Er bedriften din klar for et security operations center?

eBook

SOC: Sjekkliste

2025 Desember I SOC Readiness Assessment

Har dere behov for et Security Operations Center (SOC)?

netnordic
THE BEST COMPANION

SOC:
Er bedriften din klar for et security operations center?

Cybersikkerhet har gått fra å være et IT-anliggende til å bli en sentral del av virksomhetsstyring. Trusselbildet utvikler seg raskt, kravene fra myndigheter og kunder blir strengere, og bedrifter forventes å ha dokumentert kontroll – ikke bare gode intensjoner.

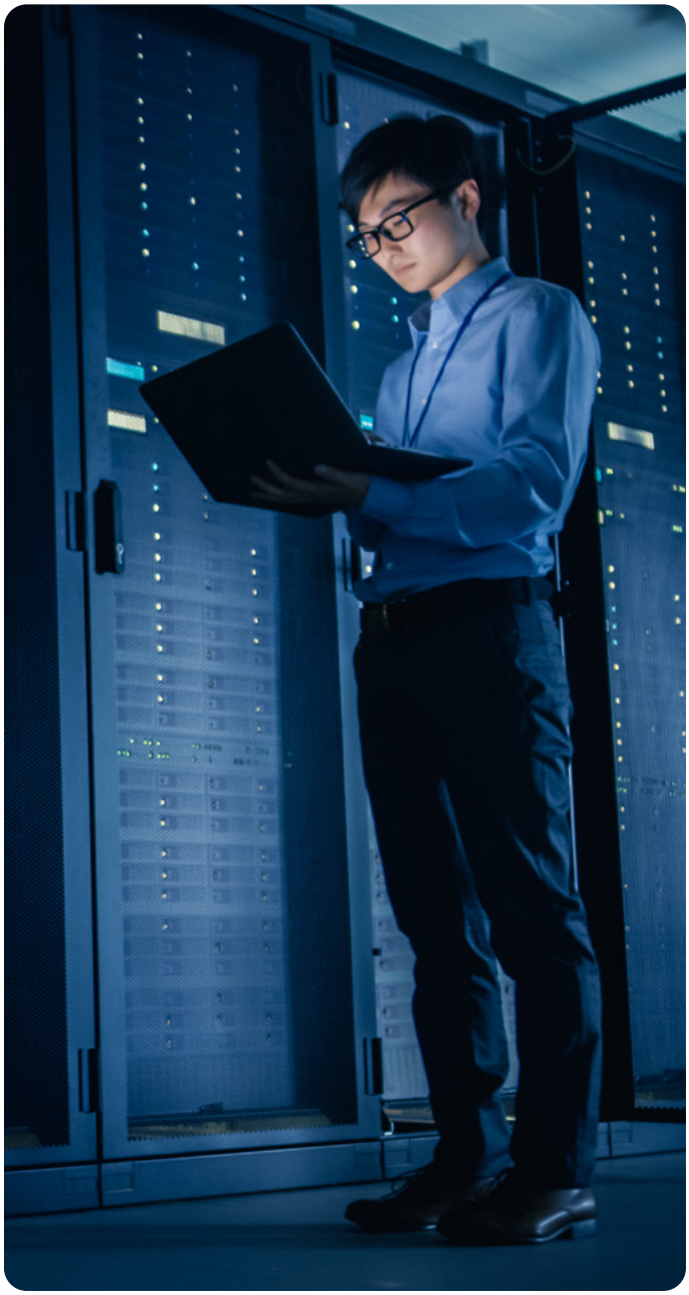
Men hvordan vet du egentlig hvor moden organisasjonen deres er? Og hvordan vet du om tiden er inne for å samarbeide med en partner på cybersikkerhet og om dere har behov for et Security Operations Center (SOC)?

For å gjøre dette enklere har vi laget en praktisk sjekkliste med 12 spørsmål som avslører om dere er klare for SOC.

SOC READINESS ASSESSMENT

Sjekkliste: 12 spørsmål som avslører om dere er klare for SOC

En strukturert gjennomgang av deres sikkerhetsstatus, ressurser, compliance og strategi



200+
Dager oppdagelsestid

10
Min med SOC-partner

24/7
Min med SOC-partner

Table of Content

01 Del 1: Dagens sikkerhetssituasjon

02 Del 2: Ressurser og kompetanse

03 Del 3: Compliance og forretningsrisiko

04 Del 4: Strategi og vekst

05 Hva svarene forteller dere

06 Hva kjennetegner en god SOC-partner?

Del 1: Dagens sikkerhetssituasjon

Spørsmål 1

Får dere et klart og entydig svar på: «Blir vi angrepet akkurat nå?»

- [ ] Ja, vi har full oversikt i sanntid ✓
- [ ] Vi får vite det innen noen timer !
- [ ] Det tar dager før vi eventuelt oppdager det x
- [ ] Vi vet egentlig ikke x

Gjennomsnittlig tid fra angrep til oppdagelse er fortsatt 200+ dager i mange organisasjoner. Bedrifter med god sikkerhetsdrift oppdager angrep i løpet av minutter, ikke måneder.

Spørsmål 2

Kan IT-avdelingen forklare styret hva som faktisk utgjør den største sikkerhetsrisikoen – på et språk styret forstår?

- [ ] Ja, klare og forretningsorienterte risikorapporter ✓
- [ ] Vi får tekniske rapporter som er vanskelige å tolke !
- [ ] Vi vet ikke hva styret trenger !
- [ ] Lite eller ingen rapportering x

Cybersikkerhet er et forretningsproblem. Uten forståelig rapportering kan dere ikke ta riktige beslutninger.

Spørsmål 3

Overvåker dere nettverket døgnet rundt, hver eneste dag?

- [ ] Ja, 24/7/365 ✓
- [ ] Kun i kontortiden !
- [ ] Vi får varsler, men ingen aktiv overvåking !
- [ ] Nei x

De fleste angrep skjer når bemanningen er lav – kveld, helg og høytid.

Spørsmål 4
Hvor lang tid tar det før noen responderer på en sikkerhetshendelse?

- [ ] Under 15 minutter ✓
- [ ] 1–4 timer !
- [ ] Innen neste virkedag x
- [ ] Ingen definert responstid x

Et angrep kan spre seg på under én time. Rask respons betyr alt.

Del 2: Ressurser og kompetanse

Spørsmål 5
Har dere utfordringer med rekruttering av cybersikkerhetskompetanse?

- [ ] Nei ✓
- [ ] Klarer det, men ressurskrevende !
- [ ] Ikke prøvd å rekruttere !
- [ ] Ja, svært vanskelig x

Det er stor mangel på sikkerhetskompetanse i Norge.

Spørsmål 6
Bruker IT-teamet tiden på brannslukking fremfor strategi?

- [ ] God balanse ✓
- [ ] Dedikerte team ✓
- [ ] Mye brannslukking !
- [ ] Ja x

Brannslukking stjeler tid fra innovasjon og forretningsutvikling.

Spørsmål 7
Har dere full oversikt over sikkerhetsverktøy og lisenser?

- [ ] Full oversikt ✓
- [ ] Mange verktøy, usikker utnyttelse !
- [ ] Overlappinger !
- [ ] Kaotisk x

Bedrifter betaler ofte for teknologi de ikke bruker effektivt.

Del 3: Compliance og forretningsrisiko

Spørsmål 8
Opplever dere økte sikkerhetskrav fra kunder og partnere?

- [ ] Ja, betydelig ✓
- [ ] Noen krav !
- [ ] Forventer økte krav !
- [ ] Nei x

Strengere krav er en del av moderne leverandørkjeder.

Spørsmål 9
Kan dere dokumentere sikkerhetsarbeidet deres?

- [ ] God dokumentasjon ✓
- [ ] Noe dokumentasjon !
- [ ] Spredt og ustrukturert !
- [ ] Ingen dokumentasjon x

NIS2 og GDPR krever dokumenterbar sikkerhetsdrift.

Spørsmål 10
Vet dere hva et alvorlig cyberangrep vil koste?

- [ ] Ja ✓
- [ ] Grov forståelse !
- [ ] Ikke regnet på det x
- [ ] Tror det ikke vil ramme oss x

Et alvorlig angrep koster ofte flere millioner.

Del 4: Strategi og vekst

Spørsmål 11
Hemmer dagens sikkerhet digitalisering eller vekst?

- [ ] Nei ✓
- [ ] Noe !
- [ ] Ikke ennå !
- [ ] Ja x

Sikkerhet skal muliggjøre vekst — ikke bremse den.

Spørsmål 12
Har dere en langsiktig plan for utvikling av cybersikkerheten?

- [ ] Ja, flerårig veikart ✓
- [ ] Uformelle planer !
- [ ] Tar det år for år !
- [ ] Ingen plan x

Cybersikkerhet er en kontinuerlig reise.

Hva kjennetegner en god SOC-partner?

Mest røde og gule avkrysninger?

Dere er klare for SOC — faktisk burde dere startet allerede.
En trinnvis modell med MDR → SOC gir rask verdi.

Litt blandet?

Mye er på plass, men hull må tettes.
En hybrid modell passer ofte best.

Mest grønne?

Sterkt nivå — men trusselbildet endrer seg.
Tid for strategimøte og videre modenhetsløft.

Hva kjennetegner en god SOC-partner?

- ✓ Vendor-uavhengighet
- ✓ Transparens og tydelig kommunikasjon
- ✓ Norsk kompetanse og lokal forståelse
- ✓ Dokumenterbar suksess — deteksjonstid < 10 min
- ✓ Skalerbar modell med trinnvis utviklingoptimization

Hvis du ønsker en vurdering av modenheten deres — eller hjelp til å se blindsoner, risiko og muligheter — tar vi gjerne en uforpliktende prat.

Vi ser på helheten, gir konkrete anbefalinger og hjelper dere med å finne en modell som passer virksomheten, uansett om veien går via MDR, hybrid overvåkning eller full SOC.

December 2025

Next Steps with NetNordic

NetNordic Group AS
www.netnordic.com

NetNordic Norway AS
Vollsvein 2B, 1366 Lysaker
salg@netnordic.no
+47 67 247 365

NetNordic Sweden AS
Rasundavägen 4, 169 67 Solna
sales.se@netnordic.com
+46 8 555 068 00

NetNordic Denmark A/S
Tobaksvejen 2a, 2860 Seborg
sales.dk@netnordic.com
+45 4331 4000

NetNordic Finland Oy
Linnoitustie 2 A, 02600 Espoo
sales.f@netnordic.com
+358 20 743 8000

netnordic
THE BEST COMPANION