

Fra enkeltstående kontroller til operativ deteksjons- og responsevne

Ser vi det som betyr noe, forstår vi hva det betyr, og klarer vi å handle i tide?

KiNS tech 2026 | 30.SEP-01.OKT 2026



SOLUTION ARCHITECT

TAM (TECHNICAL ACCOUNT MANAGER)

15+ YEARS IN SECURITY



SECURITY ARCHITECTURE



SOC & MDR



CLOUD & IDENTITY



SECURITY ADVISORY

Start with the problem.
Not the product.

John-Helge Gantz

Jeg jobber der sikkerhetsarkitektur, styring og sikkerhetsdrift møtes.

Mer enn 15 år med sikkerhet i regulerte miljøer. I dag Solution Architect og teknisk kundeansvarlig (TAM) i NetNordic.

Jeg er særlig opptatt av avstanden mellom erklært sikkerhet og det som faktisk virker i drift.

Arkitektur

som tåler møtet med
drift

SOC og MDR

som en driftsmodell
med ansvar

Styring

som endrer
prioriteringer

Start med problemet, ikke produktet.

NetNordic: nettverk, sikkerhet og hendelseshåndtering

700+

fagfolk

17

lokasjoner

3000+

kunder

Nettverk og sikkerhet i samme fagmiljø

- Vi bygger, drifter og overvåker nettverk og infrastruktur
- Nordiske eksperter, data lagret kun i Norden
- Kortere vei fra varsel til aksjon

Hendelseshåndtering hele døgnet

- Egne analytikere på vakt 24/7/365, ikke bakvakt og ikke satt ut til andre
- Eget IR-team med digital etterforskning og malwareanalyse

2,3 min

til reaksjon

12 min

til løsning

9500+

reelle angrep stanset
siste 12 måneder

Når du trenger hjelp: 67 24 73 65

irhotline@netnordic.com



Investering i verktøy gir ikke automatisk evne til å oppdage

Det vi har

Lisensene er kjøpt

Hvem bruker dem hver dag?

Det vi har

Plattformen er avansert

Har vi kompetansen den krever?

Det vi har

Loggene strømmer inn

Er de normalisert og filtrert?

Det vi har

Innsamlingen er stor

Samler vi de riktige loggene?

Et tiltak som er kjøpt og installert, er ikke en operativ evne.

Evnen finnes først når noen kan se, forstå og handle.

Fiktivt scenario: 02:14, natt til søndag

En tjenestekonto i en kommune logger seg på fra et uvanlig sted. Ti minutter senere forsøker den å nå filservere i helse og omsorg. Serveren har en kjent sårbarhet, men det vet bare skanneren. Plattformen registrerer aktiviteten. Varselet havner i en kø sammen med mange andre, og ingen er på vakt før mandag.

Hvem ser det?

**Skiller noen det fra
støyen?**

Hvem kan stanse det?

Fem gap mellom verktøy og evne

01

Verktøy uten personell

Ingen har tid eller ansvar for å følge med

02

Verktøy uten kompetanse

Gode verktøy krever folk som kan bruke dem

03

Logger uten filtrering

Mye data, lite innsikt

04

Logger uten formål

Stor innsamling, uklart hvorfor

05

Spredt sikkerhetsbilde

Data i ulike verktøy korreleres ikke

Hvert gap alene kan gjøre et godt verktøy verdiløst i en reell hendelse.

Gap 1: Verktøy uten personell

Et verktøy ingen følger med på, beskytter ingen.

Tegn å se etter

- varsler blir liggende til noen har tid
- overvåkning i arbeidstid, angrep utenfor
- sikkerhet er en tilleggsoppgave i driften
- ingen eier gjennomgangen av varsler

Spørsmål å stille

- Hvor mange timer i uken brukes faktisk på å følge opp varsler?
- Hvem ser et kritisk varsel lørdag kl. 02:00?
- Hvem dekker ferie og sykdom?

Gap 2: Verktøy som krever kompetanse

Et godt verktøy passer ikke for alle virksomheter.

Hva verktøyet krever

Tilpasning, utvikling av deteksjoner, jevnlig justering og undersøkelse av hendelser.

Hva vi har

Hvor mange kan dette i dag, og hvem tar over når de er borte?

Hva som passer

Egen drift, delt tjeneste med andre kommuner, eller en leverandør med tydelig ansvar.

Riktig løsning er ikke alltid den nyeste. Den må kunne driftes over tid.

Gap 3: Mye logger, lite innsikt

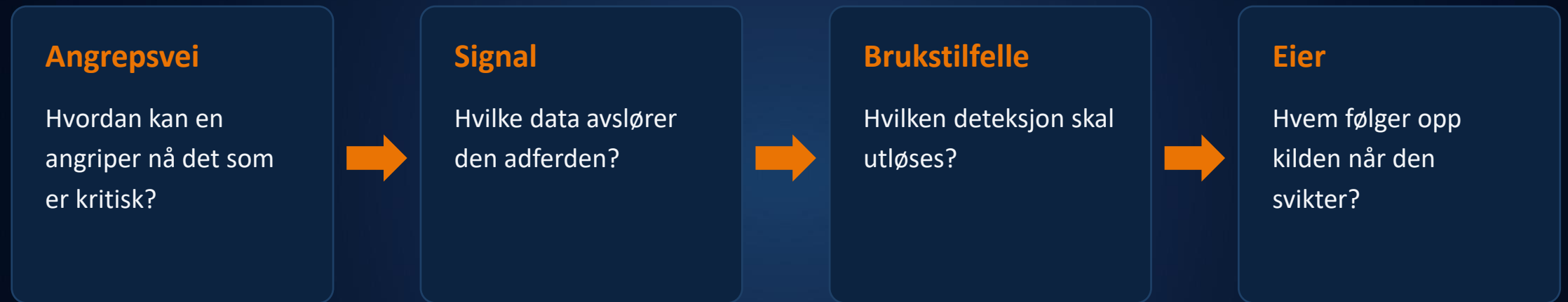
Uten normalisering og filtrering drukner vi i egne logger.

Tiltak	Hva det løser
Normalisering	Samme hendelse ser lik ut uansett kilde, og kan sammenlignes
Filtrering	Støy fjernes før den koster lagring og analytikertid
Berikelse	Varselet får kontekst: hvilket system, hvem eier det, hvor kritisk
Justering	Deteksjoner som bare gir falske alarmer, rettes eller fjernes

Flere varsler gir ikke mer sikkerhet. Når alt varsles, blir det viktigste lett oversett.

Gap 4: Riktige logger av riktige grunner

Samler vi de riktige loggene av de riktige grunnene?



For hver loggkilde bør vi kunne svare: hvilken angrepsvei avslører den, og hvem handler på den?

Gap 4: Deteksjonsdekning

En tilkoblet kilde er ennå ikke deteksjonsdekning.



Det er lett å stoppe på trinn 1 og rapportere det som dekning. Verdien ligger i trinn 3 og 4.

Gap 5: Spredt sikkerhetsbilde

Ser analytikeren hele bildet, eller bare det som når SIEM?

Kan ligge utenfor SIEM

- sårbarhetsdata i eget verktøy
- aktivaoversikt og kritikalitet
- identitet og tilganger
- EDR- og skyportaler med egne konsoller
- leverandørens egen overvåkning

Konsekvensen

Et varsel om innlogging mot en server blir ikke vurdert mot at samme server har en kjent, aktivt utnyttet sårbarhet.

Prioriteringen følger alvorlighetsgrad i hvert verktøy, ikke samlet eksponering.

Alt trenger ikke lagres i SIEM. Det som avgjør, er at sårbarhet, aktiva og identitet er tilgjengelig som kontekst når beslutningen tas.

Fra signal til handling

Døgntidvise overvåking gir ikke automatisk døgntidvis respons.

Leverandøren kan

- analysere og varsle
- isolere endepunkter etter avtalt fullmakt
- eskalere til hendelseshåndtering

Kommunen må beslutte

- å stenge en tjeneste innbyggerne trenger
- rekkefølgen for gjenoppretting
- varsling av myndigheter og innbyggere

I praksis blir fullmakten den reelle tjenestenivåavtalen.

Leverandøren drifter tjenesten. Kommunen eier konsekvensen.

Hvem hos leverandøren varsler oss, og hvem hos oss tar imot?

Hvilke signaler fra leverandørens miljø når fram til den som overvåker oss?

Har vi øvd på en hendelse sammen med leverandøren?

Regelverket peker samme vei

NSM

Grunnprinsipper for IKT-sikkerhet 2.1

Kategori 3, Oppdage, og kategori 4, Håndtere og gjenopprette, forutsetter tiltak som virker i drift.

Lov

Digitalsikkerhetsloven

I kraft fra 1. oktober 2025 og gjennomfører NIS1. Stadig flere deler av NIS2 vil også bli relevante for oss i Norge.

Etterlevelse viser at tiltak finnes. Den viser ikke alltid at de virker.

Fem spørsmål å ta med hjem

- 01** Hvem følger opp varslene våre, også utenfor arbeidstid?
- 02** Har vi kompetansen verktøyene krever, og hvem dekker fravær?
- 03** Ser vi sårbarheter, identitet og varsler i samme bilde?
- 04** Er loggene normalisert og filtrert før de når analytikeren?
- 05** Hvilken angrepsvei eller beslutning begrunner hver loggkilde?

Tre steg de neste 90 dagene

Dag 1 til 30

Kartlegg

Hvem som faktisk følger opp varsler, hvilken kompetanse som finnes, hvilke loggkilder som samles inn og hvorfor, og hvor sikkerhetsinformasjonen ligger.

Dag 31 til 60

Rydd

Filtrer eller fjern kilder uten formål. Juster deteksjoner som bare gir støy.

Dag 61 til 90

Avklar og øv

Bemanning, fullmakter og eskalering, skriftlig.

Test med en skrivebordsøvelse.

Sikkerhet må utformes, ikke erklæres.

Spørsmålet er om vi ser det som betyr noe, forstår hva det betyr og klarer å handle i tide.

John-Helge Gantz | jhg@netnordic.com | linkedin.com/in/johnhgantz/