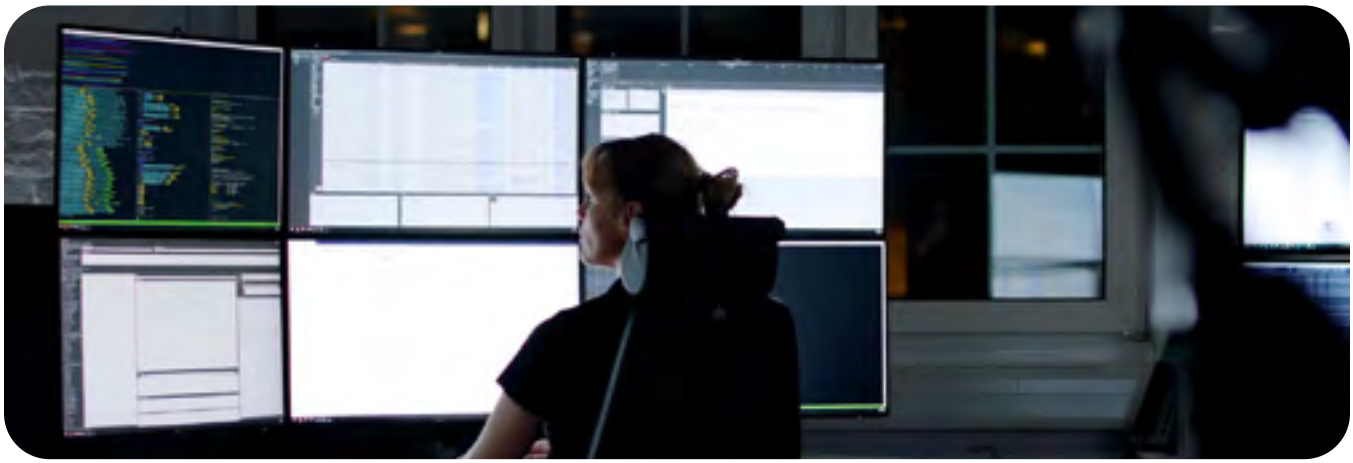
TUSSA IKT



MDR–SOC 247

Overvaking og varsling av kritiske hendingar heile døgnet, året rundt.

Tenesta overvåkar og analyserer aktivitetsloggar frå alle kritiske system. Tussa IKT si SOC-teneste gjev det du treng for å liggje i forkant av kritiske hendingar og angrep heile døgnet, året rundt.

Dei fleste cyberangrep skjer utanfor normal arbeidstid. Tida det tek før hendingar vert oppdaga er kritisk for å setje i verk tiltak og unngå nedetid og økonomiske tap.

Tenesta inkluderer overvaking av alt frå skymiljø som Microsoft Azure, Google Cloud Platform og AWS, til klientar og infrastruktur.

Analytikarane i SOC vil analysere, kategorisere og rapportere trusselhendingar, og isolere kompromitterte endepunkt og brukarkontoar etter avtalte kriteriar.

Tussa IKT står òg til teneste med handtering av truslar ved behov. For rask respons og profesjonell handtering tilrår vi òg tenesta Incident Response Team med 2 timar garantert responstid heile døgnet.

Dette får du med MDR–SOC 247:

- → Innsamling av loggar frå skymiljø, klientar og infrastruktur
- → Maskinell og manuell analyse
- → 24/7 SOC med analytikarar
- → Eigen portal med oversikt og rapportering
- → Varsling heile døgnet
- → Isolering av endepunkt ved kritiske hendingar
- → 12 månader lagring av loggar

Standard loggkjelder:

- → Microsoft 365
- → Microsoft Azure via Graph API
- → DNS og eventlogg på AD
- → Brannmurloggar
- → Trygg klient eller anna EDR-løysing*

* Sjå liste over støtta integrasjonar her

itsal@tussa.no

70 04 62 00