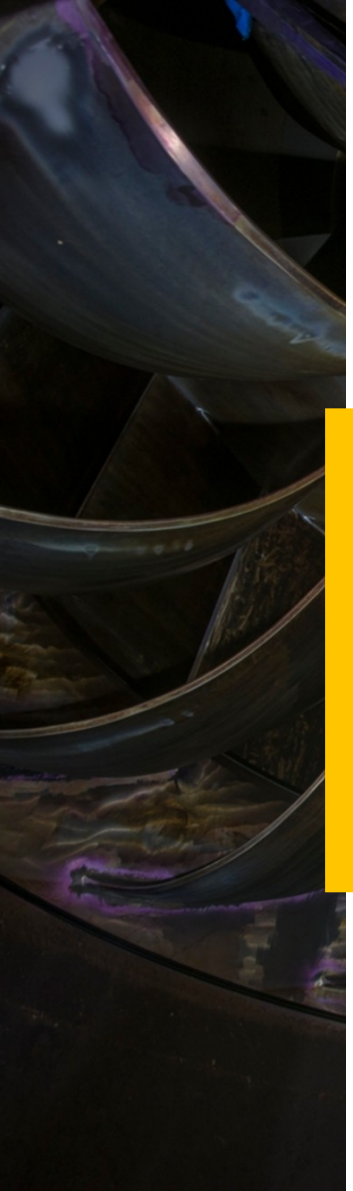
Hvem kan se et sektorvist trusselbilde?



Hva så?

Rapportering: Hjelp oss å hjelpe. PTIL og vi trenger innrapportering av hendelser.

Bygg metode og tiltro til egne vurderinger.



Startpunkt

1 Hvordan kommer vi til å bli angrepet? (Angrepsformer/ aktører)

Aktørtyper, spesfikke, intensjoner, evner, muligheter, metoder, konsekvenser, trender

2 Hvilke av våre teknologier nå og fremover vil bli angrepet/ øke graden av lykkede angrep? (Teknologi og marked)

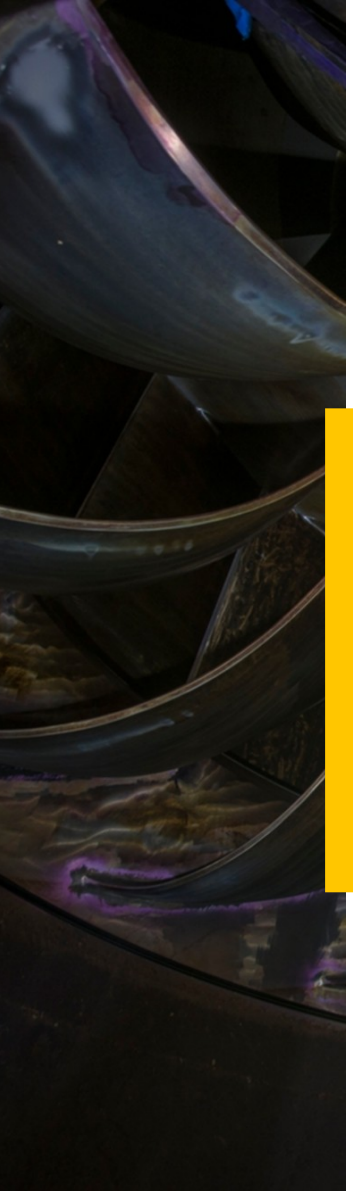
Systemer, teknologier, teknologileverandører, markedsutviklinger.

3 Hva gjør oss og verdikjedene våre til mål, nå og fremover? (Verdier og egenskaper)

Våre assets, adferd og organisatoriske trekk, lokasjoner, trussel mot våre leverandørkjeder og vår avhengighet til disse.

4 Hvordan vil vårt trusselbilde påvirkes av nasjonal og internasjonal sikkerhetspolitikk, samfunnsutvikling, sikkerhetstiltak? (Overordnet trusselbilde)

På hvilke måter er vi en del av det nasjonale? Hvilke perspektiver? Endring i kriminalitetsbilde, utvikling i lover, forskrifter og tiltak. Tolkning av nasjonale og andre vurderinger opp mot egne.



Bottom line

Nasjonale vurderinger kan ikke stå alene eller være primærgrunnlaget for trusselforståelse på sektor eller bedriftsnivå.

Sektorvist trusselbilde må bygges i sektoren.

Bedriftens trusselbilde må bygges lokalt.

Spørsmål?

Espen Nodeland, Etterretningsleder
espen.nodeland@kraftcert.no
cert@kraftcert.no
Dir: +47 95 73 25 48

kraftCERT

infraCERT