| **Bilag 10.a – IT-sikkerhedsydelser** |
| --- |

Drift af Security Operations Centre (SOC)

[**Vejledning til Leverandøren**

Vejledning til Leverandøren er angivet med kursiv i skarpe parenteser som denne. Ud over denne generelle vejledning indeholder bilaget en række specifikke vejledningstekster til Leverandøren.

Leverandøren skal besvare de i dette Bilag 10.a angivne krav i Bilag 10.a.i ”Leverandørens løsningsbeskrivelse” med Leverandørens egen løsning på kravene.

Leverandøren skal ikke ændre i bilaget, medmindre dette specifikt er angivet i vejledning til Leverandøren, eller hvor det er markeret på anden vis.

I Kontrakten er der henvist til Bilag 10.a. IT-sikkerhedsydelser i følgende punkter:

* Punkt 19 (IT-sikkerhedsydelser)

Vejledning til Leverandøren slettes inden kontraktunderskrift.]

Indholdsfortegnelse

[1. Indledning 4](#_Toc127908408)

[1.1 Baggrund 4](#_Toc127908409)

[1.2 Kommunikation og samarbejde 4](#_Toc127908410)

[2. GENERELLE KRAV 5](#_Toc127908411)

[3. Krav til løsningens tekniske egenskaber 6](#_Toc127908412)

[4. Security Operatons Centre (SOC) 7](#_Toc127908413)

[5. SOAR (SECURITY ORCHESTRATION, AUTOMATION AND RESPONSE) 8](#_Toc127908414)

Underbilag

Bilag 10.a.i Leverandørens løsningsbeskrivelse

# Indledning

Dette bilag indeholder Kundens krav til it-sikkerhedsydelser som Leverandøren skal levere under Kontrakten, med henblik på at overholde de i Bilag 7 (Servicemål) fastlagte Servicemål for Leverandørens levering af sikkerhedsservices og eventuelle øvrige fastlagte sikkerhedskrav der fremgår af Bilag 12 (Sikkerhed).

Leverandøren skal i sin levering af Sikkerhedsservices til Kunden overholde og tilpasse sin løsning i henhold til Kundens kravspecifikation og opsætning, jf. bilag 3 (Kundens it-miljø).

Dette bilag fastsætter kravene til Leverandørens levering af sikkerhedsservices til Kunden, herunder proaktiv overvågning af it-sikkerheden og mitigering af potentielle og/eller aktuelle it-sikkerhedsrisici.

Leverandøren skal ved levering af Sikkerhedsservices yde rådgivning til Kunden inden for optimering af it-sikkerheden og de forskellige sikkerhedslag samt komme med forbedringsforslag til it-sikkerheden.

## Baggrund

Kunden ønsker at øge indsatsen indenfor it-sikkerhed gennem en lang række initiativer og sikkerhedsprojekter. Kunden ønsker at styrke sikkerheden generelt for både at sikre overholdelse af gældende lovgivning og for at kunne tilbyde muligheden for at sikre arbejdet med indsamling og bearbejdning af data til det yderste.

Kunden har i dag egen SOC og SIEM/SOAR og er ved at opbygge funktionalitet heri. Kunden forventer selv at kunne varetage en del af de opgaver, der ligger i en SOC, men har ikke tilstrækkelige ressourcer.

Som led i denne indsats ønsker Kunden at købe Security Operations Center (SOC) ”as-a-service”, som modtager og proaktivt analyserer/validerer logdata, og på baggrund heraf tilbageleverer færdigt analyserede og validerede alarmer (security incidents) fra den samlede løsning til Kunden.

Det er væsentligt, at løsningen kan levere relevante rapporter på flere niveauer jf. Bilag 8 Rapportering og indsigt.

## Kommunikation og samarbejde

Kundens SOC er bemandet på hverdage fra 8-16 og skal håndtere kommunikationen internt.

For nuværende består Kundens SOC af 2 fuldtidsansatte personer samt 2 tilknyttede personer, der deltager i SOC’en efter behov indenfor deres specialer.

Leverandøren skal primært kommunikere/samarbejde med Kundens SOC og kun i undtagelsestilfælde kommunikere med personer udenfor Kundens SOC.

Kommunikationen med Kundens SOC skal ske via Kundens SOC-postkasse (Exchange delt postkasse). Hvis et incident overstiger en aftalt alvorlighed, vil der være en telefonliste, der skal benyttes. Detaljer omkring hvorledes Kunden skal kontaktes aftales nærmere under implementeringen.

Nærmere omkring Governance findes i Bilag 4, herunder særligt i Bilag 4.a Samarbejdsorganisation og Bilag 4.b Allokerede nøglemedarbejdere.

# GENERELLE KRAV

Herunder følger Kundens generelle krav til Sikkerhedsservices, der skal leveres af Leverandøren.

*Scope for Sikkerhedsservices*

Leverandøren skal tilbyde Sikkerhedsservices til Kunden. Sikkerhedsservices omfatter bl.a. overvågning, forebyggelse, beskyttelse, trusselsvurdering, rådgivning og opklaring af hackerangreb og cyber-trusler.

*Leverandørens ansvar for SOC-opgaver ifm. sygdom, ferie og fridage*

Leverandøren skal ad hoc kunne overtage alle SOC-opgaver, som Kunden ellers ville varetage selv, til konsulenttimepris.

Vi vil have mulighed for at benyttes os dette i perioder, og ønsker at få tilbud på omkostningerne herved. Kontakt til Kunden vil være en nærmere aftalt telefonliste.

Kundens SOC er beskrevet i bilag 3 ”Kundens IT-miljø og situationsbeskrivelse”.

*Use Cases*

Leverandøren skal indledningsvis på Transitionsdagen levere implementering, drift og vedligehold af 20 Use Cases (forstået som MITRE Use Cases), der er mest relevante at implementere for Kunden ud fra en betragtning af det aktuelle risikobillede rettet imod uddannelses- og forskningssektoren.

Leverandøren skal efterfølgende levere implementering, drift og vedligehold af yderligere Use Cases (forstået som MITRE Use Cases), der yderligere er relevante – efter aftale med Kunden. Dette skal også ses som led i Leverandørens effektiviseringsforpligtelse jf. Bilag 16, herunder K-7 som anfører at Leverandøren er forpligtet til kontinuerligt at effektivisere indsatsen over kontraktperioden, så der løbende kan introduceres nye sikkerheds- og overvågningstiltag dvs. Leverandøren er forpligtet til at forbedre indsatsen og levere merværdi hen over kontraktperioden.

*Logkilder*

Leverandøren skal hente Logkilder til samtlige Use Cases som angivet i K-3 Use Cases.

*Leverandørens portal*

Leverandørens løsning giver adgang til brugerinterface og visuelle dashboards, hvor Kundens medarbejdere har muligheder for at kunne arbejde med operationelle, sikkerheds- og compliancedata.

*Rollebaseret adgang til portalen*

Det er et krav, at portaladgang og adgang til løsningen i øvrigt er rollebaseret, og at al adgang og alle aktiviteter monitoreres og logges i en for kunden tilgængelig form. Leverandøren skal sikre overvågning af disse logs og straks reagere i fald der konstateres uregelmæssigheder.

*Multifaktor autentifikation*

Det er et krav, at der benyttes multifaktor autentifikation overalt i løsningen, også i forbindelse med Kundens adgange, f.eks. til portalen.

*SSO og MFA*

Kunden benytter MS Azure AD og MS Authenticator og ønsker at benytte dette til SSO og som MFA i forbindelse med Kundens adgang til Portalen.

*Kontrol med konti*

Det er et krav, at Leverandøren aktivt kontrollerer den fulde livscyklus for løsningens system- og applikationskonti og konti relateret til log collectors, herunder oprettelsen, brugen af, midlertidig inaktivering og sletning, med det formål at minimere risikoen for, at konti kan udnyttes til cyberangreb.

*Minimering af falsk positive*

Det er et krav, at Leverandøren og Kunden i et løbende samarbejde sigter mod at nedbringe antallet af falske positiver, ved validerede alarmer.

*Træning af Kundens medarbejdere*

Kunden ønsker en beskrivelse af et muligt træningsforløb forud for en idriftsættelse af løsningen, hvor Kundens SOC øver sig på Kundens reelle data med henblik på at kunne efterprøve Operating Procedure. Træningsforløbet skal være inkluderet i de indledende ydelser.

*Automatisk sletning af Kundens data*

Det er et krav, at data i løsningen kan slettes automatisk efter f.eks. tid eller bestemte handlinger. Den maksimale Retention Time er 6 måneder.

# Krav til løsningens tekniske egenskaber

*Leverandørens systemarkitektur*

Leverandøren skal levere en beskrivelse af systemarkitekturen, herunder hvordan den er gjort robust. Dette leveres som en del af dokumentationen i forbindelse med tilbudsafgivelse.

*Indsamling af logs*

Det er et krav, at løsningen kan indsamle logs i Kundens eksisterende infrastruktur.

*Log fra klienter*

Leverandøren skal indsamle logs fra klienter, herunder fra klienternes MS Defender antivirus.

*Robust dataopsamling*

Løsningens dataopsamling er robust og kan imødegå f.eks. tab af netværksforbindelse eller tilsvarende.

*Reaktion ved manglende log*

Leverandøren skal overvåge logkilderne. Hvis Kundens logkilder stopper med at sende data, skal Leverandøren advisere Kunden i henhold til forud aftalt procedure ad aftalte kanaler og med overholdelse af aftalte reaktionstider jf. Bilag 7 Servicemål.

*Sikker overførsel af logs*

Leverandøren skal i samarbejde med Kunden sikre nødvendig kryptering af logs End-to-End for at opretholde integritet af data.

*Log integritet*

Leverandøren skal sikre, at opsamlede logdata er på en form, så de kan benyttes som bevismateriale i forbindelse med en eventuel sag ved en myndighedsinstans eller domstol.

*Analyse af log i realtid*

Løsningen skal basere sig på realtidsanalyse af logdata for at sikre hurtigst mulige detektionstid.

*Analyse af flowdata fra netværkstrafik*

Løsningen skal understøtte analyse af flowdata fra routere.

# Security Operatons Centre (SOC)

*Security Operations Centre*

Leverandøren skal etablere og drive en SOC der er tilgængelig 24/7/365.

SOC har til formål at registrere, opbevare og behandle sikkerhedshændelser i et centralt system, som er tilgængeligt for udvalgte medarbejdere hos Kunden. Leverandøren skal sikre at alle sikkerhedshændelser behandles på en ensartet og effektiv måde henset til de aktuelle eller potentielle it-sikkerhedsmæssige konsekvenser som sikkerhedshændelser kan medføre. Leverandøren skal sikre at SOC opfylder følgende krav:

1. At SOC altid er bemandet med kvalificerede medarbejdere der besidder den nødvendige uddannelse og de nødvendige kompetencer til at opdage, prioritere og analysere sikkerheds-hændelser på en effektiv og hensigtsmæssig måde.
2. At SOC er i stand til at opdage trusler på alle sikkerhedslag og -niveauer i Kundens it-miljø.
3. At SOC er i stand til at prioritere alle sikkerhedshændelser og anskaffe eller opnå de nødvendige digitale bevismaterialer til analysering af sikkerhedshændelser med henblik på forebyggelse, bekæmpelse og mitigering af fremtidige sikkerhedshændelser af samme eller lignende art.
4. At SOC er i stand til omgående at opdage, stoppe, udbedre og afhjælpe sikkerhændelser samt foretage den nødvendige gendannelse, hvis det måtte være nødvendigt.
5. Sikre overvågning af sårbarheder.
6. At SOC har en etableret proces og faste procedurer inden for kontinuerlige forbedringer af SOC med henblik på løbende at automatisere, forbedre og optimere SOC og de tilknyttede arbejdsopgaver mest muligt.

*Penetrations-, trussels- og sårbarhedsscanning*

Scanning af Kundens internt og eksternt netværk skal udelukkende foretages af Kundens egen SOC. Resultaterne fra scanninger af Kundens it-miljø skal proaktivt benyttes og analyseres af leverandørens SOC i overensstemmelse med kravene til Sikkerhedsservices.

*Vidensdatabase*

Leverandøren skal opbygge og vedligeholde en detaljeret vidensdatabase om, og forståelse for, Kundens infrastruktur specifikt omkring den tilbudte løsning, men også i forhold til nærtliggende integrationsområder som Netværk, Netværkssikkerhed, Datacenter, Microsoft Defender platformen, MS Sentinel og applikationslandskab. Dette skal sikre, at leverandørens SOC forstår Kundens kontekst og dermed yder en bedre support og klassifikation af sikkerhedshændelser.

*Single Point of Contact*

Kunden skal have et Single Point of Contact (SPOC) til Leverandørens SOC.

*Om incidents registreret af Kunden*

Registrerer Kunden Incidents, der tilsyneladende er inden for Leverandørens ansvar, rapporteres disse til Leverandøren. Det er et krav, at Leverandøren skal yde bistand til diagnosticering og afhjælpning af det rapporterede Incident.

Ved indrapportering skal Kunden oplyse følgende:

* Kundens beskrivelse.
* Angivelse af den eller de funktioner, der er påvirket.
* Fejlforstyrrelse og kategorisering.
* Tidspunkt for rapporteringen.
* Impact for Kundens installation.

# SOAR (SECURITY ORCHESTRATION, AUTOMATION AND RESPONSE)

Kunden ønsker at løsningen inkluderer ”Security Orchestration, Automation and Response” (SOAR) funktionalitet, så der kan opnås automatisk respons på sikkerhedshændelser (som automatisk nedlukning af firewalls, klienter etc.).

*SOAR-løsning*

Leverandørens skal anvende et SOAR-system som understøtter Kundens forretningsgange som angivet i nærværende krav.

SOAR-systemet dækker følgende funktionalitet:

* Automation & opsætning
* Incident/Case håndtering
* Interactive undersøgelse
* Threat Intel/IoC håndtering og administration
* Automatiseret threat hunting
* Machine learning til at understøtte yderligere automation af processer

Tilbudte løsning skal understøtte Kundens IT-miljø jf. ”Bilag 3 Kundens IT-miljø og situationsbeskrivelse”.

*SOAR Integration*

SOAR-systemet skal kunne integreres med Kundens forskellige sikkerhedsmiljøer, herunder log systemer, logs fra sikkerhedsprodukter der kan afgive logs, SIEM systemer, samt EDR- og XDR-komponenter fra forskellige leverandører.

*Mitigerende handling via standard API’er*

SOAR skal kunne udføre mitigerende handlinger i Kundens infrastruktur baseret på standard API’er. En handling kan f.eks. være at isolere en inficeret klient fysisk fra nettet gennem port kontrol.

*Rollebaseret adgang*

SOAR skal understøtte rollebaseret adgang.

*Integrerede sårbarhedsskanninger*

Data fra sårbarhedsscanninger skal kunne integreres direkte i løsningen.

*Integrationspakker*

Der skal være tilknyttet en markedsplads til SOAR-produktet, som giver adgang til mange integrationspakker til forskellige kategorier af produkter og herunder AU’s kritiske infrastruktur komponenter.

* Standard integrationspakker skal være tilgængelige for:
  + Microsoft Defender for Endpoint
  + Microsoft Defender for Identity
  + Microsoft Defender for O365
  + Microsoft Azure Sentinel
  + Cisco ISE
  + Cisco Umbrella
  + Cisco Firepower
  + NSX firewall miljø

*Understøttelse af Kundens IT Service Management system (ITSM-system)*

Det er et ønske, at Leverandørens løsning understøtter Cherwell Service Management REST API, som giver mulighed for integration til løsningen, specielt med henblik på håndtering af incidents. Assistance til bistand til integration til ITSM-systemet, afregnes i henhold til den tilbudte timepris på konsulentydelser.

*Indsamling af logs fra Kundens cloud-services*

Det er et krav, at løsningen kan opsamle logs fra cloud-services, herunder specielt – men ikke afgrænset til – Microsoft Azure og AWS. Ved logopsamling benyttes native cloud API’er.

Kunden har i øjeblikket ingen opsamling af logs fra Microsoft Azure (ud over AAD/ADFS) og AWS.

*Integration af Kundens MS Defender miljø og SIEM*

Kundens nuværende MS Defender miljø og SIEM (MS Sentinel) skal kunne integreres i SOAR-systemet hvori der opsamles øvrige logs til understøttelse af detektering og kontekst for den samlede detektering samt compliance.

*Threat Intelligence (TI)*

SOAR-systemet skal indeholde Threat Intelligence (TI) fra multiple kilder.

Der skal anvendes Threat Intelligence (TI) fra både OSINT og kommercielle kilder.

Bilag 10.a.i - Leverandørens løsningsbeskrivelse

Drift af Security Operations Centre (SOC)

***[Vejledning til Leverandøren***

*Her skal Leverandøren besvare nedenstående konkurrenceparametre]*

*Evalueringen af underkriteriet vil bero på en samlet konkret vurdering af, hvordan Leverandøren har beskrevet tilbudte løsning, samt hvorledes de beskrevne arbejdsgange komplementerer hinanden og sikrer en effektiv opgaveløsning på et passende niveau under hensyn til opgavens omfang og kompleksitet. Leverandørens eventuelle meropfyldelse af et krav vægter ligeledes positivt hvis Kunden vurderer dette som værende et positivt supplement til det krævede jf. forrige sætning.*

| Krav ID | Tildelingskriterium – Sikkerhedsydelser |
| --- | --- |
| Generelt | Leverandøren skal levere en beskrivelse af systemarkitekturen, herunder hvordan den er gjort robust.  Beskrivelsen indgår i den samlede vurdering af Tildelingskriteriet |
| Besvarelse: [Leverandørens besvarelse] | |
| K-5 | Leverandørens Portal  Leverandøren bedes beskrive, hvordan Leverandørens løsning giver adgang til brugerinterface og visuelle dashboards, hvor Kundens medarbejdere har muligheder for at kunne arbejde med operationelle, sikkerheds- og compliancedata.  Det vægter positivt, at   * Leverandørens løsningsforslag demonstrerer på et indsigtsfuldt og effektiv vis, at medarbejdere får mulighed for at kunne arbejde med operationelle, sikkerheds- og compliancedata. |
| Besvarelse: [Leverandørens besvarelse] | |
| K-8 | SSO og MFA  Leverandøren bedes beskrive, hvilke muligheder Leverandørens løsning giver for SSO og MFA, herunder hvilke muligheder der er for at benytte Kundens eksisterende miljø som er MS Azure AD og MS Authenticator.  Det vægter positivt, at   * Leverandørens løsningsforslag giver en høj grad af sikkerhed, ved f.eks. at benytte Kundens eksisterende IT-miljø eller at løsningsforslaget demonstrerer en højere grad af sikkerhed end dette setup, uden at Kunden skal erhverve yderligere licenser til andre løsninger. |
| Besvarelse: [Leverandørens besvarelse] | |
| K-11 | Træning af Kundens medarbejdere  Leverandøren bedes beskrive træning af Kundens medarbejdere.  Kunden ønsker en beskrivelse af et muligt træningsforløb forud for en idriftsættelse af løsningen, hvor Kundens SOC øver sig på Kundens reelle data med henblik på at kunne efterprøve Operating Procedure. Træningsforløbet skal være inkluderet i de indledende ydelser.  Det vægter positivt, at   * Leverandøren har et dybdegående, tilstrækkeligt og efterprøvet træningsforløb som sandsynliggør at Kunden bliver i stand til at bruge de værktøjer som Leverandøren tilbyder. |
| Besvarelse: [Leverandørens besvarelse] | |
| K-15 | Log fra klienter  Leverandøren bedes beskrive dennes tilbudte indsamling af logs fra klienter, herunder fra klienternes MS Defender antivirus.  Der ønskes en beskrivelse af vejen frem mod en øget log-indsamling fra klienter (Windows, Mac, Linux), herunder værktøjer, udrulning og logopsamling. En del af beskrivelsen kan være en tids- og aktivitetsplan for udruldningen.  Det vægter positivt, at   * Leverandørens beskrivelse demonstrerer en effektiv indsamling af logs fra de anførte klienter, herunder leverandørens værktøjer, eksempler på kvaliteten af logs, dvs. at Leverandøren sandsynliggør at det er relevante logs der indsamles. * Leverandørens beskrivelse inkluderer en tids- og aktivitetsplan efter uge 27 (Transitionsdagen) som tydeliggør udrulningshastigheden og processen herfor. |
| Besvarelse: [Leverandørens besvarelse] | |
| K-21 | Analyse af flowdata fra netværkstrafik  Leverandøren bedes beskrive, hvordan denne understøtter analyse af flowdata fra routere.  Kunden ønsker en løsning med mulighed for analyse af netværkstrafik på baggrund af en dybere inspektion af datapakker (f.eks. via Snort/Suricata, gennem analyse af opsamlet datastrøm eller ved fangst af data med henblik på efterfølgende sandbox-analyse).  Det vægter positivt, at   * Leverandørens løsning indeholder analyse af netværkstrafik, herunder graden heraf og mulighederne herfor. * Leverandørens løsning indeholder beskrivelse af hvilke muligheder der er for at skalere analyserne af netværkstrafikken, hvis denne er begrænset. |
| Besvarelse: [Leverandørens besvarelse] | |
| K-22 | Leverandørens SOC  Leverandøren skal beskrive hvordan Leverandøren vil drive sin SOC og sikre den nødvendige kommunikation til Kunden i forbindelse med sikkerhedshændelser.  Leverandøren skal ligeledes beskrive hvordan Leverandøren klassificerer og prioriterer sikkerhedshændelser samt hvordan Leverandøren indhenter pålideligt og sikkert digitalt bevismateriale.  Det vægter positivt, at   * Leverandørens procedurer har en høj grad af systematisering og automatisering der sikrer en hurtig reaktionstid og en effektiv mitigering af sikkerhedshændelser. * Leverandøren har faste procedurer for indsamling af digitalt bevismateriale, der istandgør Parterne til at foretage de nødvendige sikkerhedstiltag over for gerningspersonen eller gerningspersonerne. |
| Besvarelse: [Leverandørens besvarelse] | |
| K-22 | Leverandørens sikkerhedsovervågning  Leverandøren skal beskrive hvordan Leverandøren via SOC vil sikre Kundens it-miljø og data mod trusler, sårbarheder og sikkerhedshændelser.  Leverandøren skal beskrive hvordan Leverandøren proaktivt vil overvåge Kundens it-miljø, ~~hvor ofte der vil foretages sårbarhedsscanninger,~~ procedurer og processer for vurdering af sårbarheder samt gennemførelse af mitigerende handlinger eller opdateringer på baggrund heraf. Leverandøren skal også beskrive hvordan Leverandøren effektivt vil korrelere og prioritere sårbarhedshændelser. Ved mitigerende handlinger forstår Kunden, at Leverandøren henvender sig med anbefalinger, via de aftalte kanaler.  Det vægter positivt, at   * Leverandørens procedurer har en høj grad af systematisering og automatisering. * Leverandøren har en proaktiv tilgang til overvågning af sårbarheder. * Leverandøren er i stand til at sikre hurtige og effektive mitigerende handlinger med minimal påvirkning af Kundens Brugere. * Leverandøren leverer hyppige og informative anbefalinger og at Leverandøren kan vise processen og hvorledes format på anbefalingerne vil være. |
| Besvarelse: [Leverandørens besvarelse] | |
| K-33 | Understøttelse af Kundens IT Service Management system (ITSM-system)  Leverandøren bedes beskrive, hvilke muligheder der er for at understøtte Cherwell Service Management REST API, herunder specielt med henblik på håndtering af incidents.  Det vægter positivt, at   * Leverandørens løsningsforslag understøtter Cherwell Service Management REST API som giver mulighed for integration hertil, herunder specielt med henblik på håndtering af incidents. |
| Besvarelse: [Leverandørens besvarelse] | |
| K-34 | Indsamling af logs fra Kundens cloud-services  Leverandøren bedes beskrive indsamling af logs fra Kundens cloud-services.  Det vægter positivt, at   * Leverandørens løsningsforslag sandsynliggør at det er simpelt og effektivt, at indsamle logs fra Kundens cloud-services. |
| Besvarelse: [Leverandørens besvarelse] | |
| K-36 | Threat Intelligence (TI)  Leverandøren bedes beskrive hvilke Threat Intelligence kilder Leverandøren benytter, herunder hvorfor kilden er valgt og relevant for Kunden.  Det vægter positivt, at   * Leverandørens løsningsforslag indebærer at der anvendes brede og multiple kilder, herunder at beskrivelsen sandsynliggør at kilderne er relevante og dækkende for Kunden. |
| Besvarelse: [Leverandørens besvarelse] | |