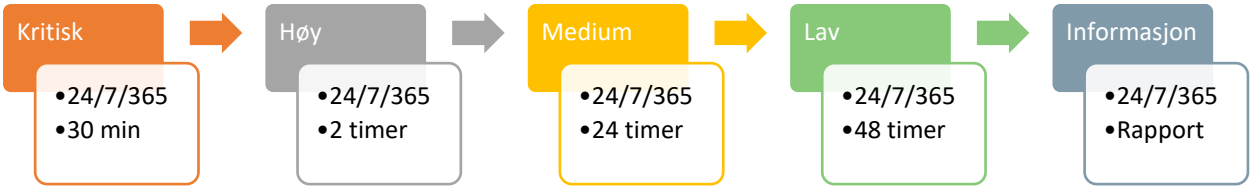
Tjenestenivå og vilkår

Digital vaktsentral

Tjenestenivå og vilkår Digital Vaktsentral

Standard avtale for tjenestenivå

Tilbudt overvåkningstjeneste er tilgjengelig for kundens utpekte personer alle dager, hele året, gjennom vårt 24/7/365 bemannede operasjonssenter. Underliggende og tilhørende tekniske løsninger understøtter denne operasjonelle tilgjengeligheten.
Kontaktinformasjon, varslingsmatriser og praktisk samarbeid utveksles og gås gjennom som en del av etableringen av tjenesten.
Leverandør bemannede operasjonssenter leverer følgende tjenestenivå / SLA som standard, for avdekkede sikkerhetshendelser og alarmer:
Vår garanterte undersøkelsestid for de forskjellige kritikalitetene:



Figur 1 - Tjenestenivå garantert undersøkelsestid

Utfyllende informasjon til tjenestenivå

1) Vår reaksjonstid vil i minimum 95% av alle alarmer og hendelser, grunnet automasjon, være på sekunder, og er inkludert i undersøkelsestiden.
2) Alle avdekkede hendelser og alarmer vil automatisk analyseres og vurderes av Leverandør. Resultatet av analysen vil kunne endre kritikaliteten, og tjenestenivået gjelder for den vurderte kritikaliteten etter vår analyse.
3) Inkludert i vår **undersøkelsestid** som presentert, er også den tekniske initielle responsen vi kan gjøre basert på bemyndigelse fra kunden og kapabilitetene i kundens løsninger.

Klassifisering av kritikaliteter for alarmtyper

Leverandørens automatiserte analyse av hendelser og alarmer vil sette kritikalitet etter følgende tabell.

	Klassifisering	
Type hendelse	Enterprise løsninger	Kritisk infrastruktur
Kompromittering av privilegert konto (Compromise of high privileged account)	Kritisk (Critical)	Kritisk (Critical)
Aktiv inntregning (Active intrusion)	Kritisk (Critical)	Kritisk (Critical)
Detektert inntregning (Intrusion)	Høy (High)	Kritisk (Critical)
Informasjons innholdssikkerhet (Information Content Security)	Høy (High)	Høy (High)
Forsøk på inntregning (Intrusion Attempts)	Medium	Høy (High)
Tilgjengelighet (Availability)	Medium	Kritisk (Critical)
Kompromitterte brukere (Compromised Users)	Medium	Kritisk (Critical)
Svindel (Fraud)	Medium	Medium
Rekognosering og informasjonsinnhenting (Recon / Information gathering)	Lav (Low)	Medium
Mistenkelige endringer (Suspicious Change)	Lav (Low)	Medium
Mistenkelig brukeraktivitet (Suspicious User Activity)	Lav (Low)	Medium
Ondsinnet kode som er stoppet/blokkert (Malicious code which has been blocked by system)	Lav (Low)	Medium
Støtende innhold (Abusive content)	Lav (Low)	Lav (Low)
Forbedringsområder – mulige fremtidige riski (Improvement areas/potential future risks)	Informasjon (Information)	Informasjon (Information)

Klassifiering av hendelser som beskrevet i SSA-L mappes på følgende måte:

- SSA-L kritikalitet A => Kritisk
- SSA-L kritikalitet B => Høy
- SSA-L kritikalitet C => Medium + Low + Informational

Ansvarsfordeling, alarmgrunnlag og begrensninger

1. Hva SLA-en gjelder

SLA-en for Digital Vaktsentral gjelder Eidsivas respons på sikkerhetsalarmer og hendelser som mottas i tjenesten fra kundens avtalte sikkerhetskilder.
Tjenesten er basert på overvåkning, vurdering, varsling og respons på relevante sikkerhetsalarmer i kundens Microsoft-miljø og eventuelle andre kilder som er særskilt avtalt.
SLA-en regulerer Eidsivas behandling av alarmer som mottas, klassifiseres og håndteres i tjenesten. Den er ikke en garanti for at alle sikkerhetshendelser oppdages, stoppes eller forhindres.

2. Alarmgrunnlag og synlighet

Digital Vaktsentral kan kun agere på alarmer, signaler og hendelsesdata som gjøres tilgjengelig for Eidsiva gjennom avtalte integrasjoner, tilganger og sikkerhetskilder.
Hva tjenesten kan oppdage, vurdere og håndtere, avhenger blant annet av:

- hvilke Microsoft-lisenser og sikkerhetsfunksjoner kunden har aktivert
- hvilke sikkerhetskilder som er inkludert i tjenesten
- hvilke alarmer som faktisk genereres av kundens miljø
- hvilke tekniske tilganger og fullmakter Eidsiva har fått
- kundens konfigurasjon, sikkerhetsnivå og datakvalitet
- eventuelle begrensninger i tredjepartsplattformer eller underliggende sikkerhetsverktøy

Det kan derfor oppstå sikkerhetshendelser som ikke genererer alarm, som ikke blir synlige for tjenesten, eller som ikke kan håndteres automatisk eller operativt gjennom Digital Vaktsentral.

3. Anbefalinger om alarmnivå

Eidsiva kan gi anbefalinger om kundens alarmgrunnlag, sikkerhetsnivå, lisenser, sensorikk, integrasjoner og tekniske forutsetninger.
Formålet med slike anbefalinger er å øke kvaliteten på alarmgrunnlaget og forbedre tjenestens evne til å oppdage, vurdere og håndtere sikkerhetshendelser.
Dersom kunden velger å ikke følge slike anbefalinger, kan dette redusere tjenestens effekt og Eidsivas mulighet til å oppdage eller håndtere hendelser.

4. Eidsivas ansvar

Eidsiva har ansvar for å levere Digital Vaktsentral i henhold til avtalt tjenestebeskrivelse, godkjente fullmakter og gjeldende SLA.
Eidsivas ansvar omfatter:

- mottak og vurdering av relevante sikkerhetsalarmer som inngår i tjenesten
- prioritering av alarmer etter alvorlighet
- varsling til kunden etter avtalt varslingsløp
- gjennomføring av avtalte sikkerhetstiltak der dette er teknisk mulig og innenfor godkjente fullmakter
- eskalering av alvorlige hendelser etter avtalt modell
- anbefalinger om forbedring av alarmgrunnlag og sikkerhetsnivå der dette er

elevant

Eidsiva skal utføre tjenesten med nødvendig faglig aktsomhet og i tråd med avtalte prosesser.

5. Kundens ansvar

Kunden har ansvar for at nødvendige forutsetninger for tjenesten er på plass og opprettholdes i avtaleperioden.

Kundens ansvar omfatter blant annet:

- å ha nødvendige Microsoft-lisenser og sikkerhetsfunksjoner aktivert
- å gi Eidsiva nødvendige tekniske tilganger og fullmakter
- å holde kontaktpersoner og varslingsløp oppdatert
- å sørge for at kundens IT-miljø er forsvarlig konfigurert og vedlikeholdt
- å følge opp anbefalinger fra Eidsiva der kunden ønsker økt alarmdekning eller bedre responsgrunnlag
- å håndtere ordinær IT-drift, lokal brukeroppfølging og interne beslutninger som ligger utenfor sikkerhetsresponsen

Manglende tilganger, fullmakter, kontaktpunkter eller tekniske forutsetninger kan påvirke Eidsivas evne til å levere tjenesten som avtalt.

6. Hendelser som ikke oppdages eller stoppes

Digital Vaktsentral reduserer risiko og styrker kundens evne til å håndtere sikkerhetshendelser, men tjenesten kan ikke garantere at alle trusler, angrep, misbruk, skadevare, datainnbrudd eller andre sikkerhetshendelser oppdages eller stoppes.

Det kan blant annet forekomme hendelser som:

- ikke genererer alarm i kundens sikkerhetsverktøy
- ikke omfattes av avtalte sikkerhetskilder
- ikke kan oppdages med kundens gjeldende lisens- eller sensorikk-nivå
- skjer før tjenesten mottar tilstrekkelige signaler
- utvikler seg raskere enn tilgjengelige responsmuligheter
- ligger utenfor Eidsivas tekniske tilgang eller godkjente fullmakter
- skyldes forhold i kundens miljø, drift, konfigurasjon, brukeratferd eller interne rutiner

7. Begrensning av ansvar

Digital Vaktsentral er en sikkerhetstjeneste som skal bidra til å redusere risiko og forbedre kundens evne til å håndtere sikkerhetshendelser. Tjenesten innebærer ikke at Eidsiva overtar kundens samlede ansvar for informasjonssikkerhet, IT-drift, risikostyring, etterlevelse eller forretningskontinuitet.

Eidsiva er ikke ansvarlig for indirekte tap, driftstap, tap av data, tap av omsetning, tap av fortjeneste, tap som følge av driftsavbrudd, krav fra tredjepart eller andre økonomiske konsekvenser av sikkerhetshendelser, uavhengig av om kunden har Digital Vaktsentral.

Eidsivas ansvar er begrenset til levering av tjenesten i henhold til avtalt tjenestebeskrivelse, gjeldende SLA og avtalte ansvarsbegrensninger.