Dodatek č. 1
ke smlouvě na dodávku a poskytování služeb

č. 056166/1

(dále jen „Dodatek č. 1")

mezi

ČEPRO, a.s.
se sídlem: Praha 7, Dělnická 213/12, Holešovice, PSČ 170 00
IČ: 60193531
DIČ: CZ60193531
zapsaná: v OR Městského soudu v Praze, oddíl B, vložka č. 2341
jednající: Mgr. Jan Duspěva, předseda představenstva a
Ing. František Todt, člen představenstva
oprávněni v rámci uzavřené Smlouvy jednat ve věcech Smlouvy bez oprávnění k jejím změnám:
[redacted]

(dále jen „**Objednatel**")

a

Corpus Solutions a.s.
se sídlem: Štětková 1638/18, Nusle, 140 00 Praha 4
IČO: 25764616
DIČ: CZ25764616
č. účtu: 69474001/5500
zapsaná: v obchodním rejstříku vedeném u Městského soudu v Praze, sp. zn. B 5936
jednající: Ing. Tomáš Přibyl, jednatel
oprávněni komunikovat v rámci uzavřené Smlouvy ve věcech Smlouvy bez oprávnění k jejím změnám:
[redacted]

(dále jen „**Zhotovitel**")

Objednatel a Zhotovitel (dále též „**Strany**", každý jednotlivě jako „**Strana**") níže uvedeného dne, měsíce a roku uzavírají tento Dodatek č. 1 ke smlouvě na dodávku a poskytování služeb č. 056166, uzavřené mezi Stranami dne 24. 8. 2022, (dále též jen „**Smlouva**") v následujícím znění:

Preambule

Objednatel na základě interních cvičení v rámci prověření nastavení kybernetické bezpečnosti společnosti a v souvislosti se stoupajícím počtem různých typů kybernetických útoků dospěl ke zjištění, že je potřeba zvýšit kybernetickou ochranu společnosti, a to formou rozšíření provozní doby služby pro analýzu kybernetických událostí a incidentů na režim 24/7 a přidání služby Incident Manažer. Vzhledem k tomu, že služba Incident Manažer je služba zcela nová, bude řešena na projektové bázi, aby mohla být nastavena dle specifických potřeb Objednatele.

1. Předmět tohoto dodatku

1.1. Objednatel má zájem o úpravu provozu služby pro řešení kritických incidentů na režim 0:00 – 24:00 hod. pro službu „analýza kybernetických událostí a incidentů" a stejně tak pro službu „řešení incidentů". Úpravy uvedených služeb budou učiněny formou nového vyhotovení přílohy č. 6 Smlouvy.

1.2. Objednatel má zájem o rozšíření a současně propojení stávajících služeb bezpečnostního dohledu s novou službou „SOC – Incident Manažer". Smluvní strany se dohodly na tom, že pro poskytování služeb bezpečnostního dohledu v rozšířeném znění včetně zejména vypracování reakčních scénářů kybernetických hrozeb pro interní prostředí Objednatele, revizí stávajících interních procesů a zhotovením související dokumentace bude nutné dobře poznat interní prostředí Objednatele, a proto bude tato činnost realizována formou projektu – „Aktualizace a dodávka služeb bezpečnostního dohledu" (dále jen „**Projekt II**"). Parametry Projektu II. a nastavení, popis a podmínky nové služby SOC-Incident Manažer jsou obsaženy v příloze č. 2 Dodatku č. 1 a tvoří novou přílohu č. 15 Smlouvy.

1.3. Smluvní strany se zavazují nejpozději po dokončení Projektu II upravit Smlouvu bez zbytečného odkladu formou dalšího písemného dodatku, neboť v rámci Projektu II a na základě interního auditu služeb bezpečnostního dohledu poskytovaných Zhotovitelem dle Smlouvy, budou zrevidovány, popsány a přenastaveny tyto Služby tak, aby lépe odpovídaly současnému faktickému stavu poskytování Služeb Zhotovitelem, došlo k jejich propojení s novou službou SOC-Incident Manažer a byly dále upraveny nové definice a pojmosloví či nově upraveny stávající definice a pojmosloví Smlouvy pro všechny typy Služeb. Hlavním záměrem těchto úprav je jasně stanovit zejména zahájení a ukončení jednotlivých poskytovaných Služeb spolu se stanovením konkrétního stavu a výstupu, kterého má být v rámci jednotlivých kroků příslušné Služby dosaženo, vše doplněné o výstupy z Projektu II tak, aby měl Objednatel zajištěnou co nejvyšší možnou míru kybernetické ochrany a bezpečnosti společnosti. Za výše uvedeným účelem Smluvní strany připravily předběžné podklady s názvem Katalogové listy, které jsou přílohou přílohy č. 15 Smlouvy a budou také použity pro úpravy Smlouvy ve smyslu ujednání uvedených v tomto Dodatku č. 1.

1.4. Smluvní strany upravily nově svoje kontaktní údaje a nové znění přílohy č. 9 Smlouvy – Kontaktní údaje tvoří přílohu č. 3 tohoto Dodatku č. 1.

1.5. Smluvní strany přečíslovaly služby uvedené v příloze č. 7 – Služby údržby a technické podpory, a to tak, že služby jsou nově číslovány od čísla 1. Nové znění přílohy č. 7 Smlouvy tvoří přílohu č. 4 tohoto Dodatku č. 1.

2. Článek 1

Preambule se doplňuje o odstavec (C) s následujícím zněním:

„Objednatel má zájem na rozšíření provozní doby některých Služeb a doplnění Služeb bezpečnostního dohledu o novou službu Incident Manažera na základě realizace nového projektu s názvem – „Aktualizace stávajících a dodávka nových služeb bezpečnostního dohledu" (dále jen „**Projekt II**"). Popis Projektu II, cíle Projektu II, obsazení realizačního týmu Projektu II, akceptační testy a kritéria a harmonogram plnění včetně nastavení, popisu a podmínek poskytování nové služby SOC-incident manažer budou upraveny formou přílohy č. 2 tohoto Dodatku č. 1, která tvoří přílohu č. 15 Smlouvy.

Odstavec 2.1 článku 2 Smlouvy se mění následujícím způsobem:

*„2.1 Za podmínek sjednaných v této Smlouvě se Zhotovitel zavazuje na svůj náklad a nebezpečí provést pro Objednatele Projekt, jehož specifikace je uvedena v Příloze č. 1 Smlouvy, spočívající v dodání, Instalaci a Implementaci Nástrojů do Prostředí Objednatele v Lokalitách, Zaškolení a zahájení poskytování Služeb a dále v realizaci Projektu II, jehož specifikace je uvedena v Příloze č. 15 (vše dále jen „**Dílo**") a Objednatel se zavazuje řádně provedenou Dílčí část Díla převzít a zaplatit za něj Cenu uvedenou v Článku 8.1 Smlouvy."*

Odstavec 2.2 článku 2 Smlouvy se doplňuje o nové písmeno (h) v následujícím znění:

„(h) realizace Projektu II"

Odstavec 3.1 článku 3 Smlouvy se mění následujícím způsobem:

- *„3.1 Účelem této Smlouvy je zajistit pro Objednatele splnění Projektu a Projektu II, tudíž vytvoření systému zajišťujícího bezpečnostní dohled ICT a OT Objednatele a to pomocí*

implementovaných Nástrojů, které zajistí komplexní monitoring ICT/OT prostředků, bezpečnostní monitoring činností koncových zařízení, sledování datového provozu informační infrastruktury a které budou detekovat útoky na prostředky ICT/OT v sítích Objednatele v daných Lokalitách, odhalovat případné interní a externí útočníky a či nestandardní chování a poskytovat službu bezpečnostního monitoringu, podporu pro vyšetřování a reakci na kybernetické události a poskytnout roli Incident Managera pro řešení nejzávažnějších kybernetických incidentů s vysokým dopadem na chod společnosti Objednatele, cílem Projektu II je zejména navrhnout, připravit a zajistit dodání aktuálních reakčních scénářů na 10 druhů kybernetických hrozeb relevantních pro prostředí Objednatele (v kombinaci IT i OT prostředí). "

Odstavec 4.1 a 4.2 článku 4 Smlouvy se mění následujícím způsobem:

„4.1 Dílo a Dílčí části Díla bude Zhotovitel provádět v termínech sjednaných v Příloze č. 8 a v Příloze č. 15.
4.2 Zhotovitel se zavazuje provést Dílo a jednotlivé Dílčí části Díla vždy tak, aby předání a převzetí Díla či Dílčí části Díla bylo dokončeno nejpozději v den, který je uveden pro příslušnou Dílčí část Díla v Příloze č. 8 a Příloze č. 15."

Odstavec 5.2 článku 5 Smlouvy se mění následujícím způsobem:

„5.2 Zhotovitel je povinen zajistit, že ke dni Akceptace předmětu Díla či Dílčí části Díla Objednatelem bude Dílo či Dílčí část Díla bez vad a v souladu se Smlouvou a s platnými a účinnými obecně závaznými právními předpisy České republiky."

Odstavec 6.1 článku 6 Smlouvy se doplňuje o nové písmeno (g) v následujícím znění:

„(g) pro realizaci a dokončení Projektu II a nastavení Služby Incident Manažer v Příloze č. 15."

„6.3 Akceptační řízení proběhne vždy do termínu sjednaného v Příloze č. 8 a v Příloze 15."

Písmeno (f) odstavce 8.1 článku 8 Smlouvy se mění takto a odstavec 8.1 článku 8 Smlouvy se dále doplňuje o nové písm. (ch) v níže uvedeném znění:

„(f) za 1 započatý kalendářní měsíc poskytování Služeb bezpečnostního dohledu ve výši 318.000,- Kč bez DPH. V případě poskytování Služeb po dobu kratší než 30 dnů se cena krátí proporcionálně dle počtu dnů, po které byla Objednateli skutečně poskytována."

„(ch) za realizaci Projektu II celkem ve výši 960.000,- Kč bez DPH."

Odstavec 8.3 článku 8 Smlouvy se mění takto:

„8.3 Služby bezpečnostního dohledu, konkrétně služby uvedené v příloze č. 6 Smlouvy - , SLA 1 (služba „Průběžný bezpečnostní dohled"), SLA 2 (služba „Řešení incidentů"), SLA 3 (služba „Správa problémů"), SLA 4 (služba – „Provádění servisních zásahů"), SLA 5 (služba „Analýza kybernetických událostí a incidentů"), SLA 6 (služba „Digitální forenzní analýza"), SLA 7 (služba „Konzultace oblasti reakce na kybernetický incident"), SLA 8 (služba „Monitorování zranitelností") a rovněž Služby údržby a technické podpory Zhotovitele uvedené v příloze č. 7, konkrétně služby SLA 1 (služba „Technická podpora HW řešení"), SLA 2 (služba „Technická podpora SW řešení") a SLA 3 (služba „Konzultace a práce na vyžádání"), jsou poskytovány v limitovaném rozsahu počtu hodin v jednom kalendářním měsíci dle specifikace uvedené v Příloze č.6 a v Příloze č.7. Služba SOC-Incident Manažer specifikovaná v Příloze č. 15 je poskytována hodinovou sazbou, jak je uvedeno níže. V tomto článku 8.3 uvedené a Objednateli poskytnuté Služby, překračující daný limitovaný rozsah počtu hodin v jednom kalendářním měsíci anebo účtované hodinovou sazbou, bude Zhotovitel Objednateli účtovat hodinovou sazbou za každou započatou 1 h takové Služby, a to dle následujícího sazebníku:

- *1 započatá hodina Služby bezpečnostního dohledu / 2.000,- Kč bez DPH*
- *1 započatá hodina Služby Incident Manažer v pracovní době, kdy pracovní doba je stanovena od 8:00 do 16:00 v pracovní dny v týdnu / 2.000,- Kč bez DPH*

- *1 započatá hodina Služby Incident Manažer mimo pracovní dobu, kdy pracovní doba je stanovena od 8:00 do 16:00 v pracovní dny v týdnu / 4.000,- Kč bez DPH*
- *1 započatá hodina Služby údržby a technické podpory /2.000,- Kč bez DPH.“*

Odstavec 10.1 a 10.2 článku 10 Smlouvy se mění takto:

„10.1 Objednatel se zavazuje poskytnout Zhotoviteli ke splnění Díla, Projektu a Projektu II veškerou potřebnou a možnou součinnost, zejména ty uvedené v Příloze č. 1, Příloze č.3, Příloze č. 4 a v Příloze č. 15 této Smlouvy a rovněž zajistit její poskytnutí všemi třetími osobami. Je-li k provedení Díla a/nebo jeho Dílčí části nutná součinnost Objednatele, určí mu Zhotovitel přiměřenou lhůtu k jejímu poskytnutí v délce nejméně 5 pracovních dnů. Uplyne-li tato lhůta marně, má Zhotovitel právo podle své volby si zajistit náhradní plnění na náklady Objednatele, anebo pokud nelze pro neposkytnutí součinnosti ze strany Objednatele Dílo/ Dílčí část Díla dokončit a upozornil-li na to Objednatele, odstoupit od Smlouvy. V případě prodlení Objednatele s poskytnutím své součinnosti potřebné k řádnému a včasnému provedení Díla a/nebo jeho Dílčí části, neodpovídá Zhotovitel Objednateli za žádnou s tím související újmu, přičemž lhůty k plnění dle Přílohy č.8 a Přílohy č. 15 se pro Zhotovitele automaticky prodlužují o prodlení na straně Objednatele.
10.2 Součinností Objednatele se rozumí zejména, že:
(a) Objednatel je povinen zajistit prostředí pro činnost Zhotovitele tak, aby mohl vykonávat práce, v nichž spočívá Dílo. Zajištění prostředí zahrnuje zajištění přístupu personálu Zhotovitele do Místa plnění v rozsahu nezbytném pro plnění této Smlouvy.
(b) Specifikace požadavků na software a hardware Objednatele, který je Objednatel povinen zajistit pro instalaci dodávaného Software je uvedena v Příloze č. 4.
(c) Objednatel je povinen zajistit následující součinnosti, které jsou dále blíže specifikovány v Příloze č.1, Příloze č.3, Příloze č. 4 a příloze č. 15 této Smlouvy:
(i) Zajištění fyzického umístění Hardware v Datovém centru a na Lokalitách.
(ii) Vytvoření komunikačních tras.
(iii) Vytvoření přístupů a prostupů do Datového centra Objednatele.
(d) Objednatel je povinen Zhotoviteli poskytnout veškeré podklady a informace nezbytné k řádnému a včasnému provedení Díla dle této Smlouvy.“

Odstavec 13.1 a 13.2 článku 13 Smlouvy se mění takto:

„13.1 Zhotovitel je povinen provést Dílo řádně a včas v souladu s harmonogramem plnění uvedeným v Příloze č. 8 a v Příloze č. 15 této Smlouvy a v souladu s obecně závaznými právními předpisy, pokyny vydanými Objednatelem, obsahem poskytnutých informací a materiálů a dodržovat při případném pohybu svých (spolu)pracovníků v objektech Objednatele interní předpisy Objednatele.

13.2 Zhotovitel je povinen postupovat při provádění Díla s náležitou péčí a podle pokynů Objednatele. Při provádění Díla je Zhotovitel oprávněn upozorňovat Objednatele na nevhodnost jeho pokynů a/nebo na nevhodnou povahu věci, kterou mu Objednatel k provedení Díla předal. Překáží-li nevhodná věc a/nebo pokyn v řádném provádění Díla a/nebo jeho části, Zhotovitel je v nezbytném rozsahu přeruší až do výměny věci a/nebo změny pokynu; trvá-li Objednatel na provádění Díla s použitím předané věci a/nebo podle daného pokynu, má Zhotovitel právo požadovat, aby tak Objednatel učinil v písemné formě. Lhůty stanovené pro dokončení dílčích částí Díla dle Přílohy č. 8 a Přílohy č. 15 se prodlužují o dobu přerušením vyvolanou. Objednatel nemá žádná práva z vady Díla a/nebo jeho Dílčí části vzniklé pro nevhodnost jeho věci a/nebo pokynu.“

Odstavec 24.9 článku 24 Smlouvy se mění takto:

„24.9 V případě rozporu mezi Přílohou č. 14 a ostatními ustanoveními Smlouvy mají přednost ustanovení Smlouvy. V případě rozporu mezi Přílohou č. 15 a ostatními ustanoveními Smlouvy mají přednost ustanovení přílohy č. 15. Je-li ve Smlouvě některý výraz uveden s počátečním velkým písmenem a není-li jeho význam definován ve Smlouvě, má význam uvedený ve VOP a/nebo v dokumentech, na které Smlouva odkazuje.“

3. Závěrečná ustanovení

3.1. Ustanovení Dodatku č. 1 včetně jeho příloh mají přednost před úpravou Smlouvy. Ve věcech neupravených se aplikují ustanovení Smlouvy.

3.2. Tento Dodatek č. 1 je vyhotoven ve dvou (2) stejnopisech, z nichž Objednatel obdrží po jednom (1) vyhotovení a Zhotovitel po jednom (1) vyhotovení. Dodatek č. 1 nabývá platnosti dnem jeho uzavření a účinnosti dnem jeho zveřejnění v registru smluv, nestanoví-li obecně závazný právní předpis něco jiného. Za den uzavření Dodatku č. 1 se považuje den uvedený u podpisů oprávněných zástupců obou Stran. Je-li takto označeno více dní, pak se považuje za den uzavření datum pozdější.

3.3. Ostatní ustanovení Smlouvy nedotčená tímto Dodatkem č. 1 zůstávají v platnosti beze změn.

3.4. Strany prohlašují, že si Dodatek č. 1 přečetly, s jeho obsahem souhlasí a na důkaz toho připojují níže své podpisy.

3.5. Strany se dohodly vedeny dobrou vírou v nabytí platnosti a účinnosti tohoto Dodatku č. 1, že poskytnou-li si s odkazem na tento Dodatek č.1 jakékoliv vzájemné plnění odpovídající předmětu Smlouvy ve znění tohoto Dodatku č. 1, pak se na toto plnění uplatní podmínky, zejména práva a povinnosti Stran stanovené Smlouvou ve znění tohoto Dodatku č. 1. Toto ujednání se vztahuje výlučně na plnění poskytnuté s výslovným odkazem na tento Dodatek č. 1 a/nebo, je-li bez jakýchkoliv pochybností zřejmé, že je takové plnění poskytováno Stranou na základě tohoto Dodatku č. 1.

3.6. Tato Dodatek č. 1 byl podepsán Stranami ve dvou vyhotoveních, z nichž každá Strana obdrží 1 vyhotovení. Pro případ, že dodatek byl Stranami podepsán elektronicky, bude vytvořeno pouze jedno vyhotovení dodatku, které si obě Strany poskytnou.

3.7. Přílohy Dodatku č. 1 jsou jeho nedílnou součástí:

- Příloha č. 1 – nová příloha č. 6 Smlouvy - SLUŽBY BEZPEČNOSTNÍHO DOHLEDU
- Příloha č. 2 – nová příloha č. 15 Smlouvy - Projekt II - „Aktualizace a dodávka služeb bezpečnostního dohledu“ a popis služby SOC-Incident Manažer
  - Příloha A – Katalogové listy
  - Příloha B - Profesní profily osob Zhotovitele na pozici zástupce Incident Manažera
- Příloha č. 3 – nová příloha č. 9 Smlouvy – Kontaktní údaje
- Příloha č. 4 – nová příloha č. 7 Smlouvy – SLUŽBY ÚDRŽBY A TECHNICKÉ PODPORY

V Praze dne .....

Za Objednatele:
ČEPRO, a.s.

V ..... dne .....

Za Zhotovitele:
Corpus Solutions a.s.

[redacted]

PŘÍLOHA Č. 6 – SLUŽBY BEZPEČNOSTNÍHO DOHLEDU

1. SPECIFIKACE POŽADAVKU NA SLUŽBU SLA–1, SLUŽBA „PRŮBĚŽNÝ BEZPEČNOSTNÍ DOHLED“

Cílem této služby je zajistit bezpečnostní dohled v rámci SOC Objednatele, úvodní vyhodnocení bezpečnostních událostí a incidentů a stanovení dalšího postupu k jejich řešení.

Služba musí obsahovat:

- Průběžný bezpečnostní dohled/monitoring v rámci technologií SOC
- Úvodní vyhodnocení událostí a bezpečnostních incidentů zaznamenaných v rámci SOC a rozhodnutí o dalším postupu
- Nahlášení incidentu nebo události k řešení (vytvoření ticketu v Service Desku podle charakteru události) a předání k dalšímu řešení

Požadované parametry služby:

Rozsah zaručeného provozu služby		**Doba odezvy**
24 x 7 (nepřetržitě)		30 minut
Vysoká priorita	**Střední priorita**	**Nízká priorita**
8 pracovních hodin	24 pracovních hodin	48 pracovních hodin

Služba může být poskytována vzdáleným přístupem k pracovišti centrálního bezpečnostního dohledu (SOC).

2. SPECIFIKACE POŽADAVKU NA SLA 2 – SLUŽBA „ŘEŠENÍ INCIDENTŮ“

Cílem této služby je zajistit co nejrychlejší obnovení dostupnosti spravovaných služeb Objednatele a současně minimalizovat důsledky takového výpadku.

Služba musí obsahovat:

- Reakci na nahlášení incidentu
- Řešení jednotlivých incidentů
- Odstranění nahlášeného incidentu
- Sběr podkladů pro aktualizaci dokumentace
- Pravidelný reporting

Požadované parametry služby:

Rozsah zaručeného provozu služby		**Doba odezvy**
24 x 7 (nepřetržitě)		30 minut
Rozsah služby		
Neomezen		
Fix time		
Vysoká priorita	**Střední priorita**	**Nízká priorita**
8 pracovních hodin	24 pracovních hodin	48 pracovních hodin

Každému incidentu je v evidenčním systému přidělena priorita z uvedené škály:

- Vysoká priorita – příklady incidentů
  - způsobí celkovou nedostupnost (nefunkčnost) funkčního celku;
  - je způsoben hardwarovou poruchou zařízení funkčního celku znemožňující provozuschopnost tohoto zařízení alespoň s omezeným výkonem. Neplatí pro zařízení, které je provozováno v režimu vysoké dostupnosti a jehož funkci zajišťuje automaticky náhradní řešení (redundance, high availability, cluster) se stejným nebo sníženým výkonem;
  - je způsoben softwarovou poruchou v rámci funkčního celku, znemožňující jeho provozuschopnost alespoň s omezeným výkonem;
  - vznikne jako důsledek jiných neplánovaných výpadků (elektrické energie) a vyžaduje provedení kontrolovaného obnovení provozuschopnosti funkčních celků;
  - znemožňuje uživatelům provádět standardní pracovní činnosti alespoň náhradním způsobem;
  - znemožňuje plnění SLA parametrů v rámci navazujících služeb
- Střední priorita
  - způsobí snížení výkonnosti funkčních celků;
  - je způsoben hardwarovou poruchou zařízení funkčního celku, která umožňuje provozuschopnost tohoto zařízení s omezeným výkonem;
  - je způsoben softwarovou poruchou v rámci funkčního celku, která umožňuje provozuschopnost instalovaného software s omezeným výkonem;
  - bezprostředně ohrožuje plnění smluvených SLA parametrů navazujících služeb
- Nízká priorita
  - nemá vliv na dostupnost funkčních celků;
  - nemá vliv na výkonnost funkčních celků;
  - může však ovlivňovat pracovní procesy

3. SPECIFIKACE POŽADAVKU NA SLA 3 – SLUŽBA „SPRÁVY PROBLÉMŮ“

Cílem služby je proaktivní předcházení incidentům a zabránění opakování stejných incidentů analyzováním jejich příčin a řízeným odstraňováním těchto příčin z ICT/OT infrastruktury.

Služba musí obsahovat následující činnosti:

- Pravidelné proaktivní vyhodnocení řešených incidentů za odpovídající časové období
- Identifikaci případných problémů (chyb v konfiguracích, hardwarových nebo softwarových závad apod.)
- Evidence problémů v evidenčním systému
- Pravidelný reporting
- Aktualizace přehledu známých chyb
- Zajištění odstranění problémů, pokud lze problém odstranit v rámci poskytovaných servisních služeb

Požadované parametry služby

Frekvence vyhodnocování	Report o provedení a vyhodnocení
Jednou za 3 měsíce	Ano

4. SPECIFIKACE POŽADAVKU NA SLA 4 – SLUŽBA „PROVÁDĚNÍ SERVISNÍCH ZÁSAHŮ“

Předmětem služby je zajistit hladkou implementaci pouze schválených změn a minimalizace rizika vzniku incidentů neřízenými změnami v ICT/OT infrastruktuře objednatele.

Služba musí obsahovat následující činnosti:

- Posouzení provozních a bezpečnostních dopadů změny
- Vypracování popisu řešení změn středního a velkého rozsahu
- Implementaci změn vyplývající z provozu technologii nebo řešení kybernetických incidentů
  - Optimalizace detekčních pravidel v rámci dodaných nástrojů
  - Nasazení nových pravidel na základě provedených šetření kybernetických incidentů.
  - Sken zranitelností na vyžádání (součástí bude specifikace rozsahu provedení skenu).
- Sběr podkladů pro aktualizaci dokumentace
- Pravidelný reporting

Požadované parametry služby

Rozsah zaručeného provozu služby		**Doba odezvy**
8:00 – 16:00 hod (5 x 8)		30 minut
Rozsah služby		
Malý rozsah / Vysoká priorita	**Střední rozsah / Střední priorita**	**Velký rozsah / Nízká priorita**
Implementace změny (pracovních dní)	**Implementace změny (pracovních dní)**	**Implementace změny (pracovních dní)**
2	5	15

Zásah/Změna je jakákoli úprava nastavení spravované technologie, modifikace verze SW upgradem (update, hotfix, service pack) nebo změna hardware.

- Změny s malým rozsahem:
  - změny, jejichž implementace nemá dopad na dostupnost nebo výkonnost funkčních celků a současně jejich implementace nevyžaduje vypracování návrhu řešení, nebo jeho vytváření není účelné (například přidání nebo změny uživatelů, změna nastavení politik detekčních scénářů apod.)
- Změny se středním rozsahem:
  - změny v rámci jednoho funkčního celku, jejichž implementace vyžaduje schválení Objednatelem na základě Zhotovitelem vypracovaného návrhu řešení a současně změny, jejichž implementace může mít i krátkodobý (v řádu minut) dopad na dostupnost nebo výkonnost funkčních celků
- Změny s velkým rozsahem:
  - změny, jejichž implementace vyžaduje schválení Objednatelem dle Zhotovitelem vypracovaného návrhu řešení a plánu implementace

Na vyžádání Objednatele mohou být činnosti prováděny i mimo tuto pracovní dobu.

5. SPECIFIKACE POŽADAVKŮ NA SLA 5 – SLUŽBA „ANALÝZA KYBERNETICKÝCH UDÁLOSTÍ A INCIDENTŮ“

Cílem této služby je zajistit co nejrychlejší vyhodnocení detekované kybernetické události nebo incidentu v infrastruktuře objednatele, zajištění provedení analýzy incidentu a odpovídají reakce.

Služba musí obsahovat následující činnosti:

- Reakci na nahlášený kybernetického incidentu nebo události přijaté z první úrovně podpory objednatele
- Provedení analytických činností
- Návrh řešení na snížení nebo eliminaci dopadu kybernetického incidentu
- Identifikace vektoru útoku a jeho cíle

Požadované parametry služby

Rozsah zaručeného provozu služby		**Doba odezvy**	
24 x 7 (nepřetržitě)		30 minut	
Rozsah služby			
Neomezen			
Fix time			
Kritická priorita	**Vysoká priorita**	**Střední priorita**	**Nízká priorita**
8 pracovních hodin	16 pracovních hodin	24 pracovních hodin	48 pracovních hodin

Priorita je určena na základě kritičnosti detekované události v kombinaci s definovanou důležitostí aktiva zasaženého kybernetickým incidentem nebo jeho celkovým rozsahem.

Požadovaná stupnice závažnosti detekované události:

- Kritická závažnost události/incidentu
- Vysoká závažnost události/incidentu
- Střední závažnost události/incidentu
- Nízká závažnost události/incidentu

V případě, kdy technologie pro detekci kybernetických událostí nepodporuje uvedenou škálu požadujeme provedení mapování závažnosti incidentů na výše uvedenou stupnici.

6. SPECIFIKACE POŽADAVKŮ NA SLA 6 - SLUŽBA „DIGITÁLNÍ FORENZNÍ ANALÝZA“

Předmětem služby je v rámci kybernetického incidentu, zajištění důkazních materiálů v oblasti informační technologií, jejich interpretaci a následnou prezentaci nad rámec automatizované forenzní analýzy obsažené v nástrojích bezpečnostního monitoringu.

Služba musí obsahovat následující činnosti:

- Příjem požadavku nad rámec automatizované forenzní analýzy
- Sběr a zajištění digitálních stop
- Kontrola a extrakce „artefaktů“
- Provedení analýzy
- Vypracování závěrečné zprávy

Požadované parametry služby

Rozsah zaručeného provozu služby		**Doba odezvy**
8:00 – 16:00 hod (5 x 8)		30 minut
Rozsah služby		
24 hod. měsíčně		
Fix time		
Vysoká priorita	**Střední priorita**	**Nízká priorita**
16 pracovních hodin	24 pracovních hodin	48 pracovních hodin

7. SPECIFIKACE POŽADAVKŮ NA SLA 7 – SLUŽBA „KONZULTACE OBLASTI REAKCE NA KYBERNETICKÝ INCIDENT "

Služba bude poskytována za účelem odborné pomoci a rady při řešení konkrétního kybernetického incidentu odpovědným zástupcům na straně Objednatele.

Služba musí pokrýt následující oblasti:

- Návrh preventivních opatření, zamezující nebo minimalizující dopad kybernetického incidentu (technická, procesní, organizační opatření)
- Spolupráce při obnově napadených systémů (vzdáleně a na vyžádání pak v místě určeném objednatelem)
- Návrh nových detekčních scénářů

Požadované parametry služby

Rozsah zaručeného provozu služby		**Doba odezvy**
8:00 – 16:00 hod (5 x 8)		30 minut
Rozsah služby		
32 hod. měsíčně		
Fix time		
Vysoká priorita	**Střední priorita**	**Nízká priorita**
16 pracovních hodin	24 pracovních hodin	48 pracovních hodin

8. SPECIFIKACE POŽADAVKŮ NA SLA 8 – SLUŽBA „MONITOROVÁNÍ ZRANITELNOSTÍ"

Cílem služby je aktivní zjišťování zranitelností infrastruktury a informačních systémů dostupných z prostředí internetu objednatele. Výstupem poskytované služby je sestavení seznamu zranitelností nalezených ve skenovaném adresním rozsahu objednatele.

Služba musí obsahovat následující činnosti:

- Automatizované skenování zranitelností
- Vyhodnocení identifikovaných zranitelností (s ohledem na možné chybné detekce)
  - Evidence případných výjimek

- Prioritizace nálezů s ohledem na potenciální dopad do infrastruktury
- Hodnocení závažnosti zranitelností na škále dle celkového dosaženého skóre
- Formulace konkrétních konfiguračních doporučení pro odstranění identifikovaných zranitelností na infrastruktuře
- Vypracování pravidelného reportu s rozdílovou analýzou z minulých skenování a uvedením priorit nálezů.
- Sken zranitelností na vyžádání (součástí bude specifikace rozsahu provedení skenu).

Report s identifikovanými nálezy bude 1x měsíčně vyhodnocen ve spolupráci s odpovědnými zástupci objednatele a dodavatele, kde bude stanoven postup pro jejich zmírnění nebo eliminace. Předpokládá se minimální zpracování zranitelností se závažností kritická a vysoká. Zpracované nálezy budou zaevidovány v evidenčním systému objednavatele a předány k řešení odpovědným osobám na straně objednatele.

Technické prostředky na naplnění služby "Monitorování zranitelností" požadujeme zajistit v na straně dodavatele.

Požadované parametry služby

Rozsah zaručeného provozu služby	**Doba odezvy**
8:00 – 16:00 hod (5 x 8)	30 minut
Rozsah služby: 12 hodin měsíčně	

PŘÍLOHA Č. 15 – PROJEKT II - „Aktualizace stávajících a dodávka nových služeb bezpečnostního dohledu" a popis Služby SOC-Incident Manažer.

Fáze Projektu II:

1. SPECIFIKACE ZPŮSOBU REALIZACE ROZŠÍŘENÍ SLUŽBY BEZPEČNOSTNÍHO DOHLEDU

Rozšíření služby bezpečnostního dohledu zahrnuje i dodávku služeb technických a bezpečnostních specialistů pracoviště SOC Zhotovitele, a to ve variantě projektové činnosti i průběžného plnění Služeb.

Nabízené řešení umožní čerpat know-how Incident Managera, který navrhne, připraví a zajistí aktuálnost reakčních scénářů na 10 druhů kybernetických hrozeb relevantních pro prostředí Objednatele (v kombinaci IT i OT prostředí). Scénáře budou popisovat reakci např. na následující situace:

- Sofistikované Phishing a Spear-phishing útoky na privilegované uživatele
- Malware a Ransomware útoky
- DDoS útoky (Distributed Denial of Service)
- Únik citlivých dat (Data Breach)
- Interní hrozba (Insider threat)
- Ztráta nebo krádež zařízení (Device Loss or Theft)
- Neautorizovaný přístup k systémům (Unauthorized Access)

Přesné specifikování, které scénáře budou popsány, bude součástí provedení implementačního Projektu II, jak je dále uvedeno v odstavci 3 a 4.

2. OBSAZENÍ REALIZAČNÍHO TÝMU ZHOTOVITELE V RÁMCI PROJEKTU II A NÁSLEDNĚ I PŘI POSKYTOVÁNÍ SLUŽBY

Uvedené certifikace potvrzují nejvyšší možnou specializaci pro kybernetickou bezpečnost. Objednateli budou k dispozici odborníci v IT/OT a CLOUD prostředí, se specializací na procesy a řízení a offensive security, a to jak pro realizaci Projektu II, tak pro poskytování Služeb.

Specializace týmu SOC pro zvládání kybernetických bezpečnostních událostí a incidentů:

Počet osob	Název certifikace	Tým CS	Dostupnost
1	Certificate of Completion Certified Cloud Security Professional (CCSP)	SOC	24 x 7
1	CompTIA Advanced Security Practitioner (CASP+)	SOC	24 x 7
2	CompTIA Security Analytics Expert - CSAE	SOC	24 x 7
4	CompTIA Security+	SOC	24 x 7
1	ISC2 - Certified in Cybersecurity	SOC	24 x 7
1	Microsoft Certified: Security Operations Analyst Associate	SOC	24 x 7
1	SANS FOR508: Advanced Incident Response, Threat Hunting, and Digital forensics	SOC	24 x 7

Specializace týmu Zhotovitele, který zajistí přípravnou část Projektu II

Počet osob	Název certifikace	Tým CS	Dostupnost
2	CSSLP Certified Secure Software Lifecycle Professional	Security Expert	8 x 5
2	CyberGym Certified Cyber Defender	Security Expert	24 x 7
1	ISA/IEC 62443 Cybersecurity Fundamentals Specialist	Security Expert	8 x 5
2	OSCP Offensive Security Certified Professional	Security Expert	8 x 5
1	SANS FOR508: Advanced Incident Response, Threat Hunting, and Digital forensics	Security Expert	24 x 7
1	CCSP Certified Cloud Security Professional	Konzultant	8 x 5
1	CCSP Certified Cloud Security Proffesional	Konzultant	8 x 5
1	CISSP Certified Information Systems Security Professional	Konzultant	8 x 5
1	CRISC_Certified in Risk and Information Systems Control	Konzultant	8 x 5
1	ITIL Foundation Certificate in IT Service Management	Konzultant	8 x 5
1	ITIL V3 Foundation	Konzultant	8 x 5
1	Microsoft Certified Azure Security Engineer Associate	Konzultant	8 x 5
1	Microsoft Certified: Azure Fundamentlas	Konzultant	8 x 5
1	Microsoft Certified: Cybersecurity Architect Expert	Konzultant	8 x 5

3. POPIS VÝSTUPŮ DODÁVKY A AKCEPTAČNÍ KRITÉRIA PROJEKTU II

Etapa	Popis činnosti	Výstup	Akceptační kritéria
0	Kickoff - zahájení projektu	• Kontaktní matice • Projektová pravidla • Projektový plán	N/A
1	Úvodní seznámení a organizační struktura s cílem poskytnout Incident Manažerovi přehled o organizaci, její struktuře a hlavních kontaktních osobách.	• Seznámení s vedením IT a bezpečnosti, rolemi a odpovědnostmi. • Přehled důležitých obchodních procesů a jejich kritické závislosti na IT. • Seznámení s kontaktními osobami pro interní IT, právní oddělení, PR a klíčovými partnery mimo organizaci (např. externí SOC).	
1	Seznámení s infrastrukturou a systémy Objednatele s cílem zajistit, aby měl Incident Manažer přehled o technické infrastruktuře organizace a kritických systémech.	• Představení aktuální architektury IT včetně serverů, síťových prvků, aplikací a cloudových řešení. • Přehled kritických systémů a datových toků, které jsou zásadní pro podnikání (např. finanční systémy, CRM, ERP). • Seznámení s monitorovacími nástroji,	

		logováním, SIEM systémy a dalšími bezpečnostními platformami používanými organizací. • Identifikace míst, která jsou zranitelná vůči útokům a kde je potřeba zvláštní pozornost.	
1	Bezpečnostní politika a regulační požadavky s cílem poskytnout Incident Manažerovi znalosti o interních bezpečnostních pravidlech a právních/regulačních požadavcích.	• Studium stávajících bezpečnostních politik a směrnic včetně incident response politiky. • Pochopení, jaké regulační a právní povinnosti se na organizaci vztahují (např. GDPR, ISO/IEC 27001, NIST). • Seznámení s protokoly pro ohlášení bezpečnostních incidentů regulačním orgánům a externím partnerům.	
2	Návrh možností realizace tohoto projektu	• Na základě předchozí etapy 1 - podrobného seznámení s prostředím Objednatele bude předložen Zhotovitelem návrh 10-ti playbooků a možnost realizace zakomponování IRT do procesů Objednatele	• Playbooky adekvátně řeší identifikovaná rizika • Musí být v souladu s obchodními cíli a strategiemi Objednatele • Návrhy splňují technickou proveditelnost a splňují cíl a účinnost celého projektového plánu
2	Playbooky a scénáře incidentů	• Incident Manažer tvoří reakční scénáře, které umožní Objednateli rychle reagovat na různé typy incidentů pomocí zavedených pracovních postupů.	Předané reakční scénáře musí splnit zejména: • IRP je v souladu se všemi relevantními normami a standardy, jako jsou např. ISO 27001, NIST, NIS2 a obdobné normy týkající se IRP (např. NIST Cyber Incident Response, SANS Incident Response Framework, ISO/IEC 27035) • Projektový plán pokrývá všechny fáze reakce na incident, od

			detekce po obnovu • Projektový plán je technicky a organizačně proveditelný • Projektový plán účinně minimalizuje dopady kybernetického incidentu, na který je zaměřen • Projektový plán je srozumitelný a snadno použitelný pro Objednatele • Projektový plán splňuje všechny relevantní zákonné normy a regulační požadavky
3	Rekapitulace navržených opatření s vazbou na Smlouvu, zpřesnění popisu, definic, pojmosloví, propojení Služeb navzájem včetně a faktického zařazení služby Incident Manažer mezi Služby bezpečnostního dohledu a parametrů dodávaných Služeb a zapracování těch úprav do Smlouvy.		

4. ROZPAD PŘEDPOKLÁDANÉ NÁROČNOSTI PROJEKTU II

Objednatel nedisponuje vstupy, které jsou nutné pro onboarding role Incident Managera a zahájení funkčního procesu. Zhotovitel tak dle svých zkušeností a best practice předpokládá níže uvedenou náročnost jednotlivých bodů kapitoly 3 a uvádí ji v jednotkách MD níže v tabulce. Úvodní seznámení a organizační struktura s cílem poskytnout Incident Manažerovi přehled o společnosti Objednatele, její struktuře a hlavních kontaktních osobách.

Úvodní seznámení a organizační struktura s cílem poskytnout Incident Manažerovi přehled o interním prostředí Objednatele, jeho struktuře a hlavních kontaktních osobách.	
Jednotlivé kroky projektu	**Počet jednotek MD**
Seznámení s vedením IT a bezpečnosti, rolemi a odpovědnostmi.	1
Přehled důležitých obchodních procesů a jejich kritické závislosti na IT.	4
Seznámení s kontaktními osobami pro interní IT, právní oddělení, PR a klíčovými partnery mimo organizaci (např. externí SOC ISP).	3
Seznámení s infrastrukturou a systémy s cílem zajistit, aby měl Incident Manažer přehled o technické infrastruktuře organizace a kritických systémech.	
Představení aktuální architektury IT včetně serverů, síťových prvků, aplikací a cloudových řešení.	2
Přehled kritických systémů a datových toků, které jsou zásadní pro podnikání (např. finanční systémy, CRM, ERP).	3
Seznámení s monitorovacími nástroji, logováním, SIEM systémy a dalšími bezpečnostními platformami používanými organizací.	1
Identifikace míst, která jsou zranitelná vůči útokům a kde je potřeba zvláštní pozornost.	3

Bezpečnostní politika a regulační požadavky s cílem poskytnout Incident Manažerovi znalosti o interních bezpečnostních pravidlech a právních/regulačních požadavcích.	
Studium stávajících bezpečnostních politik a směrnic včetně incident response politiky.	5
Pochopení, jaké regulační a právní povinnosti se na organizaci vztahují (např. GDPR, ISO/IEC 27001, NIST).	3
Seznámení s protokoly pro ohlášení bezpečnostních incidentů regulačním orgánům a externím partnerům.	1
Předložení návrhu možnosti realizace tohoto projektu	
na základě předchozího podrobného seznámení s prostředím bude předložen Zhotovitelem návrh 10-ti playbooků a možnost realizace zakomponování IRT do procesů a interního prostředí Objednatele	2
Playbooky a scénáře incidentů	
Playbook 1 - první pro IT	8
Playbook 2 - první pro OT	8
Playbooky 3 - 10	16

5. POŽADAVKY NA SOUČINNOST OBJEDNATELE

- Rozmyšlení a popsání situací, které budou vyžadovat aktivaci role Incident Manager
- Nominace osob v projektu odpovědných za jednotlivá odvětví/oddělení
- Součinnosti pro připomínky a akceptaci
- Zajištění účasti odpovědných a kompetentních osob na interview při přípravné projektové aktivitě a při následné implementaci a poskytování Služeb
- Přístupné informace z analýzy rizik a dopadové analýzy Objednatele
- Přístupné informace z evidence aktiv (technických i business)

6. HARMONOGRAM PROJEKTU II

Etapa	Popis činnosti	Trvání
0	Kickoff - zahájení Projektu II	T0
1	Onboarding role Incident Manažer	T+10
2	Návrh možnosti realizace Projektu II	T+30
2	Zhotovení a úspěšná akceptace Objednatelem playbooků a scénářů incidentů	T+40

Trvání je uvedeno v jednotkách pracovních dnů.

7. SPECIFIKACE POŽADAVKU NASTAVENÍ SLUŽBY „SOC – INCIDENT MANAGER“

Incident Manažer zastává při řešení kybernetického bezpečnostního incidentu klíčovou roli v řízení a koordinaci aktivit zaměřených na rychlé zvládnutí a nápravu incidentu u Objednatele.
Jeho činnosti jsou zaměřeny na minimalizaci dopadů na společnost a fungování Objednatele a zajištění co nejrychlejšího a nejefektivnějšího vyřešení incidentu.

Konkrétní činnosti Incident Manažera zahrnují:

- Identifikaci a klasifikaci incidentu podle závažnosti a priorit.
- Koordinaci týmu odpovědného za řešení incidentu, včetně rozdělování úkolů a zajišťování potřebných zdrojů.
- Shromažďování informací o incidentu a dokumentaci průběhu jeho řešení.
- Rozhodování o eskalaci incidentu na vyšší úroveň řízení, pokud to situace vyžaduje.

Příloha č. 2 Dodatku č. 1 – nová Příloha č. 15 Smlouvy - Projekt II - „Aktualizace a dodávka služeb bezpečnostního dohledu" a popis služby SOC-Incident Manažer

- Komunikaci se zainteresovanými stranami, jako jsou vedení společnosti Objednatele, IT oddělení, bezpečnostní týmy a případně externí subjekty.
- Monitorování efektivity prováděných opatření a jejich případné úpravy podle potřeby.
- Zajištění důkazů a příprava podkladů pro případnou následnou forenzní analýzu.
- Vedení aktivit spojených s obnovou běžného provozu po vyřešení incidentu.

Službu SOC – Incident Manažer bude za Zhotovitele plnit tým lidí s níže nadefinovanou odbornou kvalifikací s tím, že Zhotovitel stanoví konkrétní osoby (3 osoby), které budou v rámci této služby Zhotovitele zastupovat a komunikovat s Objednatelem a jejich profesní profily budou nedílnou součástí této přílohy, kde bude tato služba upravená (dále jen „**zástupce Incident Manažera**"). V případě jakékoliv změny v osobách zástupce Incident Manažera, dojde k aktualizaci přílohy.

Specializace týmu pro Službu „SOC – INCIDENT MANAŽER":

Počet osob	Název certifikace	Tým CS	Dostupnost
1	Certificate of Completion Certified Cloud Security Professional (CCSP)	SOC	24 x 7
1	CompTIA Advanced Security Practitioner (CASP+)	SOC	24 x 7
2	CompTIA Security Analytics Expert - CSAE	SOC	24 x 7
4	CompTIA Security+	SOC	24 x 7
1	ISC2 - Certified in Cybersecurity	SOC	24 x 7
1	Microsoft Certified: Security Operations Analyst Associate	SOC	24 x 7
1	SANS FOR508: Advanced Incident Response, Threat Hunting, and Digital forensics	SOC	24 x 7

Incident Manažer tedy zajišťuje efektivní řízení, koordinaci a komunikaci, která vede k rychlému a úspěšnému zvládnutí kybernetického bezpečnostního incidentu.

Vztah Incident Manažer k procesu zvládání kybernetických bezpečnostních incidentů Objednatele:

- Incident Manažer operativně řídí a koordinuje řešení incidentu od okamžiku detekce až po jeho vyřešení a obnovení běžného provozu.
- Pravomoci Incident Manažera končí v okamžiku, kdy incident vyžaduje strategická rozhodnutí, která přesahují jeho operativní kompetence, nebo když je nezbytná širší koordinace s celkovou bezpečnostní strategií společnosti Objednatele.
- Krizový štáb Objednatele (architekt KB, manažer KB, atd.) přebírá roli zejména v oblasti strategických rozhodnutí, schvalování opatření s dlouhodobým dopadem, změn v bezpečnostní architektuře a v koordinaci činností, které vyžadují širší manažerský dohled či významnější zdroje.
- Krizový štáb Objednatele je také zodpovědný za dohled nad implementací preventivních opatření navržených Incident Manažerem po ukončení incidentu.

Příprava (Preparation)

Fáze přípravy je základem pro úspěšné zvládnutí kybernetických incidentů. Cílem je zajistit, aby byl Objednatel připraven reagovat na bezpečnostní incidenty rychle a efektivně. Příprava zahrnuje vytvoření a pravidelnou aktualizaci plánu reakce na incidenty, který definuje postupy, role a odpovědnosti jednotlivých členů týmu. Dalším klíčovým prvkem je školení zaměstnanců, testování schopností týmu prostřednictvím simulovaných cvičení a zajištění potřebných nástrojů a zdrojů. Dobrá příprava minimalizuje chaos a zpoždění při reálném incidentu, čímž snižuje možné dopady na Objednatele.

- **Vypracování a udržování plánu reakce na incidenty**: Incident Manažer je zodpovědný za přípravu a pravidelnou aktualizaci plánu na zvládání incidentů. Tento plán zahrnuje role a odpovědnosti jednotlivých členů týmu, postupy detekce incidentů a scénáře reakce.

- **Školení týmu a testování plánu**: Pravidelná školení týmu na incidenty a testování plánu (např. simulace) jsou zásadní pro zajištění připravenosti.

- **Zajištění dostupnosti nástrojů**: Incident Manažer dohlíží na to, aby byly k dispozici všechny potřebné nástroje pro detekci a řešení incidentů (např. monitorovací systémy, forenzní nástroje).

Obnova (Recovery)

Po zvládnutí akutní fáze incidentu následuje obnova, jejímž cílem je co nejrychleji vrátit postižené systémy do běžného provozu. Incident Manažer v této fázi dohlíží na obnovu dat, konfigurací a služeb, aby zajistil jejich správné fungování bez dalších bezpečnostních rizik. Důležitým krokem je také ověření, že byla eliminována všechna rizika, která k incidentu vedla, a že systémy fungují podle očekávání. Tento proces zahrnuje také komunikaci s vedením společnosti Objednatele a dalšími zainteresovanými stranami, aby byla zajištěna transparentnost a informovanost o stavu obnovy.

- **Obnovení provozu**: Incident Manažer zajišťuje, že všechny systémy jsou bezpečně obnoveny a dohlíží na ověření, že byly všechny bezpečnostní díry odstraněny.

- **Dokumentace a reportování**: Incident Manažer je odpovědný za vedení podrobné písemné dokumentace všech kroků provedených během incidentu a jejich následné reportování vedení společnosti Objednatele a případně příslušným regulačním orgánům.

Post-incident aktivity (Post-Incident Activities)

Po vyřešení incidentu je klíčové vyhodnotit celý proces a identifikovat oblasti pro zlepšení. Incident Manažer svolává tým na tzv. post-incident review, kde jsou analyzovány silné a slabé stránky reakce na incident a zjištěné poznatky jsou použity k vylepšení budoucího postupu. Součástí této fáze je i vytvoření podrobné písemné zprávy, která shrnuje kroky provedené během incidentu a návrhy na zlepšení bezpečnostních opatření nebo změny v procesech. Cílem je zlepšit připravenost na další incidenty a zajistit, aby se podobné problémy neopakovaly.

- **Post-incident review**: Incident Manažer organizuje přezkoumání incidentu, kde se diskutují silné a slabé stránky reakce a provádí se hodnocení, jak lze zlepšit stávající procesy.

- **Zavádění zlepšení**: Na základě získaných poznatků Incident Manažer implementuje nová opatření nebo aktualizuje existující bezpečnostní politiky a plány.

Komunikace (Communication)

Úspěšné zvládnutí incidentu vyžaduje efektivní komunikaci na všech úrovních společnosti Objednatele. Incident Manažer zajišťuje, aby byl interní tým informován o postupu řešení a udržuje transparentní komunikaci s vedením společnosti Objednatele. V případě potřeby také komunikuje s externími partnery, jako jsou regulační orgány, obchodní partneři, zákazníci nebo dodavatelé. Komunikace během incidentu je klíčová pro minimalizaci dopadu na obchodní činnost a pro udržení důvěry zúčastněných stran. Dobře řízená komunikace také snižuje riziko reputačních škod v případě úniku citlivých dat nebo jiných vážných problémů.

- **Interní a externí komunikace**: Incident Manažer zajišťuje, že je v průběhu incidentu vedena jasná a efektivní komunikace jak interně mezi týmy, tak externě s třetími stranami (např. regulačními orgány, zákazníky, dodavateli).

- **Koordinace s právníky a PR**: V případě úniku dat nebo jiného závažného incidentu je Incident Manažer odpovědný za komunikaci s právním oddělením a veřejností, aby minimalizoval reputační škody.

Rozsah činností:

Příloha č. 2 Dodatku č. 1 – nová Příloha č. 15 Smlouvy - Projekt II - „Aktualizace a dodávka služeb bezpečnostního dohledu" a popis služby SOC-Incident Manažer

Rozsah činností je definován výše zmíněnými standardy jako je NIST SP 800-61, ISO/IEC 27035 nebo SANS Incident Handlers' Handbook.

Zejména se jedná o tyto činnosti:

Incident Manager – řídí činnost a komunikaci týmů

- Vede tým reakce na incidenty a koordinuje všechny činnosti reakce na incidenty
- Během incidentu navrhuje kritická rozhodnutí, například kdy eskalovat, zda zapojit externí strany a jak komunikovat se zúčastněnými stranami.
- Zajišťuje strategii komunikace s vrcholovým vedením Objednatele a dalšími zúčastněnými stranami (NÚKIB, PČR, ÚOOÚ atd.), poskytuje aktuální informace o stavu incidentu a všech přijatých rozhodnutích
- Dohlíží na analýzu po incidentu a zajišťuje, aby získané poznatky byly zdokumentovány a použity ke zlepšení budoucích reakcí

Parametry služby:

	Kategorie incidentu
0:00 – 24:00 hod (7 x 24)	Kritická,
8:00 – 16:00 hod (5 x 8) Pouze pracovní dny v týdnu	Kritická, Vysoká, Střední, Nízká a dále Konzultační služby
Doba odezvy pro všechny kategorie incidentu - online	30 minut
Doba odezvy pro všechny kategorie incidentu – onsite (zejména sídlo Objednatele a datové centrum na skladě v Hněvicích)	4 hodiny
Fix time pro kategorii incidentu	Po uplynutí Doby odezvy
Kritická	8 hodin
Vysoká	12 pracovních hodin
Střední	16 pracovních hodin
Nízká	48 pracovních hodin

Práva povinnosti smluvních Stran upravené ve Smlouvě se vztahují jak na realizaci Projektu II, tak na poskytování služby – Incident Manažer. Projekt II je považován za realizaci Díla dle Smlouvy a vztahují se na něj proto všechna relevantní ustanovení Smlouvy, zejména o povinnostech Zhotovitele, akceptačního řízení, způsobu provedení Díla, odpovědnosti za vady, sankce a odpovědnost za újmu, důvěrné informace, odstoupení od smlouvy s tím, že pokud tato příloha upraví práva, povinnosti a podmínky jinak než Smlouva, má přednost právní úprava této přílohy. Pro službu – Incident Manažer se vztahují všechna relevantní ustanovení Smlouvy, zejména o povinnostech Zhotovitele, odpovědnosti za vady, sankce a odpovědnost za újmu, důvěrné informace, odstoupení od smlouvy s tím, že pokud tato příloha upravuje práva, povinnosti a podmínky pro službu Incident Manažer jinak než Smlouva samotná, má přednost právní úprava této přílohy oproti právní úpravě uvedené ve Smlouvě.

Příloha č. A Přílohy č. 15 Smlouvy – Katalogové listy

Příloha č. B Přílohy č. 15 Smlouvy – Profesní profily osob Zhotovitele na pozici zástupce Incident Manažera

Katalogové listy SOC

Obsah

Manažerské shrnutí

Tento dokument obsahuje sjednocenou a rozšířenou specifikaci služeb poskytovaných v rámci Security Operations Center (SOC). Každý katalogový list představuje jednu konkrétní službu s jasně popsaným účelem, rozsahem činností, parametry poskytování, vstupy a výstupy. Cílem tohoto shrnutí je poskytnout přehled vedení a manažerům odpovědným za řízení bezpečnosti o rozsahu nabízených služeb a jejich vzájemné provázanosti.

SOC služby pokrývají kompletní životní cyklus kybernetických událostí a incidentů – od detekce, přes analýzu, řízení incidentů, až po forenzní šetření, návrh nápravných opatření a zpětnou revizi.

Přínosy pro zákazníka:

- Nepřetržité pokrytí (24x7) pro detekci a reakci na incidenty
- Proaktivní prevence díky využívání výstupů služby monitorování zranitelností
- Odborná podpora a konzultace v případě složitých incidentů nebo krizí
- Důkazní podpora díky digitální forenzní analýze

Pokrytí životního cyklu události/incidentu

SANS fáze	**Služba(y)**
Preparation	Konzultace reakce na incident
Identification	Průběžný bezpečnostní dohled Incident Response (24x7)
Containment	Incident Response (24x7) Incident manažer
Eradication	Incident Response (24x7) Incident manažer, Digitální forenzní analýza
Recovery	Zajištění vstupů pro tuto fázi ze služeb: - Konzultace reakce na incident - Incident manažer
Lessons Learned	Konzultace reakce na incident

Incident Manažer je především aktivován při komplexnějších či krizových incidentech. Jeho hlavní přínos spočívá v řízení reakce a organizaci všech zapojených služeb i osob.

Matice vztahů

Tato matice popisuje logické a funkční vazby mezi jednotlivými službami SOC. Každý vztah vyjadřuje směr toku informací, závislostí nebo přímé spolupráce. Cílem je ukázat, jak jednotlivé služby spolupracují v rámci řešení bezpečnostních událostí a incidentů.

Typy vztahů

Code	English Term	Český popis
FWD	Forward	Služba předává událost, incident nebo report další službě k dalšímu zpracování.
USE	Use Output	Služba používá výstupy (data, reporty, výsledky) z jiné služby jako vstup do své činnosti.
ACT	Activate	Služba vyhodnotí potřebu a spustí (aktivuje) specializovanou navazující službu.
CON	Consult	Služby spolupracují formou konzultace či metodické podpory k dosažení lepšího rozhodnutí.
ENH	Enhance	Služba poskytuje doporučení či zpětnou vazbu pro vylepšení detekčních schopností nebo procesů.

Matice vztahů

Zdroj \ Cíl	Průběžný dohled	Incident Response	Forenzní analýza	Threat Hunting	Zranitelnosti	Konzultace	Incident Manažer
Průběžný dohled	—	FWD	—	—	USE	CON	ACT
Incident Response	USE	—	ACT	—	USE	CON	ACT
Forenzní analýza	—	FWD	—	—	—	CON	CON
Threat Hunting	FWD	FWD	FWD	—	USE	CON	ACT
Zranitelnosti	USE	FWD	—	FWD	—	ENH	—
Konzultace	—	CON	USE		ENH	—	CON
Incident Manažer	—	USE	USE		—	CON	—

Vysvětlivky vztahů:

- FWD (Forward) – např. tok událostí z detekční vrstvy do Incident Response nebo výsledků forenzního šetření zpět do IR.
- USE (Use Output) – služba využívá výstupy jiné služby (např. IR pracuje s klasifikací z dohledu; konzultace vychází z reportu zranitelností).
- ACT (Activate) – IR aktivuje Forenzní analýzu, pokud je nutné detailní šetření či zajištění důkazů.
- CON (Consult) – služby si vzájemně předávají know-how (např. IR a Konzultace při složitém incidentu).
- ENH (Enhance) – výstupy z konzultací nebo analýzy zranitelností se používají k úpravám či rozvoji detekčních pravidel.

Katalogové listy služby SOC

Tato kapitola sdružuje všechny detailní katalogové listy jednotlivých služeb, které Security Operations Center nabízí. Každý list poskytuje rychlý přehled o účelu služby, jejím rozsahu a jednoznačně definovaných parametrech – včetně rozsahu provozu, reakčních dob a fix-time závazků. Strukturovaný formát usnadňuje srovnání služeb a jejich přímé začlenění do bezpečnostní architektury zákazníka.

SOC – Průběžný bezpečnostní dohled

Tato služba tvoří základní stavební kámen bezpečnostního dohledu. Jejím hlavním úkolem je průběžné sledování bezpečnostního stavu monitorovaných systémů zákazníka, včasné odhalení potenciálních hrozeb a zahájení procesu jejich předání k dalšímu zpracování. Služba operuje 24x7 a zajišťuje, že žádná významná bezpečnostní událost (security event) nezůstane bez povšimnutí.

Cíl služby

Cílem služby je zajistit kontinuální bezpečnostní dohled nad ICT infrastrukturou zákazníka. SOC zajišťuje příjem, předzpracování a úvodní analýzu všech bezpečnostních událostí, jejich klasifikaci a rozhodnutí o tom, zda událost vykazuje charakteristiku potenciálního bezpečnostního incidentu. V takovém případě je událost předána službě Incident Response k dalšímu řízení. Tímto způsobem služba minimalizuje riziko přehlédnutí klíčových bezpečnostních hrozeb a zajišťuje rychlou reakci v případě potřeby.

Rozsah činností

- Průběžný monitoring a zpracování bezpečnostních událostí z detekčních nástrojů v rámci SOC
- Úvodní analýza a klasifikace bezpečnostních událostí a rozhodnutí o dalším postupu
- Identifikace událostí s potenciálem stát se bezpečnostním incidentem
- Vytvoření ticketu a předání k následnému řízení v rámci služby Incident Response

Parametry služby

Parametr	Hodnota
Rozsah provozu	24 x 7 (nepřetržitě)
Reakční doba	30 minut
Fix Time – Kritická priorita	1 hodina
Fix Time – Vysoká priorita	2 pracovních hodin
Fix Time – Střední priorita	4 pracovních hodin
Fix Time – Nízká priorita	8 pracovních hodin

Reakční doba: Čas od detekce nebo přijetí nové bezpečnostní události do jejího prvotního zpracování analytikem SOC a zapsáním do tiketovacího systému dodavatele.

To zahrnuje „Event Collection & Triage“, zahájení analýzy události, klasifikaci její závažnosti a rozhodnutí, zda má být událost eskalována jako potenciální incident.

Fix Time: Maximální doba, do které má být zajištěno ukončení zpracování události v rámci této služby, tedy provedení její klasifikace, rozhodnutí o jejím dalším osudu (např. předání k řešení v Incident Response nebo uzavření jako neškodné) a zápis informací o bezpečnostním incidentu do ticketovacího systému zákazníka včetně doporučení nebo komentáře.

Vstupy služby:

- **Logy a bezpečnostní události z detekčních systémů**

Závislost na vstupních informacích:

- Přístup do SIEM a souvisejících bezpečnostních nástrojů
- Znalost kritických aktiv a jejich prioritizace

Výstupy služby:

- Notifikace o bezpečnostní události nebo potenciálním incidentu v rámci týmu SOC
- Vytvořený ticket v systému zákazníka v případě zjištění potenciálního incidentu (tento tiket může být vytvořený až v rámci výkonu služby IR).
- Předání události ke zpracování navazující službou Incident Response (Escalation to Incident Handling)
- Překlasifikace události nebo její vyloučení jako neopodstatněné podezření

SOC – Incident Response

Tato služba kombinuje původní schopnosti technické analýzy bezpečnostních incidentů s pokročilým řízením celého životního cyklu bezpečnostních incidentů. Zajišťuje nejen hloubkovou analýzu bezpečnostních událostí a bezpečnostních incidentů, ale i jejich mitigaci, eskalaci, koordinaci a ukončení. Služba je doplněna o dostupnost 24x7, schopnost operativního zásahu a plnou návaznost na krizové a provozní procesy zákazníka.

Cíl služby

Cílem služby Incident Response je zajistit komplexní reakci na kybernetické bezpečnostní incidenty nebo bezpečnostní události s potenciálem stát se incidentem. Služba zahrnuje potvrzení incidentu, návrh rychlých kroků ke zmírnění dopadů (mitigace), koordinaci zainteresovaných stran včetně aktivace týmu zákazníka a zajištění technických či organizačních opatření k jeho zvládnutí. Součástí služby je detailní dokumentace a návrh kroků k minimalizaci budoucího opakování incidentu. Incident Response slouží jako centrální nástroj zvládání kybernetických krizí.

Rozsah činností

- Reakce na bezpečnostní události eskalované z dohledu (L1)
- Validace události jako incidentu nebo její vyloučení (Incident Triage)
- Analýza průběhu, rozsahu a dopadu incidentu (Incident Analysis)
- Identifikace vektoru útoku, zasažených aktiv (a jejich zranitelností) a dat
- Návrh a koordinace aplikace dočasných opatření (Mitigation), eskalace a komunikace
- Návrh opatření k minimalizaci opakování, trvalé odstranění příčiny (Remediation)
- Dokumentace průběhu a závěrů řešení incidentu

Parametry služby

Parametr	Hodnota
Rozsah provozu – Kritická priorita	0:00 – 24:00 hod (7 x 24)
Rozsah provozu – Ostatní priority	8:00 – 16:00 hod (5 x 8)
Reakční doba	30 minut
Fix Time – Kritická	8 hodin
Fix Time – Vysoká	8 pracovních hodin
Fix Time – Střední	24 pracovních hodin
Fix Time – Nízká	48 pracovních hodin

Reakční doba: Čas od přijetí události nebo incidentu procesem Incident Response (předání je evidováno v tiketovacím systému SOC i zákazníka) do okamžiku zahájení činnosti analytikem IR týmu. Zahrnuje posouzení stavu, ověření priority a zahájení odpovídajících kroků v souladu s IR procesem.

Fix Time: Maximální doba, do které má být dokončena hlavní reakce na incident včetně, přijetí dočasných opatření (Mitigation), analýza a odstranění příčiny, návrhu a aktivace nápravných opatření (Remediation), případně předání do navazujících procesů obnovy a forenzního šetření.

Vstupy služby:

- **Eskalovaná bezpečnostní událost z dohledovaných bezpečnostních technologií**
- **Incident nahlášený zákazníkem nebo automatizovaným systémem**
    - **E-mail**
    - **Telefon**
    - **Tiket v tiketovacím systému SOC**

Závislost na vstupních informacích:

- Přístup k logům, SIEM, EDR, CMDB, zranitelnostem, kontaktním osobám

Výstupy služby:

- Zahájený proces řízení incidentu
- Analýza příčiny (Root Cause Analysis)
- Záznam o průběhu a stavu řešení do interního tiketovacího systému SOC i zákazníka
- Koordinace nápravných kroků se zákazníkem
- Návrh opatření proti opakování (Remediation)
- Závěrečná dokumentace a report
- Překlasifikace nebo vyloučení incidentu (např. jako false positive)

SOC – Digitální forenzní analýza

Tato služba je určena pro podrobnou technickou analýzu digitálních stop spojených s bezpečnostním incidentem. Je využívána především tehdy, kdy je třeba získat důkazní materiál, ověřit podezření na interní nebo externí útok, rekonstruovat průběh incidentu nebo podpořit právní nebo disciplinární řízení. Služba poskytuje důkladné technické zhodnocení, navazuje na incidenty kritické a vysoké závažnosti a může být vyžádána i pro střední a nízké priority.

Cíl služby

Cílem služby je provést formální sběr, zajištění, analýzu a vyhodnocení digitálních stop souvisejících s bezpečnostním incidentem. Služba je vykonávána s důrazem na integritu důkazního materiálu, dokumentaci analytických postupů a vytvoření výstupů využitelných jak pro technické vyhodnocení, tak pro případné právní účely.

Rozsah činností

- Přijetí požadavku nad rámec automatizované forenzní analýzy
- Zajištění digitálních artefaktů (např. disky, paměti, logy)
- Získání, uchování a analýza důkazního materiálu
- Vyhodnocení stop a hledání vazeb s incidentem
- Vytvoření formální zprávy včetně metodiky a nálezů

Parametry služby

Parametr	Hodnota
Rozsah provozu – Kritická priorita	0:00 – 24:00 hod (7 x 24)
Rozsah provozu – Ostatní priority	8:00 – 16:00 hod (5 x 8)
Reakční doba	30 minut
Fix Time – Kritická	8 pracovních hodin
Fix Time – Vysoká	8 pracovních hodin
Fix Time – Střední	24 pracovních hodin
Fix Time – Nízká	48 pracovních hodin

Reakční doba: Čas od přijetí požadavku do převzetí úkolu forenzním analytikem v tiketovacím systému SOC a zahájení úkonů spojených se zajištěním nebo analýzou digitálních stop.

Fix Time: Maximální doba pro dokončení forenzní analýzy a zpracování dokumentovaného výstupu včetně závěrů a doporučení.

Vstupy služby:

- **Požadavek na forenzní analýzu související s incidentem**
  - **Eskalace z ostatních činností SOC**
  - **E-mail**
  - **Telefon**

- **Tiket v tiketovacím systému SOC**
- Přístup k relevantním systémům nebo médiím
- Kontext a předchozí zjištění z incident response nebo analytických služeb

Výstupy služby:

- Forenzní zpráva popisující metodiku a závěry šetření
- Zajištěné digitální důkazy včetně přehledu artefaktů (IOCs)
- Identifikace škodlivé aktivity, způsobu průniku, zasažených dat
- Překlasifikace nebo vyloučení incidentu na základě důkazů

SOC – Threat Hunting

Služba Threat Hunting je určena k proaktivnímu vyhledávání pokročilých nebo skrytých hrozeb v prostředí zákazníka, které nebyly detekovány standardními nástroji. Zaměřuje se na identifikaci podezřelé nebo anomální aktivity dříve, než dojde ke vzniku incidentu.

Cíl služby

Zkrátit dobu detekce a reakce na pokročilé hrozby v prostředí zákazníka prostřednictvím proaktivního vyhledávání a analýzy projevů kybernetických hrozeb, které běžné detekční mechanismy nemusí zachytit. Služba přináší hlubší porozumění aktuálním i skrytým hrozbám, zvyšuje úroveň bezpečnostního povědomí a umožňuje přímou adaptaci detekčních schopností na měnící se taktiky útočníků. Proaktivně čerpá z veřejně dostupných informací o aktuálních hrozbách, popřípadě informací dodaných Zákazníkem.

Rozsah činností

- Analýza síťového provozu a logů.
- Vyhledávání IOC a TTP v historických datech.
- Korelace dat z více zdrojů.
- Hypotézové pátrání na základě znalosti prostředí, chování útočníků, trendů vývoje kybernetických hrozeb.
- Dokumentace zjištění a doporučení k nápravě.

Parametry služby

Parametr	Hodnota
Rozsah provozu	8:00 – 16:00 hod (5 x 8)
Měsíční rozsah služby	16 hod.
Fix Time – Kritická	8 pracovních hodin
Fix Time – Vysoká	8 pracovních hodin
Fix Time – Střední	Reporting 1x týdně
Fix Time – Nízká	Nepožadováno

Fix Time: Maximální doba pro dokončení výstup služby.

Vstupy služby:

- **Činnost je prováděna v rámci sjednané četnosti (viz. parametry služby)**
- Logy z IT/OT systémů, historická i aktuální data pro analýzu

- Indikátory kompromitace (IOCs) a Threat Intelligence (TTPs), které budou získávány z komerčních i otevřených zdrojů
- Kontext o prostředí, znalost architektury, aktiv, segmentace

Výstupy služby:

- Nález hrozby obsahující podezřelá aktivita vyžadující ověření nebo zásah
- Specifikace IOCs a TTPs zachycených v prostředí zákazníka včetně použití klasifikace dle frameworku MITRE ATT&CK
- Návrh doporučení na detekční pravidlo, úpravu prostředí, předání do IR
- Shrnutí zjištění včetně analýzy a dopadů

SOC – Konzultace oblasti reakce na incident

Tato služba slouží jako rozšiřující expertní kapacita při řešení specifických kybernetických incidentů, plánování preventivních opatření a zvyšování připravenosti zákazníka. Jejím cílem je podpořit rozhodovací procesy, obnovu systémů a zefektivnění reakce na hrozby formou odborné konzultace a návrhů.

Cíl služby

Cílem služby je poskytnout kvalifikovanou odbornou podporu při řešení bezpečnostních incidentů nad rámec ostatních katalogových služeb a zvýšit úroveň připravenosti zákazníka na kybernetické hrozby. Konzultace probíhají v přímé součinnosti se zákazníkem a jsou zaměřeny na návrh opatření, obnovu prostředí nebo zlepšení detekčních schopností. Výstupem jsou konkrétní doporučení, podpora rozhodování a návrhy scénářů pro krizové i standardní situace.

Rozsah činností

- Návrh preventivních technických, organizačních a procesních opatření
- Konzultace při obnově napadených systémů (na dálku nebo na místě)
- Tvorba a revize detekčních scénářů a alert logiky
- Tvorba a revize reakčních scénářů
- Posouzení aktuálního nastavení prostředí z pohledu reakce na incidenty
- Diskuze nad výsledky forenzní analýzy nebo detekčních nálezů

Parametry služby

Parametr	Hodnota
Rozsah provozu	8:00 – 16:00 hod (5 x 8)
Reakční doba	30 minut
Měsíční rozsah služby	32 hod. měsíčně
Fix Time – Kritická	16 pracovních hodin
Fix Time – Vysoká	16 pracovních hodin

Fix Time – Střední	24 pracovních hodin
Fix Time – Nízká	48 pracovních hodin

Reakční doba: Čas od obdržení požadavku do navázání kontaktu s konzultantem a zahájení koordinace potřebné činnosti.

Fix Time: Maximální doba pro poskytnutí konzultace, návrhu opatření nebo předání výstupů podle závažnosti situace a priority.

Vstupy služby:

- **Specifický požadavek zákazníka na odbornou podporu při incidentu**
  - **E-mail**
  - **Telefon**
  - **Tiket v tiketovacím systému SOC**

Závislosti:

- Kontext bezpečnostních událostí a incidentů nebo výsledků jiných služeb (IR, monitoring zranitelností, forenzní analýza)
- Přístup ke kontaktním osobám a informacím o infrastruktuře

Výstupy služby:

- Odborné doporučení k technickým nebo procesním opatřením
- Návrhy detekčních scénářů nebo změn v konfiguraci
- Návrhy reakčních scénářů
- Podpora při obnově provozu a návrh postupu
- Překlasifikace nebo přehodnocení závažnosti incidentu na základě diskuse a dostupných dat

SOC – Incident Manažer

Tato služba zajišťuje roli dedikovaného Incident Manažera, který v případě kritických incidentů přebírá vedení celého procesu řešení, koordinuje zúčastněné strany, zabezpečuje komunikaci a odpovídá za dokumentaci průběhu. Incident Manažer představuje klíčový prvek krizového řízení a zajištění součinnosti všech SOC služeb i zákaznických týmů.

Cíl služby

Cílem služby je zajistit profesionální řízení bezpečnostních incidentů prostřednictvím role Incident Manažera. Ten přebírá odpovědnost za plánování, koordinaci a vedení incident response procesů, včetně komunikace se zákazníkem, řízení jednotlivých aktivit a zajištění výstupní dokumentace. Služba umožňuje sjednocené řízení náročných incidentů a krizí v prostředí zákazníka.

Rozsah činností

- Aktivace Incident Manažera na základě požadavku zákazníka nebo rozhodnutí SOC po potvrzení zákazníkem
- Koordinace všech zapojených týmů (SOC, zákazník, dodavatelé, regulátor)
- Moderace incident war-room (např. MS Teams, telefonické krizové řízení)
- Zajištění transparentního průběhu řešení incidentu
- Zajištění zákonných požadavků (postup v souladu ZKB a příslušných vyhlášek)
- Řízení časové osy a priorit kroků v rámci incident response
- Tvorba incident logbooku, evidence IOCs, milníků a rozhodnutí
- Komunikace se zákazníkem včetně eskalací, zpráv a shrnutí

Parametry služby

Parametr	Hodnota
Rozsah provozu	Na vyžádání, aktivace 24 x 7
Reakční doba	0,5 hodiny
Fix Time - online	Vedení procesu zahájeno do 0,5 hodiny
Fix Time – onsite	Převedení na onsite do 4 hodin

Reakční doba: Čas od požadavku nebo rozhodnutí aktivovat Incident Manažera do jeho zapojení a převzetí řízení incidentu.

Fix Time: Maximální doba do formálního zahájení řízení a aktivace war-room pro incident.

Vstupy služby:

- **Eskalace z ostatních činností SOC po potvrzení zákazníkem**
- **Požadavek na aktivaci řízení incidentu (z IR, Forenzní analýzy nebo zákazníka)**
  - **E-mail**

    - **Telefon**
    - **Tiket**
- Kontext a průběžná zjištění ze SOC, IR, Forenzní analýzy nebo konzultací
- Přístup ke kontaktním osobám zákazníka

Výstupy služby:

- Založený incident logbook
- Koordinace a řízení incident response procesu
- Zajištěná komunikace mezi všemi účastníky
- Podněty pro informování všech relevantních složek státu
- Shrnutí incidentu a návrh kroků k jeho ukončení

Společné definice

Definice bezpečnostní událost

Bezpečnostní událost (security event) - Pozorovatelný jev v systému nebo síti, který může být relevantní z hlediska bezpečnosti informací nebo systémů.

Důležité vlastnosti:

- Může být normální nebo abnormální.
- Neznamená nutně hrozbu nebo škodu.
- Slouží jako vstup pro monitoring, korelaci nebo detekci incidentů.

Definice bezpečnostní incident

Bezpečnostní incident (security incident) - Jedna nebo více nežádoucích nebo neočekávaných bezpečnostních událostí, které mají významný dopad na bezpečnost informací nebo na provoz organizace.

Důležité vlastnosti:

- Je potvrzený nebo důvodně podezřelý.
- Narušuje důvěrnost, integritu nebo dostupnost (CIA) dostupnost informací, služeb nebo systémů.
- Vyžaduje reakci organizace (obvykle aktivuje odpovídající procesy analýzy, izolace, nápravy a komunikace).
- Může mít právní, regulatorní a obchodní důsledky.

Definice priorit bezpečnostních událostí

Kritická bezpečnostní událost

Definice: Událost, která s vysokou pravděpodobností signalizuje aktivní nebo právě probíhající bezpečnostní incident s vážnými dopady.

Kritické události jsou ihned eskalovány jako incidenty.

Důvody klasifikace: Obsahuje potvrzené indikátory kompromitace (IoC), týká se kritického systému, nebo je v souladu s taktikami známých útočníků (TTP).

Příklady:

- Detekce známého exploitu s úspěšným dopadem.
- Korelované události typu brute-force → přihlášení → změna oprávnění.
- Cílený útok na produkční web.
- Pravděpodobný ransomware útok

Vysoká bezpečnostní událost

Definice: Událost s významnými znaky hrozby nebo anomálie, která může vést k incidentu, zejména pokud není včas prověřena.

Události jsou analyzovány; rozhoduje se, zda přerostou v incident.

Důvody klasifikace: Detekce aktivity typické pro útočné chování nebo přístup k citlivým aktivům bez odpovídajícího kontextu.

Příklady:

- Přihlášení správce z nové geografické lokality.
- Neobvyklý PowerShell skript na stanici běžného uživatele.
- Vysoký počet neúspěšných přihlášení.

Střední bezpečnostní událost

Definice: Událost se známkami podezřelého chování, ale bez jasných důkazů útoku nebo narušení.

Vyžaduje analýzu v kontextu. Reálné hrozby potvrzeny, probíhá jejich řešení.

Důvody klasifikace: Prvotní odchylka od normálu, bez silného kontextu nebo dopadu.

Příklady:

- První přihlášení z nové IP adresy.
- Přístup uživatele mimo jeho obvyklý časový rámec.
- Skenování síťových portů bez navazující komunikace.

Nízká / informační bezpečnostní událost

Definice: Událost bez známek ohrožení, ale užitečná pro audit, korelaci nebo trendovou analýzu.

Edukativní, informační nebo statistická data. Bez potřeby zásahu.

Důvody klasifikace: Normální provozní záznamy s minimálním rizikem.

Příklady:

- Úspěšné přihlášení přes VPN.
- Automatická aktualizace systému.
- Změna hesla uživatelem.

Definice priorit bezpečnostních incidentů

Kritická priorita

Definice: Potvrzený bezpečnostní incident s bezprostředním a závažným dopadem na důvěrnost, integritu nebo dostupnost důležitých aktiv.

Důvody klasifikace: Vysoký dopad + vysoká naléhavost. Například narušení dostupnosti služeb, únik osobních údajů, ransomware, útok na produkční prostředí.

Příklady:

- Ransomware šifrující data
- Únik osobních údajů
- Kompromitace účtu doménového administrátora
- Aktivní síťový útok na kritický systém

V prostředí ČEPRO jsou důležitá aktiva KII (regulované služby v režimu vyšších povinností) nebo byznys služby s hodnocením Business criticality: 1 - most critical.

Vysoká priorita

Definice: Incident, který neohrožuje bezprostředně celou organizaci, ale týká se citlivých systémů a může eskalovat.

Důvody klasifikace: Vysoký nebo střední dopad + střední naléhavost. Např. malware na důležitém počítači, podezřelé skripty na serverech.

Příklady:

- Malware v interní síti
- Přístup k důvěrným datům neoprávněnou osobou
- Laterální pohyb v síti
- Podezřelé administrátorské akce mimo pracovní dobu
- Detekce C2 komunikace z interního systému.

Střední priorita

Definice: Ověřený, ale lokalizovaný incident bez přímého dopadu na klíčová aktiva. Vyžaduje zpracování, ale není urgentní.

Důvody klasifikace: Střední nebo nízký dopad, nízká urgence. Incidenty bez potvrzeného zneužití, ale se známkami abnormality.

Příklady:

- Kliknutí na phishingový odkaz
- Infikovaný pracovní notebook bez přístupu do klíčové infrastruktury
- Nesprávná konfigurace přístupových práv

Nízká priorita

Definice: Incident s minimálním nebo žádným dopadem, plně zablokovaný obrannými mechanismy. Eviduje se pro korelaci nebo audit.

Důvody klasifikace: Nízký dopad + nízká urgence. Události, které nevyžadují reakci, ale mohou sloužit jako indikátor v budoucnu.

Příklady:

- Zablokovaný pokus o phishing
- Port scanning zachycený IDS
- Automatické mazání malwaru na stanici bez připojení do sítě

Příloha B Přílohy č. 2 Dodatku č. 1 – Profesní profily osob Zhotovitele na pozici zástupce Incident Manažera

JMÉNO OSOBY	[redacted]
ROLE NA PROJEKTU	**Incident Response Manager**
PROFESNÍ PRAXE	01/2025 - dosud SOC Specialist L3 Expert / Teamleader, Corpus Solutions a.s. 09/2019 - 01/2025 SOC specialista L3, Corpus Solutions a.s. 04/2017 - 09/2019 Technický specialista SOC, Corpus Solutions a.s. 03/2013 - 03/2017 Wincor Nixdorf - System & Security Architekt 01/2007 - 02/2013 Corpus Solutions a.s. - Technický specialista / Security Consultant
POZICE VE FIRMĚ	**SOC Specialist L3 Expert / Teamleader**
KLÍČOVÉ ZNALOSTI	RSA DLP, RSA enVision, RSA Archer eGRC, RSA SecurID, RSA NetWitness, RSA Security Analytics, IBM Qradar, Juniper SSL VPN, F5 GTM, MS Windows Server, MS ActiveDirectory Domain Services, MS Hyper-V, MSSCVMM, MS Exchange, McAfee EPO, Cisco, Checkpoint, Barracuda, VMware, Fidelis Elevate
CERTIFIKACE	Fidelis Deception, Network, Endpoint, Elevate - Associate GIAC Certified Forensic Analyst CompTIA Security+ certificate CompTIA Advanced Security Practitioner (CASP+) IBM Certified Deployment Professional – Security QRadar SIEM V7.5 IBM Certified Administrator - Security QRadar SIEM V7.5 compTIA Security Analytics Expert - CSAE Bursík - IBM Certified Deployment Professional IBM QRadar SIEM V7.3.2 Bursík - Fidelis Elevate Network – Admin Training Bursík - Fidelis Elevate Endpoint – Admin Training Bursík - Fidelis Deception Training Fidelis Deception Training - Bursík Fidelis Network Training_Bursík Fidelis Endpoint Training_Bursík IBM Certified Associate Administrator Security QRadar SIEM V7.2.8
DÉLKA PRAXE V OBORU ICT	[redacted]
NEJVYŠŠÍ DOSAŽENÉ VZDĚLÁNÍ	[redacted]
POMĚR K DODAVATELI	Zaměstnanec
1 OBJEDNATEL PROJEKTU	[redacted]

Příloha B Přílohy č. 2 Dodatku č. 1 – Profesní profily osob Zhotovitele na pozici zástupce Incident Manažera

	NÁZEV PROJEKTU	[redacted]
	ROZSAH PROJEKTU	
	ROLE NA PROJEKTU	
	DOBA TRVÁNÍ PROJEKTU	
	KONTAKTNÍ OSOBA (JMÉNO, TEL., EMAIL)	
2	OBJEDNATEL PROJEKTU	
	NÁZEV PROJEKTU	
	ROLE NA PROJEKTU	
	DOBA TRVÁNÍ PROJEKTU	
	KONTAKTNÍ OSOBA (JMÉNO, TEL., EMAIL)	
3	OBJEDNATEL PROJEKTU	
	NÁZEV PROJEKTU	
	ROZSAH PROJEKTU	
	ROLE NA PROJEKTU	
	DOBA TRVÁNÍ PROJEKTU	
	KONTAKTNÍ OSOBA (JMÉNO, TEL., EMAIL)	
4	OBJEDNATEL PROJEKTU	
	NÁZEV PROJEKTU	
	ROLE NA PROJEKTU	
	DOBA TRVÁNÍ PROJEKTU	
	KONTAKTNÍ OSOBA (JMÉNO, TEL., EMAIL)	
5	OBJEDNATEL PROJEKTU	
	NÁZEV PROJEKTU	
	ROZSAH PROJEKTU	
	ROLE NA PROJEKTU	
	DOBA TRVÁNÍ PROJEKTU	

Příloha B Přílohy č. 2 Dodatku č. 1 – Profesní profily osob Zhotovitele na pozici zástupce Incident Manažera

	KONTAKTNÍ OSOBA (JMÉNO, TEL., EMAIL)	[redacted]
6	OBJEDNATEL PROJEKTU	
	NÁZEV PROJEKTU	
	ROLE NA PROJEKTU	
	DOBA TRVÁNÍ PROJEKTU	
	KONTAKTNÍ OSOBA (JMÉNO, TEL., EMAIL)	
7	OBJEDNATEL PROJEKTU	
	NÁZEV PROJEKTU	
	ROLE NA PROJEKTU	
	DOBA TRVÁNÍ PROJEKTU	
	KONTAKTNÍ OSOBA (JMÉNO, TEL., EMAIL)	
8	OBJEDNATEL PROJEKTU	
	NÁZEV PROJEKTU	
	ROLE NA PROJEKTU	
	DOBA TRVÁNÍ PROJEKTU	
	KONTAKTNÍ OSOBA (JMÉNO, TEL., EMAIL)	
9	OBJEDNATEL PROJEKTU	
	NÁZEV PROJEKTU	
	ROZSAH PROJEKTU	
	ROLE NA PROJEKTU	
	DOBA TRVÁNÍ PROJEKTU	
	KONTAKTNÍ OSOBA (JMÉNO, TEL., EMAIL)	
10	OBJEDNATEL PROJEKTU	
	NÁZEV PROJEKTU	
	ROZSAH PROJEKTU	
	ROLE NA PROJEKTU	
	DOBA TRVÁNÍ PROJEKTU	
	KONTAKTNÍ OSOBA (JMÉNO, TEL., EMAIL)	

Příloha B Přílohy č. 2 Dodatku č. 1 – Profesní profily osob Zhotovitele na pozici zástupce Incident Manažera

11	OBJEDNATEL PROJEKTU	[redacted]
	NÁZEV PROJEKTU	
	ROLE NA PROJEKTU	
	DOBA TRVÁNÍ PROJEKTU	
	KONTAKTNÍ OSOBA (JMÉNO, TEL., EMAIL)	
12	OBJEDNATEL PROJEKTU	
	NÁZEV PROJEKTU	
	ROZSAH PROJEKTU	
	ROLE NA PROJEKTU	
	DOBA TRVÁNÍ PROJEKTU	
	KONTAKTNÍ OSOBA (JMÉNO, TEL., EMAIL)	
13	OBJEDNATEL PROJEKTU	
	NÁZEV PROJEKTU	
	ROZSAH PROJEKTU	
	ROLE NA PROJEKTU	
	DOBA TRVÁNÍ PROJEKTU	
	KONTAKTNÍ OSOBA (JMÉNO, TEL., EMAIL)	
14	OBJEDNATEL PROJEKTU	
	NÁZEV PROJEKTU	
	ROLE NA PROJEKTU	
	DOBA TRVÁNÍ PROJEKTU	
	KONTAKTNÍ OSOBA (JMÉNO, TEL., EMAIL)	
15	OBJEDNATEL PROJEKTU	
	NÁZEV PROJEKTU	
	ROZSAH PROJEKTU	
	ROLE NA PROJEKTU	
	DOBA TRVÁNÍ PROJEKTU	

Příloha B Přílohy č. 2 Dodatku č. 1 – Profesní profily osob Zhotovitele na pozici zástupce Incident Manažera

	KONTAKTNÍ OSOBA (JMÉNO, TEL., EMAIL)	[redacted]
16	OBJEDNATEL PROJEKTU	
	NÁZEV PROJEKTU	
	ROLE NA PROJEKTU	
	DOBA TRVÁNÍ PROJEKTU	
	KONTAKTNÍ OSOBA (JMÉNO, TEL., EMAIL)	
17	OBJEDNATEL PROJEKTU	
	NÁZEV PROJEKTU	
	ROLE NA PROJEKTU	
	DOBA TRVÁNÍ PROJEKTU	
	KONTAKTNÍ OSOBA (JMÉNO, TEL., EMAIL)	
18	OBJEDNATEL PROJEKTU	
	NÁZEV PROJEKTU	
	ROLE NA PROJEKTU	
	DOBA TRVÁNÍ PROJEKTU	
	KONTAKTNÍ OSOBA (JMÉNO, TEL., EMAIL)	
19	OBJEDNATEL PROJEKTU	
	NÁZEV PROJEKTU	
	ROLE NA PROJEKTU	
	DOBA TRVÁNÍ PROJEKTU	
	KONTAKTNÍ OSOBA (JMÉNO, TEL., EMAIL)	
20	OBJEDNATEL PROJEKTU	
	NÁZEV PROJEKTU	
	ROLE NA PROJEKTU	
	DOBA TRVÁNÍ PROJEKTU	
	KONTAKTNÍ OSOBA (JMÉNO, TEL., EMAIL)	
21	OBJEDNATEL PROJEKTU	
	NÁZEV PROJEKTU	
	ROZSAH PROJEKTU	
	ROLE NA PROJEKTU	

Příloha B Přílohy č. 2 Dodatku č. 1 – Profesní profily osob Zhotovitele na pozici zástupce Incident Manažera

	DOBA TRVÁNÍ PROJEKTU	[redacted]
	KONTAKTNÍ OSOBA (JMÉNO, TEL., EMAIL)	
22	OBJEDNATEL PROJEKTU	
	NÁZEV PROJEKTU	
	ROLE NA PROJEKTU	
	DOBA TRVÁNÍ PROJEKTU	
	KONTAKTNÍ OSOBA (JMÉNO, TEL., EMAIL)	
23	OBJEDNATEL PROJEKTU	
	NÁZEV PROJEKTU	
	ROLE NA PROJEKTU	
	DOBA TRVÁNÍ PROJEKTU	
	KONTAKTNÍ OSOBA (JMÉNO, TEL., EMAIL)	
24	OBJEDNATEL PROJEKTU	
	NÁZEV PROJEKTU	
	ROLE NA PROJEKTU	
	DOBA TRVÁNÍ PROJEKTU	
	KONTAKTNÍ OSOBA (JMÉNO, TEL., EMAIL)	

Příloha B Přílohy č. 2 Dodatku č. 1 – Profesní profily osob Zhotovitele na pozici zástupce Incident Manažera

JMÉNO OSOBY	[redacted]
ROLE NA PROJEKTU	**Incident Response Manager**
PROFESNÍ PRAXE	02/2025 - dosud Security Operations Center Specialist L3, Corpus Solutions a.s. 11/2023 - 11/2024 Cybersecurity engineer - SafeDX s.r.o., 11/2022 - 01/2023 IT Security analytik - Packeta innovations s.r.o., 12/2021 - 10/2022 Cybersecurity engineer, team leader - Cyber Fusion Centre, Accenture services, s.r.o., 01/2021 - 08/2021 Specialista informační bezpečnosti - PPL CZ s.r.o., 11/2016 - 06/2020 IT security administrator - Seznam.cz a.s., 01/2015 - 10/2016 IT specialista / teamleader - Scanservice a.s.,
POZICE VE FIRMĚ	**Security Operations Center Specialist L3**
KLÍČOVÉ ZNALOSTI	Rozsáhlé zkušenosti v oblasti kybernetické bezpečnosti Zaměření na návrh, implementaci a správu bezpečnostních systémů a strategií. řízení bezpečnostních incidentů, hodnocení souladu standardy, zavádění opatření ke zlepšení bezpečnostního postavení organizací, zkušenost s vedením týmů a strategické plánování bezpečnosti. Implementace bezpečnostní strategie. **Technologie**: MS Azure security technoogies, Microsoft 365 portfolio v rozsahu licence E5 i nadstavbových služeb (Office365, Exchange, Sharepoint, Teams, Intune MDM; Purview DLP, atd.) IBM Qradar – kompletní nasazení platformy Flowmon FMC / ADS / FTR / DDoS defender flow-based i ruční pcap analýza trafficu [Wireshark] NBA, monitoring a analytika, Threat Intel (Greycortex) Politiky / výjimky / compliance Alert management, incident handling & response Testování a analýza zabezpečení (Nessus / ZAP / Burp / Kali) Splunk - log management ESET - nasazení a správa řešení s cca 2000 endpointy Security Management Center, Endpoint security, File Security, Mail Security for MS Exchange,
DÉLKA PRAXE V OBORU ICT	[redacted]
NEJVYŠŠÍ DOSAŽENÉ VZDĚLÁNÍ	
POMĚR K DODAVATELI	Zaměstnanec

Příloha B Přílohy č. 2 Dodatku č. 1 – Profesní profily osob Zhotovitele na pozici zástupce Incident Manažera

1	OBJEDNATEL PROJEKTU	[redacted]
	NÁZEV PROJEKTU	
	ROLE NA PROJEKTU	
	DOBA TRVÁNÍ PROJEKTU	
	KONTAKTNÍ OSOBA (JMÉNO, TEL., EMAIL)	
2	OBJEDNATEL PROJEKTU	
	NÁZEV PROJEKTU	
	ROLE NA PROJEKTU	
	DOBA TRVÁNÍ PROJEKTU	
	KONTAKTNÍ OSOBA (JMÉNO, TEL., EMAIL)	
3	OBJEDNATEL PROJEKTU	
	NÁZEV PROJEKTU	
	ROLE NA PROJEKTU	
	DOBA TRVÁNÍ PROJEKTU	
	KONTAKTNÍ OSOBA (JMÉNO, TEL., EMAIL)	
4	OBJEDNATEL PROJEKTU	
	NÁZEV PROJEKTU	
	ROZSAH PROJEKTU	
	ROLE NA PROJEKTU	
	DOBA TRVÁNÍ PROJEKTU	
	KONTAKTNÍ OSOBA (JMÉNO, TEL., EMAIL)	

Příloha B Přílohy č. 2 Dodatku č. 1 – Profesní profily osob Zhotovitele na pozici zástupce Incident Manažera

JMÉNO OSOBY		[redacted]
ROLE NA PROJEKTU		**Incident Response Manager**
PROFESNÍ PRAXE		01/2025 - dosud SOC Specialist L3 / Teamleader, Corpus Solutions a.s. 01/2023 - 01/2025 Technický specialista SOC, Corpus Solutions a.s. 03/2010 - 12/2022 Gity a.s. – Konzultant bezpečnosti IT 01/2006 - 02/2010 2N Telekomunikace a.s. – technická podpora, technický produkt manager, školitel
POZICE VE FIRMĚ		**SOC Specialist L3 / Teamleader**
KLÍČOVÉ ZNALOSTI		SIEM – IBM security Qradar SIEM, Logmanager, Elastic XDR - Fidelis Vulnerability management – Nessus, Tenable SC, Tenable IO, R Programovací jazyky – Python, bash Operační systémy – Windows, Linux Správa MS Active Directory, MS Exchange, Hyper-V, VMware JIRA Service Desk, Zabbix Síťové technologie – Fortinet Fortigate, CISCO, HP/Aruba
CERTIFIKACE		GIAC Cloud Forensics Responder TeskaLabs LogMan.io, LogMan.io PLUS a TeskaLabs SIEM IBM Certified Analyst - Security QRadar SIEM V7.5
DÉLKA PRAXE V OBORU ICT		[redacted]
NEJVYŠŠÍ DOSAŽENÉ VZDĚLÁNÍ		[redacted]
POMĚR K DODAVATELI		Zaměstnanec
1	OBJEDNATEL PROJEKTU	[redacted]
	NÁZEV PROJEKTU	
	ROZSAH PROJEKTU	
	ROLE NA PROJEKTU	
	DOBA TRVÁNÍ PROJEKTU	
	KONTAKTNÍ OSOBA (JMÉNO, TEL., EMAIL)	
2	OBJEDNATEL PROJEKTU	
	NÁZEV PROJEKTU	
	ROLE NA PROJEKTU	
	DOBA TRVÁNÍ PROJEKTU	

Příloha B Přílohy č. 2 Dodatku č. 1 – Profesní profily osob Zhotovitele na pozici zástupce Incident Manažera

	KONTAKTNÍ OSOBA (JMÉNO, TEL., EMAIL)	[redacted]
3	OBJEDNATEL PROJEKTU	
	NÁZEV PROJEKTU	
	ROLE NA PROJEKTU	
	DOBA TRVÁNÍ PROJEKTU	
	KONTAKTNÍ OSOBA (JMÉNO, TEL., EMAIL)	
4	OBJEDNATEL PROJEKTU	
	NÁZEV PROJEKTU	
	ROLE NA PROJEKTU	
	DOBA TRVÁNÍ PROJEKTU	
	KONTAKTNÍ OSOBA (JMÉNO, TEL., EMAIL)	
5	OBJEDNATEL PROJEKTU	
	NÁZEV PROJEKTU	
	ROZSAH PROJEKTU	
	ROLE NA PROJEKTU	
	DOBA TRVÁNÍ PROJEKTU	
	KONTAKTNÍ OSOBA (JMÉNO, TEL., EMAIL)	
6	OBJEDNATEL PROJEKTU	
	NÁZEV PROJEKTU	
	ROZSAH PROJEKTU	
	ROLE NA PROJEKTU	
	DOBA TRVÁNÍ PROJEKTU	
	KONTAKTNÍ OSOBA (JMÉNO, TEL., EMAIL)	
7	OBJEDNATEL PROJEKTU	
	NÁZEV PROJEKTU	
	ROZSAH PROJEKTU	

Příloha B Přílohy č. 2 Dodatku č. 1 – Profesní profily osob Zhotovitele na pozici zástupce Incident Manažera

		[redacted]
	ROLE NA PROJEKTU	
	DOBA TRVÁNÍ PROJEKTU	
	KONTAKTNÍ OSOBA (JMÉNO, TEL., EMAIL)	
8	OBJEDNATEL PROJEKTU	
	NÁZEV PROJEKTU	
	ROZSAH PROJEKTU	
	ROLE NA PROJEKTU	
	DOBA TRVÁNÍ PROJEKTU	
	KONTAKTNÍ OSOBA (JMÉNO, TEL., EMAIL)	
9	OBJEDNATEL PROJEKTU	
	NÁZEV PROJEKTU	
	ROLE NA PROJEKTU	
	DOBA TRVÁNÍ PROJEKTU	
	KONTAKTNÍ OSOBA (JMÉNO, TEL., EMAIL)	
10	OBJEDNATEL PROJEKTU	
	NÁZEV PROJEKTU	
	ROZSAH PROJEKTU	
	ROLE NA PROJEKTU	
	DOBA TRVÁNÍ PROJEKTU	
	KONTAKTNÍ OSOBA (JMÉNO, TEL., EMAIL)	
11	OBJEDNATEL PROJEKTU	
	NÁZEV PROJEKTU	
	ROZSAH PROJEKTU	

Příloha B Přílohy č. 2 Dodatku č. 1 – Profesní profily osob Zhotovitele na pozici zástupce Incident Manažera

		[redacted]
	ROLE NA PROJEKTU	
	DOBA TRVÁNÍ PROJEKTU	
	KONTAKTNÍ OSOBA (JMÉNO, TEL., EMAIL)	
12	OBJEDNATEL PROJEKTU	
	NÁZEV PROJEKTU	
	ROLE NA PROJEKTU	
	DOBA TRVÁNÍ PROJEKTU	
	KONTAKTNÍ OSOBA (JMÉNO, TEL., EMAIL)	
13	OBJEDNATEL PROJEKTU	
	NÁZEV PROJEKTU	
	ROZSAH PROJEKTU	
	ROLE NA PROJEKTU	
	DOBA TRVÁNÍ PROJEKTU	
	KONTAKTNÍ OSOBA (JMÉNO, TEL., EMAIL)	
14	OBJEDNATEL PROJEKTU	
	NÁZEV PROJEKTU	
	ROLE NA PROJEKTU	
	DOBA TRVÁNÍ PROJEKTU	
	KONTAKTNÍ OSOBA (JMÉNO, TEL., EMAIL)	
15	OBJEDNATEL PROJEKTU	
	NÁZEV PROJEKTU	
	ROZSAH PROJEKTU	
	ROLE NA PROJEKTU	
	DOBA TRVÁNÍ PROJEKTU	
	KONTAKTNÍ OSOBA (JMÉNO, TEL., EMAIL)	
16	OBJEDNATEL PROJEKTU	
	NÁZEV PROJEKTU	
	ROZSAH PROJEKTU	

Příloha B Přílohy č. 2 Dodatku č. 1 – Profesní profily osob Zhotovitele na pozici zástupce Incident Manažera

	ROLE NA PROJEKTU	[redacted]
	DOBA TRVÁNÍ PROJEKTU	
	KONTAKTNÍ OSOBA (JMÉNO, TEL., EMAIL)	
17	OBJEDNATEL PROJEKTU	
	NÁZEV PROJEKTU	
	ROZSAH PROJEKTU	
	ROLE NA PROJEKTU	
	DOBA TRVÁNÍ PROJEKTU	
	KONTAKTNÍ OSOBA (JMÉNO, TEL., EMAIL)	
18	OBJEDNATEL PROJEKTU	
	NÁZEV PROJEKTU	
	ROLE NA PROJEKTU	
	DOBA TRVÁNÍ PROJEKTU	
	KONTAKTNÍ OSOBA (JMÉNO, TEL., EMAIL)	
19	OBJEDNATEL PROJEKTU	
	NÁZEV PROJEKTU	
	ROZSAH PROJEKTU	
	ROLE NA PROJEKTU	
	DOBA TRVÁNÍ PROJEKTU	
	KONTAKTNÍ OSOBA (JMÉNO, TEL., EMAIL)	
20	OBJEDNATEL PROJEKTU	
	NÁZEV PROJEKTU	
	ROZSAH PROJEKTU	
	ROLE NA PROJEKTU	
	DOBA TRVÁNÍ PROJEKTU	
	KONTAKTNÍ OSOBA (JMÉNO, TEL., EMAIL)	
21	OBJEDNATEL PROJEKTU	
	NÁZEV PROJEKTU	

Příloha B Přílohy č. 2 Dodatku č. 1 – Profesní profily osob Zhotovitele na pozici zástupce Incident Manažera

	ROLE NA PROJEKTU
	DOBA TRVÁNÍ PROJEKTU
	KONTAKTNÍ OSOBA (JMÉNO, TEL., EMAIL)

PŘÍLOHA Č. 9 – KONTAKTNÍ ÚDAJE

Adresa pro doručování.

(a) Adresa pro doručování Objednateli:

ČEPRO, a.s.
Dělnická 213/12
170 00 Praha 7
Datová schránka: hk3cdqj

ve věcech smluvních:

[redacted]

ve věcech technických:

[redacted]

(b) Adresa pro doručování Zhotoviteli:

Corpus Solutions, a.s.
Štětkova 1638/18
Praha 4, 140 00
Datová schránka: 2xhpac2

ve věcech smluvních:

Příloha č. 3 Dodatku č. 1 - nová příloha č. 9 Smlouvy – Kontaktní údaje

ve věcech technických:

PŘÍLOHA Č. 7 – SLUŽBY ÚDRŽBY A TECHNICKÉ PODPORY

1. SPECIFIKACE POŽADAVKŮ NA SLA 1 – SLUŽBA „TECHNICKÁ PODPORA HW ŘEŠENÍ“

Předmětem služby podpory HW je servisní podpora výrobce všech dodaných hardwarových technologií řešení (např. servery, síťové prvky, apod.) vč. všech souvisejících softwarových komponent (mikrokódy, firmware, řídící software), které tvoří nedílnou součást dané HW technologie. Tuto službu požaduje objednatel zajistit nejen jako reaktivní, ale i proaktivní podporu (pravidelné upgrade na aktuální verze firmware, patch analýzy apod.).

Klíčové činnosti služby

- zajištění diagnostiky a asistence při určování, zda se jedná o HW nebo SW problém na místě plnění služby v příslušné lokalitě
- zajištění servisu vadných komponent a technologií v místě instalace, odstranění problému na všech dodaných HW zařízeních dle provedené diagnostiky včetně problémů v konfiguraci a uvedení do původního stavu před vznikem incidentu a dle specifikace zařízení, fyzická výměna všech nefunkčních komponent nebo celého zařízení a provedení jeho konfigurace či rekonfigurace
- plánování, rozvržení a instalace oprav dle specifikace výrobce, dále diagnostiku chybových stavů a aplikace mikrokódových změn včetně jejich aktualizace
- zasílání oznámení o dostupnosti opravných softwarových balíků (preventivní a opravné softwarové balíky) včetně jejich elektronického či fyzického dodání na datovém nosiči
- eskalace potenciálních problémů středisku podpory konkrétního výrobce dodaného HW

Požadované parametry služby

Rozsah zaručeného provozu služby		**Doba odezvy**
8:00 – 16:00 hod (5 x 8)		2 hodiny
Rozsah služby: cca 4 hodiny měsíčně		
Doba poskytnutí služby:		
Vysoká priorita	**Střední priorita**	**Nízká priorita**
do konce následujícího pracovního dne	do konce druhého pracovního dne	do konce pátého pracovního dne

2. SPECIFIKACE POŽADAVKŮ NA SLA 2 – SLUŽBA „TECHNICKÁ PODPORA SW ŘEŠENÍ“

Služba podpory k dodanému komerčnímu SW představuje plnění, které se skládá z podpory výrobce všech dodaných softwarových technologií a řešení (OS, virtualizace, zálohování atd.).

Klíčové činnosti služby

- zajištění diagnostiky a asistence při určování, zda se jedná o HW nebo SW problém na místě plnění služby v příslušné lokalitě
- zajištění servisu vadných SW komponent a technologií v místě instalace, odstranění problému na všech dodaných SW technologií a řešení na zařízeních dle provedené diagnostiky včetně problémů v konfiguraci a uvedení do původního stavu před vznikem incidentu a dle specifikace zařízení, fyzická instalace a/nebo reinstalace všech nefunkčních SW komponent nebo celého řešení a provedení jeho konfigurace či rekonfigurace
- plánování, rozvržení a instalace oprav dle specifikace výrobce, dále diagnostiku chybových stavů a aplikace opravných softwarových balíků včetně aktualizace

- zasílání oznámení o dostupnosti opravných softwarových balíků (preventivní a opravné softwarové balíky) včetně jejich elektronického či fyzické dodání na datovém nosiči
- eskalace potenciálních problémů středisku podpory konkrétního výrobce dodaného SW

Požadované parametry služby

Rozsah zaručeného provozu služby		**Doba odezvy**
8:00 – 16:00 hod (5 x 8)		2 hodiny
Rozsah služby: cca 8 hodin měsíčně		
Doba poskytnutí služby:		
Vysoká priorita	**Střední priorita**	**Nízká priorita**
do konce následujícího pracovního dne	do konce druhého pracovního dne	do konce pátého pracovního dne

3. SPECIFIKACE POŽADAVKŮ NA SLA 3 – SLUŽBA „KONZULTACE A PRÁCE NA VYŽÁDÁNÍ“

Služba "konzultace a práce na vyžádání" představuje plnění, které se skládá z:

- aktivní konzultační technické podpory dodaného řešení (technické a metodické otázky související s provozem a rozvojem dodaného řešení), nebo
- provedení konkrétní činnosti související s provozem dodaného řešení, a to na vyžádání (např. telefonicky, emailem, apod.)
  - na dálku (např. telefonicky, emailem, apod.) nebo
  - přímo v místě instalace technologií.

Klíčové činnosti služby jsou zejména:

- odborná pomoc při rekonfiguraci řešení dle požadavků Objednatele
- odborná pomoc při konfiguraci a rekonfiguraci komponent dle požadavků Objednatele a doporučení výrobce;
- řešení konfiguračních prací, konzultační činnost k zajištění maximálního efektu využití všech prvků dodané řešení, jejich optimalizaci, možnosti další integrace a ujednocení postupů při vyšetřování kybernetických bezpečnostních incidentů a následné remediaci, vytváření automatizovaných procesů pro bezpečnostní dohled a řešení alertů, optimalizaci pracovních postupů a nastavení reportingu;
- odborná pomoc při rozvoji řešení;
- odborná pomoc při návrhu změn v architektuře/konfiguraci ICT infrastruktury na základě výsledků bezpečnostního dohledu, identifikovaných rizik nebo výsledků penetračních testů;
- odbornou asistenci zhotovitele při provádění analýz reportingu událostí, alertů a incidentů, a jejich trendů;
- odborná pomoc při tvorbě pomocné dokumentace (např. návrhy pro optimalizaci provozu technologií, návrhy opatření proti vzniku nestandardních stavů, odborná pomoc při zpracování projektové bezpečnostní dokumentace, případně odborná pomoc při zpracování provozní bezpečnostní dokumentace;
- pracovníci dodavatele budou na vyžádání Objednatele zajišťovat součinnost nebo odbornou asistenci související se nestandardními stavy při provozu řešení.

Požadované parametry služby

Rozsah zaručeného provozu služby	**Doba odezvy**
8:00 – 16:00 hod (5 x 8)	2 hodiny
Rozsah služby	
cca 24 hod. měsíčně	
Doba poskytnutí služby (zahájení činností): do dvou pracovních dnů	

4. SPECIFIKACE POŽADAVKU NA SLUŽBU MAINT – SLUŽBA „TECHNOLOGICKÁ A LICENČNÍ ÚDRŽBA ŘEŠENÍ“

Cílem této služby je zajistit údržbu a aktualizace dodaného řešení zejména v následujících oblastech:

- produktové aktualizace – dodávky a přístup k nejaktuálnějším verzím produktů (revize a aktuální verze);
- servisní aktualizace – odstraňování závad produktů, včetně aktualizací případných použitých operačních systémů;
- bezpečnostní aktualizace – dodávky a přístup (včetně automatizace procesu aktualizace) k nejnovějším databázím a popisům hrozeb (tzv. threat intel) pro systém ochrany proti APT útokům, popisům zranitelností SW a HW apod.;
- antivirová aktualizace – dodávky a přístup k aktualizacím databází antivirového řešení včetně automatizace procesu aktualizace;
- poskytování přístupu a práva k užití služeb výrobce poskytovaných na dálku (portál technické podpory, znalostní báze, specializovaným vzdáleným službám apod.).