Návrh Smlouvy o poskytování služeb

Níže uvedeného dne, měsíce a roku uzavřely tyto smluvní strany

Město Mikulov

Sídlo: Náměstí 1 692 20 Mikulov

IČO: 00283347

DIČ: CZ00283347

Zastoupen: Mgr. Jitka Sobotková, starostka města

Číslo smlouvy objednatele: SML2200256

(dále jen „**Objednatel**")

a

VISITECH, a.s.

Sídlo: Košinova 655/59, 612 00 Brno, Královo pole

IČO: 25543415

DIČ: CZ25543415

Zastoupen: Pavel Kocour, předseda představenstva

Číslo smlouvy poskytovatele: SOD/2112/2022/LB

(dále jen „**Poskytovatel**")

v souladu s ust. § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, tuto smlouvu (dále jen „**Smlouva**").

1. ÚVODNÍ USTANOVENÍ

1.1 Objednatel prohlašuje, že je právnickou osobou řádně založenou a existující podle českého právního řádu, splňuje veškeré podmínky a požadavky v této Smlouvě stanovené a je oprávněn tuto Smlouvu uzavřít a řádně plnit závazky v ní obsažené.

1.2 Poskytovatel prohlašuje, že je právnickou osobou řádně založenou a existující podle českého právního řádu, splňuje veškeré podmínky a požadavky v této Smlouvě stanovené a je oprávněn tuto Smlouvu uzavřít a řádně plnit závazky v ní obsažené.

2. PŘEDMĚT SMLOUVY

2.1 Poskytovatel se na základě této Smlouvy zavazuje poskytovat Objednateli službu „Dohledového centra kybernetické bezpečnosti (SOC)", specifikované v příloze č. 1 této Smlouvy (dále jen „**Služba**"). Součástí plnění Poskytovatele podle této Smlouvy je zřízení Služby za podmínek vymezených v čl. 4 této Smlouvy.

2.2 Služba specifikovaná v příloze č. 1 této Smlouvy se v textu Smlouvy dále společně označují jako „**Služby**".

2.3 Objednatel se zavazuje poskytnuté plnění převzít za podmínek stanovených touto Smlouvou, uhradit Poskytovateli za poskytnuté plnění cenu sjednanou v této Smlouvě a poskytnout mu veškerou součinnost potřebnou k poskytování plnění.

3. MÍSTO PLNĚNÍ

3.1 Služby mohou být poskytovány v místě sídla Objednatele, v provozovnách Objednatele, na jejichž specifikaci se strany domluví, a dále v provozovnách Poskytovatele.

3.2 Pokud to povaha plnění nevylučuje, je Poskytovatel oprávněn poskytovat své plnění vzdáleným přístupem. Objednatel se zavazuje poskytnout Poskytovateli veškerou součinnost potřebnou k poskytování Služeb v souladu s podmínkami dle předchozí věty.

4. PODMÍNKY POSKYTOVÁNÍ SLUŽEB

4.1 Poskytovatel se zavazuje zřídit Službu nejpozději do 30 dnů ode dne nabytí účinnosti této Smlouvy. Zřízením Služby se rozumí vytvoření technických podmínek nezbytných pro řádné poskytování Služby.

4.2 Služba bude Poskytovatelem poskytována průběžně, a to ode dne následujícího po zřízení Služby Poskytovatelem.

4.3 Objednatel zajistí potřebné podmínky, organizační opatření a případnou součinnost svých pracovníků tak, aby Poskytovatel mohl bez překážek provádět potřebné úkony a činnosti pro zajištění Služby.

5. CENA A PLATEBNÍ PODMÍNKY

5.1 Cena za Službu je sjednána v příloze č. 2 této Smlouvy. Cena za Službu bude Objednatelem uhrazena na základě faktury, kterou je Poskytovatel oprávněn vystavit vždy v poslední den daného kalendářního měsíce ve kterém byly Služby poskytnuty.

5.2 Cena za dílo obsahuje veškeré náklady Poskytovatele spojené se splněním jeho závazků (zahrnuje cenu veškeré práce, úkony, činnosti, úpravy a náklady).

5.3 Změna (překročení) nabídkové ceny je možná pouze v případě, že v průběhu platnosti smlouvy dojde ke změnám sazeb DPH. V tomto případě bude k nabídkové ceně na základě

smlouvy účtována DPH ve výši podle právních předpisů platných v době vzniku zdanitelného plnění.

5.4 Není-li v příloze č. 2 této Smlouvy výslovně uvedeno jinak, jsou veškeré ceny tam uvedené stanoveny bez DPH. DPH bude Poskytovatelem účtována v souladu s platnými a účinnými právními předpisy.

5.5 Splatnost faktur činí 30 dní ode dne jejich vystavení. Poskytovatel doručí Objednateli veškeré jím vystavené faktury do 5 pracovních dnů ode dne jejich vystavení. V případě, že faktura nebude doručena ve lhůtě uvedené v předchozí větě, doba splatnosti se přiměřeným způsobem posouvá.

5.6 Poskytovatel je oprávněn přerušit poskytování Služeb v případě, že se Objednatel dostane do prodlení s plněním jeho finančních závazků dle této Smlouvy. Poskytovatel v takovém případě není v prodlení s poskytováním Služeb.

5.7 Objednatel neposkytuje zálohy.

5.8 Faktura musí obsahovat všechny náležitosti řádného účetního a daňového dokladu.

5.9 V případě, že faktura nebude mít odpovídající náležitosti, je objednatel oprávněn zaslat ji ve lhůtě splatnosti zpět poskytovateli k doplnění nebo opravě. Nová lhůta splatnosti počíná běžet od data doručení doplněné nebo opravené faktury.

5.10 Platba bude uskutečněna formou převodu finančních prostředků na účet Poskytovatele. Termínem úhrady se rozumí den odepsání finančních prostředků z účtu Objednatele.

6. ODPOVĚDNOST ZA ÚJMU

6.1 Obě strany se zavazují k vyvinutí maximálního úsilí k předcházení škodám a k minimalizaci vzniklých škod.

6.2 Žádná ze smluvních stran neodpovídá za újmu, která vznikla v důsledku věcně nesprávného nebo jinak chybného zadání, které obdržela od druhé smluvní strany.

6.3 Smluvní strany se dohodly, že celková výše náhrady újmy, kterou může smluvní strana požadovat po druhé smluvní straně v souvislosti s porušením této Smlouvy, se omezuje do výše celkové ceny za poskytování Služby bez DPH. Ujednání dle předchozí věty se nevztahuje na újmu způsobenou člověku na jeho přirozených právech, anebo způsobenou úmyslně nebo z hrubé nedbalosti.

7. OCHRANA INFORMACÍ

7.1 Žádná ze smluvních stran nesmí zpřístupnit třetí osobě důvěrné informace, které při plnění této Smlouvy získala od druhé smluvní strany v souvislosti s plněním této Smlouvy. To neplatí, mají-li být za účelem plnění této Smlouvy potřebné informace zpřístupněny zaměstnancům smluvních stran, jejich orgánům nebo jejich členům nebo subdodavatelům smluvních stran.

7.2 Za důvěrné informace jsou dle této Smlouvy smluvními stranami považovány veškeré informace poskytnuté vzájemně, zejména informace smluvních stran, které se strany dozvěděly v souvislosti s touto Smlouvou, jakož i know-how, jímž se rozumí veškeré poznatky obchodní, výrobní, technické či ekonomické povahy související s činností smluvní strany, které mají skutečnou nebo alespoň potenciální hodnotu a které nejsou v

příslušných obchodních kruzích běžně dostupné a mají být utajeny, a to za předpokladu, že jsou předmětné informace označeny jako důvěrné informace. Za důvěrné informace se výslovně považují rovněž veškerá uživatelská data, údaje či informace, obsažené v informačních systémech, jichž se plnění této Smlouvy dotýká.

7.3 Bez ohledu na výše uvedená ustanovení se za důvěrné nepovažují informace:

7.3.1 které se staly veřejně známými, aniž by to zavinila záměrně či nedbalostně přijímající strana,

7.3.2 které měla přijímající strana legálně k dispozici před uzavřením této Smlouvy, pokud takové informace nebyly předmětem jiné, dříve mezi stranami uzavřené smlouvy o ochraně informací,

7.3.3 které jsou výsledkem postupu, při kterém k nim přijímající strana dospěje nezávisle a je to schopna doložit svými záznamy nebo důvěrnými informacemi třetí strany,

7.3.4 které poskytne přijímající straně třetí osoba, jež takové informace přitom nezíská přímo ani nepřímo od strany, jež je jejich vlastníkem.

7.4 Za porušení povinnosti chránit důvěrné informace se nepovažuje zpřístupnění důvěrných informací třetí osobě:

7.4.1 jsou-li poskytovány ekonomickým, daňovým a právní poradcům smluvních stran a přijímající strana nezbaví tyto osoby povinnosti mlčenlivosti,

7.4.2 je-li jejich zveřejnění nezbytné k tomu, aby se smluvní strana mohla domáhat ochrany svých práv u soudu nebo rozhodčího soudu,

7.4.3 je-li jejich zveřejnění důvodně vyžadováno zákonem či pravomocným rozhodnutím orgánu státní správy, obecných či rozhodčích soudů.

7.5 Obě smluvní strany se zavazují nakládat s důvěrnými informacemi, které jim byly poskytnuty druhou smluvní stranou nebo je jinak získaly v souvislosti s plněním této Smlouvy, jako s obchodním tajemstvím; zavazují se zejména uchovávat je v tajnosti a učinit veškerá smluvní a technická opatření zabraňující jejich zneužití či prozrazení.

7.6 Povinnost utajovat důvěrné informace zavazuje smluvní strany po dobu účinnosti této Smlouvy a pět let po ukončení její účinnosti.

8. TRVÁNÍ SMLOUVY

8.1 Tato Smlouva se uzavírá na dobu určitou 24 měsíců a nabývá účinnosti od 1. 1. 2023.

8.2 Objednatel je oprávněn odstoupit od Smlouvy v případě, že Poskytovatel je v prodlení s plněním povinností dle této Smlouvy déle než 30 dnů a nezjedná nápravu ani do 30 dnů od doručení písemné výzvy Objednatele k odstranění tohoto prodlení, přičemž za prodlení Poskytovatele se nepovažuje pozastavení poskytování Služeb dle odst. 5.6 této Smlouvy.

8.3 Poskytovatel je oprávněn odstoupit od Smlouvy v případě, že Objednatel je v prodlení s plněním svých peněžitých závazků z této Smlouvy déle než 30 dnů.

8.4 V případě odstoupení od Smlouvy kteroukoliv smluvní stranou tato Smlouva zaniká ke dni doručení odstoupení druhé smluvní straně. Smluvní strany vylučují aplikaci § 2004 odst. 1 občanského zákoníku.

8.5 Ukončením účinnosti této Smlouvy z jakéhokoliv důvodu není dotčeno právo Poskytovatele na úhradu ceny již poskytnutého plnění.

8.6 Ukončení účinnosti této Smlouvy se nedotýká ujednání o náhradě újmy, ochraně informací, řešení sporů, ani ujednání, z jejichž povahy vyplývá, že mají trvat i po dobu po ukončení této Smlouvy.

9. ZÁVĚREČNÁ USTANOVENÍ

9.1 Tato Smlouva představuje úplnou dohodu smluvních stran o předmětu Smlouvy, přičemž tuto Smlouvu je možné měnit pouze písemnou dohodou smluvních stran ve formě číslovaných dodatků, oboustranně odsouhlasených a podepsaných oprávněnými zástupci obou smluvních stran.

9.2 Pokud by se kterékoliv ustanovení Smlouvy ukázalo být neplatným z důvodu rozporu s kogentním ustanovením obecně závazných právních předpisů, pak tato skutečnost nepůsobí neplatnost než onoho konkrétního ustanovení. Smluvní strany se zavazují takové neplatné ustanovení dohodou nahradit ustanovením svým obsahem nejbližším duchu takového neplatného ustanovení, respektujícím požadavky kogentních ustanovení právních předpisů.

9.3 Nedílnou součást Smlouvy tvoří tyto přílohy:

Příloha č. 1 – Specifikace Služeb

Příloha č. 2 – Cena Služeb

9.3.1 Objednatel podpisem této Smlouvy potvrzuje, že se s jejím obsahem řádně seznámil, její ustanovení jsou mu srozumitelná a plně s nimi souhlasí. Smluvní strany tímto v souladu s § 1801 občanského zákoníku, vylučují aplikaci ustanovení § 1799 a § 1800 občanského zákoníku.

9.4 O uzavření Smlouvy za podmínek v ní uvedených, rozhodla starostka Města Mikulov na základě článku V. odst. 1 písm. a3) Vnitřní směrnice Městského úřadu č. 3/2020/R pro zadávání veřejných zakázek orgány Města Mikulov, schválené radou města na její schůzi konané dne 8. 6. 2020, v platném znění.

9.5 Smlouva byla vyhotovena a smluvními stranami podepsána ve dvou (2) vyhotoveních, z nichž každá ze smluvních stran obdrží po jednom (1) vyhotovení.

Objednatel:

V Mikulově

[redacted]

MĚSTO MIKULOV
Mgr. Jitka Sobotková

Poskytovatel:

V Brně

[redacted]

VISITECH, a.s.
Pavel Kocour

Příloha č. 1
Specifikace služeb

A. Paušální služby

Dohledové centrum kybernetické bezpečnosti (SOC)

Předmětem služby je zajištění služeb dohledového centra kybernetické bezpečnosti (SOC – Security Operation Centrum), především:

Popis služby SOC365
V rámci služby bude Poskytovatelem služby vytvořeno bezpečné uložiště pro sdílení kompletních materiálů k poskytované službě.
Síťový dohled Zajištění centralizované správy, ukládání a vyhodnocování komunikačních spojení a výkonnostních parametrů datové sítě
Bezpečnostní dohled Zajištění správy a provozu nástroje SIEM, který bude dodán a implementován společně s poskytnutou službou bezpečnostního dohledového centra.
Incident management Zajištění Operátorské činnosti, Incident handling, Incident Response.
Analýza incidentů Zajištění odborné činnosti v detekci a lokalizaci příčin incidentů Analytikem incidentů ze strany Poskytovatele služby.
Návrhy systematických opatření Sestavení opatření na organizační a technické úrovni pro posouzení Objednatelem.
Návrhy řešení incidentů Zajištění odborné činnosti pro kategorizaci na interní a externí příčiny incidentů a k nim příslušných opatření.
Reporting a analýza stavů, událostí a incidentů Zajištění odborné činnosti pro doložení úrovně bezpečnosti vůči interním kontrolním procesům nebo pro doložení vůči externím kontrolním autoritám.
Kybernetická bezpečnost Personální zajištění služby pracovníky s odbornou způsobilostí vyhovující požadavkům na zajištění kybernetické bezpečnosti v souladu s požadavky *zákona 181/2014Sb. o kybernetické bezpečnosti* v celém průběhu služby a všech jejích procesů a rutin.
Business Continuity Služba (včetně všech komponent, které využívá) musí být odolná proti výpadkům a poruchám. Všechny komponenty služby musí být schopny dlouhodobého provozu bez změny chování a úbytku výkonu.
Zajištění souladu se zákonem ZoKB (Compliance) Všechny parametry služby musí zajistit na úrovni technologií i procesů splnění požadavků na zajištění potřebné míry informační bezpečnosti, zejména pak: Důvěrnost, Dostupnost, Nepopíratelnost, Autentizaci, Autorizaci.
Adaptace a akceptace sdílených procesů Služba zajistí úpravu procesů na straně poskytovatele služby a návrh na jejich integraci s relevantními procesy na straně Objednatele.
SLA procesních vstupů a výstupů Služba zajistí monitoring procesů na straně Poskytovatele služby i Objednatele.
Vizitace zadavatele v místě výkonu služby Poskytovatel služby před podpisem smlouvy umožní Objednateli návštěvu vlastního bezpečnostního dohledového centra, aby si mohl ověřit splnění požadavků. Zjištění nedodržení požadavků je důvod pro vyloučení Poskytovatele služby.
Poskytovatel služby provozuje vlastní Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních

událostí.
V rámci služby Poskytovatel zajistí *provozní monitoring* bezpečnostních nástrojů, dle předmětu zakázky, v rozsahu: • dostupnost a funkčnost bezpečnostních nástrojů, • vytíženost bezpečnostních nástrojů, • detekce vyčerpání kapacitních zdrojů u bezpečnostních nástrojů.
V rámci služby Poskytovatel zajišťuje *nastavování bezpečnostních nástrojů*, dle předmětu zakázky, v rozsahu: • úprava a optimalizace korelačních pravidel, dle požadavků Objednatele nebo dle best-practice Poskytovatele, • přidávání nových zařízení pro bezpečnostní monitoring, • vytváření nových scénářů pro detekci, • úprava nastavení nástrojů, dle požadavku Objednatele nebo NÚKIB. Pro některé úkony v rámci *nastavování bezpečnostních nástrojů* může být vyžadována součinnost Objednatele (např. při napojování nových zdrojů logů,…).
Podpora SOC365
Tiketovací systém Služba s on-line přístupem pro kompletní správu požadavků, včetně uchování historie požadavků a jejich řešení.
Přístup Objednatele k podpoře *provozu systémů* – Helpdesk
Přístup Objednatele k podpoře *Incident Response* – Helpdesk, telefon/ email na členy CSIRT
Proaktivní komunikace. Zakládání tiketů a jejich řešení. Komunikace s třetí stranou jako NBÚ, NÚKIB, kooperující CSIRT atd.
Přístup *administrátorů Zadavatele* ke sledovaným parametrům služby prostřednictvím grafického rozhraní (GUI – dashboard apod.), alespoň v režimu čtení nebo v přístupové roli *Auditor*.
Notifikace/Eskalace Informování odpovědných osob Objednatele o vzniku bezpečnostního incidentu v reálném čase za pomocí základních komunikačních nástrojů (mail / SMS / telefon).
Vulnerability management Služba musí zajistit kontinuální skenování aktiv Objednatele definovaných danou sítí/sítěmi a zranitelnostmi relevantními pro daná aktiva. Minimálně na začátku poskytování služby budou provedeny a vyhodnoceny plné skeny a dále vždy 1x měsíčně skeny rozdílové.
Reporty – ***Standard*** Poskytovatel v rámci služby zpracuje a poskytne zadavateli 1x za 2 měsíce Report, ve kterém je popsáno: • průběh realizace Plnění služby za uplynulé období; • provedené služby za uplynulé období; • návrh doporučených opatření pro další období pro zvýšení bezpečnosti, dostupnosti a prevenci eliminace incidentů.
Reporty – Rozšířený *reporting* Detailní report o událostech a incidentech s návrhy systematických opatření 1x za 2 měsíce. Vzdálená prezentace reportu, např. formou videokonference. Prezentace čtvrtletních reportů v rozsahu min. 30 min, max. 2 hod.
Reporty – ***on-demand*** Služba zajistí na vyžádání provádění on-demand spouštění některých pravidel a z výstupu bude vytvářet reporty.
Technologie sběru dat Služba zajistí zprovoznění nástrojů SIEM pro sběr a vyhodnocení síťového provozu jako základního zdroje dat a bude s nimi komunikovat průmyslově standardními protokoly. Navrhované řešení Poskytovatele služby: • zajišťuje na straně Poskytovatele sběr, přenos a uložení logů a jejich vyhodnocování a korelaci v rámci nástroje SIEM nasazeným v infrastruktuře Objednatele.

Base line analýza
Služba zajistí porovnání neobvyklých počtů určitých událostí oproti jinému období z minulosti.

Kategorizace aktiv
Služba zajistí jednotnou evidenci a vyhodnocení kategorií aktiv. Podle těchto kategorií bude poskytovatel služby utvářet další pravidla nebo reporty v prostředcích Objednatele.

Služba Monitoring Privilegovaných účtů – Sdílené *účty*
Služba musí umožnit detekci užití privilegovaných přístupů pro konkrétního uživatele v systémech Objednatele.

Režim Maintenance
Služba musí být schopna běhu v režimu údržby ohlášenou Objednatelem, kdy se údržbou dotčených zdrojů/aktiv nebudou vyhlašovat alerty.

Proaktivní ochrana
Monitoring sítě s proaktivní ochranou sítě a blokováním komunikace útočníků do i z internetu.

Služba Monitoringu a detekce

- Průběžné sledování provozu prostředí Objednatele.
- Real-time analýza situace v napojených nástrojích podle skupin, kategorií zařízení a podle kontextu log záznamů nebo událostí.
- 2x denně odborné posouzení bezpečnostní situace a provozního stavu. V případě anomálie posouzení její relevance a závažnosti.
- Posouzení kontextu anomálie a příčin vzniku situace s případnou eskalací problému Objednatele na analytického specialistu Poskytovatele služby.

Služba včasné výstrahy a reakce na nestandardní situace v provozu bezpečnostních systémů

- Zpracování analytických scénářů na aktuální kybernetické hrozby.
- Posouzení eskalovaného problému Objednatele analytickým specialistou Poskytovatele.
- Detekce a vyhodnocení závažnosti identifikovaných anomálií.
- Posouzení a případná eskalace nestandardní situace v provozu Objednatele na službu včasné výstrahy a reakce na incident v rámci bezpečnostních struktur ČR.

SLA

Poskytovatel služby musí provozovat vlastní bezpečnostní dohledovou službu v režimu 24x7x365 na úrovni systémů, s minimální dostupností operátorů SOC v pracovní dny od 9:00 do 17:00 hodin a s minimální dostupností Analytiků/expertů bezpečnosti v pracovní dny od 9:00 do 17:00 hodin.

Pro detekované anomálie v bezpečnostních nástrojích prochází Poskytovatel služby následným postupem k určení kategorií kybernetických bezpečnostních událostí a incidentů (dle §31, VoKB) podle následků a negativních projevů pro doporučení opatření či součinnosti v následné reakci:

<u>Fáze Detekce</u>

- Monitoring prostředí vymezeného Objednatelem.
- Dohledování bezpečnostní situace Objednatele.
- Detekce anomálie – rozpoznání odchylky od běžného stavu nebo od Objednatelem normovaného stavu.

<u>Fáze Přiřazení</u>

- Klasifikace anomálie – určení závažnosti ve škále:
    - False-Positive Alarm – způsobuje falešný alarm z důvodu:
        - chyby v úsudku míry závažnosti anomálie;
        - nepřesnosti rozpoznání odchylky vzniklé při dohledování a monitoringu v

předchozí fázi Detekce.
    - Bezpečnostní událost – anomálie, která může způsobit narušení bezpečnosti:
        - informací v informačních systémech Objednatele;
        - služeb Objednatele;
        - a integrity datových sítí Objednatele.
    - Bezpečnostní incident – anomálie, která narušila či narušuje bezpečnost:
        - informací v informačních systémech Objednatele;
        - služeb Objednatele;
        - a integritu datových sítí zadavatele nebo jiných subjektů.

Fáze Analýza

- Vyhodnocení anomálie – vyhodnocení relevance:
    - k systémům Objednatele;
    - k procesům Objednatele;
    - k zákonným normám ČR vztažených na Objednatele.
- Klasifikace incidentu – začlenění incidentu do bezpečnostního typu kategorie dle určení zadavatelem nebo dle §30, VoKB:
    - Podle příčiny:
        - incident způsobený kybernetickým útokem nebo jinou událostí vedoucí k průniku do systému nebo k omezení dostupnosti služeb;
        - incident způsobený škodlivým kódem;
        - incident způsobený překonáním technických opatření;
        - incident způsobený porušením organizačních opatření;
        - incident spojený s projevem trvale působících hrozeb;
        - ostatní incidenty způsobené kybernetickým útokem.
    - Podle dopadu:
        - incident způsobující narušení důvěrnosti aktiv;
        - incident způsobující narušení integrity aktiv;
        - incident způsobující narušení dostupnosti aktiv;
        - incident způsobující kombinaci výše uvedených dopadů.
- Kategorizace incidentu – začlenění incidentu podle významnosti.

Kategorie III – do 30 minut – velmi závažný kybernetický bezpečnostní incident, při kterém je přímo a významně narušena bezpečnost poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje neprodlené zásahy obsluhy s tím, že musí být všemi dostupnými prostředky zabráněno dalšímu šíření kybernetického bezpečnostního incidentu, včetně minimalizace vzniklých i potenciálních škod.

Kategorie II – do 2 hodin – závažný kybernetický bezpečnostní incident, při kterém je narušena bezpečnost poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje neprodlené zásahy obsluhy s tím, že musí být vhodnými prostředky zabráněno dalšímu šíření kybernetického incidentu včetně minimalizace vzniklých škod.

Kategorie I – do 24 hodin – méně závažný kybernetický bezpečnostní incident, při kterém dochází k méně významnému narušení bezpečnosti poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje zásahy obsluhy s tím, že musí být vhodnými prostředky omezeno další šíření kybernetického bezpečnostního incidentu včetně minimalizace vzniklých škod. Jedná se o bezpečnostní incidenty, které nespadají do kategorií III a II.

B. Ad hoc služby

Poskytovatel bude dále poskytovat Objednateli na základě požadavků Objednatele další služby nad rámec Paušálních služeb spočívající v aktivním zásahu blokováním komunikace útočníků do i z internetu.

Příloha č. 2

Cena služeb

A. Cena Služby „Dohledové centrum kybernetické bezpečnosti (SOC)"

Popis položky	Počet měsíců	Cena za měsíc	Cena celkem
Služba SOC365	24	40 000,00 Kč	960 000,00 Kč
Celkem bez DPH			**960 000,00 Kč**
Výše DPH (21%)			**201 600,00 Kč**
Celková cena vč. DPH			**1 161 600,00 Kč**

B. Cena za Proaktivní ochranu – volitelné položky (Ad hoc služby)

Monitoring sítě s proaktivní ochranou sítě a blokováním komunikace útočníků do i z internetu na prostředcích zákazníka. (na firewalu)

Povýšení služby SOC365	Počet	Měsíční cena v Kč bez DPH	Jednorázová cena v Kč bez DPH
Měsíční poplatek za navýšení služby SOC365	1	1 500,00 Kč	
Cena za jednorázový zásah	1		10 000,00 Kč