# PRODUKTBESKRIVELSE

# DIGIFLOW SECURITY OPERATIONS CENTER

## 1. Leveransen

### 1.1 Leveranser som inngår i Tjenesten

**Sikkerhetsovervåkning**
Automatisk overvåkning av Kundens driftsmiljø for å avdekke mulige sikkerhetsproblemer. Inklusive overvåkning av nettverk, servere, databaser og tilknytningspunkter for å avdekke mulige trusler, forsøk på ulovlig inntrengning i Kundens systemer og andre sikkerhetsrisikoer.

**Oppfølgning, diagnostikk og gjenopprettinger**
Reparasjon av kompromitterte brukertilganger, bistand til Kundens brukere med gjenoppretting av tilganger, oppsett av nye passord mv. Innledende diagnostisering av årsaksforhold og konsekvenser ved dypere hackerangrep.

**Varslingsrutiner:**
Felles omforente varslingsrutiner blir utarbeidet i samarbeid med kunden ved etablering av tjenesten. Kontaktpersoner, eskaleringsrutinger mm vil være del av dette.
Alle saker som detekteres av Leverandør vil klassifiseres og kategoriseres og registreres mot gjeldende SLA. Avvik fra SLA eskaleres internt, og vil bli vurdert for kundens konsekvenser, før de meldes kunden etter avtalt metode.

**Rapportering:**
For tilbudt tjeneste vil det utarbeides regelmessige rapporter, sammenfallende med oppfølgingsmøter som beskrevet i tabellen for tjenestenivå.

# 2. SLA – Oversikt over tjenestenivå og garanti

## 2.1 Tjenestenivå

| | |
|---|---|
| **Servicetid** | 24/7/365 |
| **Tjenestens tilgjengelighet (oppetid innen servicetiden) *** | 99 % |
| **Sikkerhetsovervåking – Garantert responstid**<br>*Tiden er fra deteksjon, via analyse/beriking til respons.* | |
| «Kritisk» klassifiserte deteksjoner/mulige sikkerhetshendelser | 30 min |
| Høy klassifiserte deteksjoner/mulige sikkerhetshendelser | 2 timer |
| Medium klassifiserte deteksjoner/mulige sikkerhetshendelser | 24 timer |
| Lav klassifiserte deteksjoner/mulige sikkerhetshendelser | 48 timer |
| «Informasjon» klassifiserte deteksjoner/mulige sikkerhetshendelser | Rapport |
| **Oppfølgning, diagnostikk og gjenopprettinger – responstid **** | |
| Alle/flere brukere er påvirket ved at server eller applikasjon(er) er nede | Så fort som mulig etter deteksjon |
| Bruker får ikke gjort jobben sin og må ha rask hjelp | 1 time |
| Alle/flere brukere har redusert Servicenivå (noe jobb kan gjøres) | 1 time |

*Note* ** Nedetid som skyldes Kunden eller eksterne faktorer er utenfor garanti*
***Responstid for oppfølgning leveres i Serviceperioden, hverdager 0800-1600*

## 2.2 Kompensasjoner ved brudd på tilgjengelighet

Standardisert kompensasjon beregnes med utgangspunkt i samlet månedskostnad for tjenesten for den måned garantert tilgjengelighet ikke er levert. Kunden får automatisk kompensasjon i henhold til tabellen under for avvik fra krav til tilgjengelighet.

| Tilgjengelighet - avvik fra garantert nivå i % | Kompensasjon |
|---|---|
| 99,0 til 98 % | 5 % |
| 98 til 97 % | 10 % |
| 97 til 96 % | 15 % |
| 96 til 90 % | 20 % |
| Under 90 % | 30 % |

## 2.3 Klassifisering av kritikaliteter for alarmtyper

Digiflows 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) |

# 3. Tilleggstjenester

I tillegg til standard SOC-tjenester som beskrevet over, kan Digiflow tilby følgende konsulenttjenester på avtalt fastpris eller etter løpende timer:

## 3.1 Opplæring og sikkerhetstesting

- Opplæringsprogram i IT-sikkerhet og systembruk for nyansatte
- Årlige/jevnlige treningsprogram for gi ny kunnskap om sikkerhet og oppdatere kunnskap om programvare
- Phishing-tester, penetrasjonstester og andre former for sikkerhetstesting av organisasjonen

## 3.2 Bistand etter angrep

- Disaster Response Team
- Gjenopprettelse av slettede/korrumperte data etter angrep