SMLOUVA O DODÁVCE A IMPLEMENTACI SÍŤOVÉ BEHAVIORÁLNÍ ANALÝZY

uzavřená dle zákona č. 89/2012 Sb., občanského zákoníku

mezi:

Odběratelem				
Název:	**Fakultní nemocnice Ostrava**			
Sídlo:	17. listopadu 1790, 708 52 Ostrava-Poruba			
IČ:	00843989	**DIČ:**	CZ00843989	je plátcem DPH
Zřizovací listina MZ ČR ze dne 25. listopadu 1990 č. j. OP-054-25.11.90				
Zastoupena:	MUDr. Jiřím Havrlantem, MHA, ředitelem			
Bankovní spojení:	Česká národní banka, č. ú. 43 - 65137761/0710			

a

Dodavatelem				
Obchodní firma:	**GreyCortex s.r.o.**			
Sídlo:	Purkyňova 649/127, Medlánky, 612 00 Brno			
IČ:	05060711	**DIČ:**	CZ05060711	je* ~~není*~~ plátcem DPH
zapsaná v obchodním rejstříku vedeném Krajským soudem v Brně oddíl C, vložka 93360				
Jednající:	Ing. Michal Drozd, jednatel			
Bankovní spojení:	Fio banka a.s., č.ú. 2400994488/2010			

Odběratel a Dodavatel jsou dále souhrnně označeni jako „**Smluvní strany**" nebo jednotlivě „**Smluvní strana**"

I.
Základní ustanovení

1. Odběratel a dodavatel uzavírají tuto Smlouvu o dodávce a implementaci síťové behaviorální analýzy (dále také jen „**Smlouva**") na základě výsledku výběru nejvhodnější nabídky veřejné zakázky **„Dodávka a zavedení síťové behaviorální analýzy"** (dále také jen „**Veřejná zakázka**"), na základě které má Dodavatel provést dodávku a implementaci síťové behaviorální analýzy (dále také jen „**Síťová behaviorální analýza**" nebo „**Řešení**") dle zadávací dokumentace Veřejné zakázky (dále také jen „**Zadávací dokumentace**"), jejíž součástí je mimo jiné technická specifikace Síťové behaviorální analýzy, která tvoří rovněž přílohu č. 1 této Smlouvy (dále také jen „**Technická specifikace**").

2. Veřejná zakázka **„Dodávka a zavedení síťové behaviorální analýzy"** byla vyhlášena podle zákona č. 134/2016 Sb. o zadávání veřejných zakázek, ve znění platném ke dni vyhlášení veřejné zakázky.

3. Dodávka a implementace Síťové behaviorální analýzy, která je předmětem této Smlouvy, je spolufinancována v rámci Integrovaného regionálního operačního programu, specifického cíle 3.2 – Zvyšování efektivity a transparentnosti veřejné správy prostřednictvím rozvoje využití a kvality systémů IKT, 10. výzva „Kybernetická bezpečnost" a v souladu s projektem Odběratele „*Kybernetická bezpečnost ICT Fakultní nemocnice Ostrava*" (reg. č.: CZ.06.3.05/0.0/0.0/15_011/0007023). Zajištění technické podpory dodané Síťové behaviorální analýzy po uplynutí prvních dvou let jejího trvání, a to na dobu následujících 3 let, je hrazeno z vlastních zdrojů Odběratele, nikoliv z poskytnutých prostředků regionálního operačního programu.

4. Součástí plnění Smlouvy je krom dodání technických zařízení, vybavení a jejich příslušenství (dále také jen „**Hardware**" nebo „**Technická zařízení**") a převodu vlastnického práva k tomuto vybavení na Odběratele, také mimo jiné dodání všech potřebných licencí a subskripcí (dále také jen „**Licence**") pro počítačové programy (včetně operačních systémů) potřebné pro řádný chod Síťové behaviorální analýzy (dále také jen „**Software**"), instalace, nastavení a zprovoznění Síťové behaviorální analýzy dle Zadávací dokumentace a požadavků Odběratele včetně spuštění do ostrého provozu (dále také jen „**Implementace**") v rámci počítačového prostředí – IT infrastruktury Odběratele (dále také jen „**IT Infrastruktura**"), provedení školení personálu Odběratele (dále také jen „**Školení**") a poskytování technické podpory pro zajištění náležitého chodu Síťové behaviorální analýzy po jeho uvedení do ostrého provozu (dále také jen „**Technická podpora**"). Technická podpora bude poskytována v délce 2 (slovy: dvou) let s možností rozšíření o další 3 (slovy: tři) roky na celkovou dobu 5 (slovy: pět) let.

II.
Předmět smlouvy

1. Dodavatele se zavazuje poskytnout a provést Odběrateli následující plnění dle Zadávací dokumentace, které zahrnuje:
   a) dodávku Hardware (včetně převodu vlastnického práva k Hardware na Odběratele);
   b) dodávku a poskytnutí všech potřebných Licencí pro řádný chod Síťové behaviorální analýzy;
   c) provedení Implementace včetně uvedení Síťové behaviorální analýzy do ostrého provozu;
   d) provedení Školení;
   e) poskytování Technické podpory;
   f) další plnění dle Zadávací dokumentace;

   (dále souhrnně také jen „**Předmět plnění**"), přičemž detaily a rozsah jsou vymezeny v Technické specifikaci, která je přílohou č. 1 této Smlouvy a v příloze č. 2 této Smlouvy – Položkový rozpočet předmětu plnění (dále také jen „**Rozpočet**").

2. V rámci Předmětu plnění bude Odběrateli dodán Hardware, který je originální, nový a nepoužitý. V databázi výrobce Hardware a Software bude Odběratel veden jako první uživatel dodaného Hardware/Licence. Dodavatel je povinen doložit do 7 (slovy: sedmi) pracovních dnů od doručení žádosti Odběratele potvrzení výrobce o určení dodávaného Hardware pro evropský trh, včetně sériových čísel dodávaného Hardware, případně jiný doklad výrobce prokazující pro dodaná Technická zařízení provozovaná na území ČR poskytnutí plné podpory výrobce při řešení technických problémů (požadavek uvedený v Technické specifikaci). Před převzetím Hardware si Odběratel vyhrazuje právo kontroly dle sériových čísel (pokud jsou přidělena) u výrobce. Shodně pro Software je Dodavatel povinen na výzvu poskytnout doklad o poskytnutí plné podpory výrobce při řešení technických problémů. Pokud v databázi výrobce bude uveden jiný koncový uživatel než Odběratel (a to historicky), bude se jednat o podstatné porušení této Smlouvy.

3. Veškeré potřebné Licence budou Dodavatelem dodány v rozsahu potřebném pro řádné užívání Síťové behaviorální analýzy včetně možnosti jeho správy, konfigurace a provádění obnovy dat. Časový rozsah těchto Licencí bude na celou dobu trvání majetkových autorských práv k dodanému Software.

4. Předmět plnění zahrnuje rovněž vyhotovení a dodání instalační, administrační a provozní dokumentace Síťové behaviorální analýzy (dokumentace bude zpracována nejméně v rozsahu potřebném pro zajištění užívání, správy a údržby Síťové behaviorální analýzy Odběratelem a dále bude obsahovat popis skutečného provedení Síťové behaviorální analýzy včetně jeho vazeb na další části IT Infrastruktury).

III.
Místo a způsob poskytnutí Předmětu plnění

1. Místem dodání Předmětu plnění je:
   a) v sídle Odběratele - Fakultní nemocnice Ostrava – prostory ve správě Útvaru náměstka ředitele pro informační technologie;
   b) na detašovaném pracovišti Odběratele – Léčebna pro dlouhodobě nemocné Klokočov, Klokočov 59, Vítkov – Klokočov, PSČ 747 47

   (dále také jen „**Místo plnění**").
2. Náklady na dodání Předmětu plnění a jeho částí do místa dodání hradí Dodavatel.
3. Předmět plnění včetně dodání veškerého Hardware, Licencí a provedení Implementace a uvedení Síťové behaviorální analýzy do ostrého provozu bude provedeno nejpozději do 60 (slovy: šedesáti) kalendářních dnů ode dne podpisu této Smlouvy oběma Smluvními stranami (dále také jen „**Termín plnění**"), a to dle vzájemně odsouhlaseného harmonogramu (dále také jen „**Harmonogram**").
4. Termín plnění může být posunut pouze o délku případného prodlení zaviněného na straně Odběratele, a to formou písemného dodatku k této Smlouvě.
5. Smluvní strany se dohodly, že po instalaci a uvedení Síťové behaviorální analýzy do provozu, budou Dodavatelem v místě plnění provedeny zkoušky provozu, činností a veškerých funkcí Síťové behaviorální analýzy (dále také jen „**Akceptační testy**"). Odběratel je oprávněn se Akceptačních testů zúčastnit. Termín provádění Akceptačních testů je povinen Dodavatel sdělit Odběrateli nejméně 2 (slovy: dva) pracovní dny před plánovaným dnem jejich provádění; v případě, že by takto navržený termín Odběrateli z relevantních důvodů nevyhovoval, je oprávněn požadovat odložení Akceptačních testů o nejvýše 4 (slovy: čtyři) pracovní dny. V případě, že Síťová behaviorální analýza nebo její příslušenství bude vykazovat vady, není Síťová behaviorální analýza způsobilá předání a Odběratel nemá povinnost ji převzít. Po provedení Akceptačních testů, dle kterých bude Síťová behaviorální analýza bez vad, bude spuštěna do ostrého provozu (dále také jen „**Ostrý provoz**").
6. Předmět plnění je způsobilý předání Odběrateli, pokud budou provedeny všechny plnění, které jsou jeho součástí, tj. zejména dodání Hardware a jeho příslušenství, dodání a poskytnutí Licencí (včetně dodání dokumentů ohledně oprávnění Odběratele k užívání Software na základě Licencí), dodání veškeré dokumentace, instalace a uvedení Síťové behaviorální analýzy do Ostrého provozu (Implementace) v Místě plnění a v rámci Akceptačních testů nebude Síťová behaviorální analýza vykazovat jakékoliv vady nebo nedostatky. Předmět plnění se považuje za řádně dodaný podpisem akceptačního protokolu Odběratelem (dále také jen „**Akceptační protokol**") po uvedení Síťové behaviorální analýzy do Ostrého provozu. Nárok na úhradu ceny za Předmět plnění sjednané v čl. IV. odst. 3 písm. A/ této Smlouvy vzniká Dodavateli podpisem Akceptačního protokolu Odběratelem.
7. **Přechod nebezpečí škody a vlastnického práva**

7.1. Nebezpečí škody na dílčích částech Předmětu plnění (typicky jednotlivého Hardware) přechází na Odběratele převzetím jednotlivých dílčích částí Předmětu plnění Odběratelem a podpisem protokolu o takovém převzetí k tomu oprávněným zástupcem Odběratele (dále také jen „**Protokol o dodání dílčí části**"). Protokol o dodání dílčí části slouží pouze pro evidenční účely, že došlo k dovozu/provedení dílčí části Předmětu plnění, neboť není fakticky možné, aby byl celý Předmět plnění dodán najednou.

7.2. Převzetí dílčích částí Předmětu plnění dle odst. 7.1 tohoto článku výše, ani podepsání Protokolu o dodání dílčí části, nelze považovat za částečné plnění předmětu této Smlouvy Dodavatelem. Dodavatel v této souvislosti bere na vědomí, že Odběratel požaduje dodání Předmětu plnění jako celku, když očekává plně funkční Síťovou behaviorální analýzu a dílčí plnění pro něj nemají žádný význam ani užitek.

7.3. Vlastnické právo k movitým věcem dodaným Odběrateli na základě této Smlouvy přechází na Odběratele podpisem Akceptačního protokolu.

8. Realizační tým

8.1 Dodavatel bude Předmět plnění realizovat majoritně za účasti (prostřednictvím) osob, které jsou uvedeny v příloze č. 3 této Smlouvy – Realizační tým dodavatele. V případě, že dojde ke změně těchto osob, je Dodavatel povinen tuto skutečnost oznámit Odběrateli nejpozději do 5 (slovy: pěti) pracovních dnů od vzniku této skutečnosti. Nová osoba, která bude součástí realizačního týmu, musí splňovat podmínky, které Odběratel stanovil v Zadávací dokumentaci. Zároveň s oznámením o změně osoby tak budou doručeny doklady, které budou prokazovat osvědčení o vzdělání a odborné kvalifikaci této nové osoby. O této změně bude vyhotoven písemný dodatek k této Smlouvě.

9. Dodavatel je povinen realizovat Předmět plnění tak, aby se vyhnul jednání, které způsobí nebo by mohlo způsobit narušení, ohrožení či přerušení IT infrastruktury Odběratele nebo narušení integrity či kvality služeb poskytovaných IT infrastrukturou Odběratele.

IV.
Cena a platební podmínky

1. Cena Předmětu plnění (dále také jen „**Cena**") je stanovena jako nejvýše přípustná a nepřekročitelná a zahrnuje veškeré náklady, rizika, zisk a finanční vlivy (např. inflace nebo vývoj kurzu české měny vůči zahraničním měnám), a to po celou dobu realizace zakázky v souladu s podmínkami uvedenými v Zadávací dokumentaci. Ceny jsou závazné a nejvýše přípustné.

2. Cena zahrnuje veškeré náklady spojené s realizací Předmětu plnění dle čl. II. této Smlouvy včetně dodání/poskytnutí Licencí.

3. V souladu se zněním zákona č. 526/1990 Sb., o cenách se Smluvní strany dohodly na celkové Ceně za Předmět plnění ve výši:

Nabídková cena bez DPH	**3 199 000,00 Kč**
DPH 21 %	**671 790,00 Kč**
Nabídková cena celkem vč. DPH	**3 870 790,00 Kč**

přičemž

A/ z projektu Odběratele *„Kybernetická bezpečnost ICT Fakultní nemocnice Ostrava"* (reg. č.: CZ.06.3.05/0.0/0.0/15_011/0007023 bude uhrazena částka za pořízení jednotlivých položek Předmětu plnění vč. potřebných Licencí, jejich instalace, Implementace, zaškolení, zhotovení dokumentace a záruční technické podpory Síťové behaviorální analýzy v prvních dvou letech ve výši

Nabídková cena bez DPH	3 145 000,00 Kč
DPH 21 %	660 450,00 Kč
Nabídková cena celkem vč. DPH	3 805 450,00 Kč

Podrobný položkový Rozpočet Předmětu plnění je uveden v příloze č. 2 této Smlouvy.

B/ Z vlastních zdrojů Odběratele bude uhrazena částka za zajištění Technické podpory nad rámec prvních 2 (slovy: dvou let), přičemž cena za zajištění Technické podpory po dobu následujících 3 (slovy: tří) let od uplynutí prvních dvou let doby poskytování Technické podpory činí:

Nabídková cena bez DPH **za 3 roky**	54 000,00 Kč
DPH 21 %	11 340,00 Kč
Nabídková cena celkem **za 3 roky** vč. DPH	65 340,00 Kč
Nabídková cena bez DPH **za rok**	18 000,00 Kč
DPH 21 %	3 780,00 Kč
Nabídková cena celkem **za rok** vč. DPH	21 780,00 Kč

a tato cena bude hrazena ročně, vždy na 1 (slovy: jeden) rok trvání Technické podpory nad rámec prvních dvou let trvání Technické podpory, tj. od 3 (slovy: třetího) roku.

4. Zálohy nebudou poskytovány.

5. Dodavatel vyúčtuje Cenu nebo její část v souladu se Smlouvou, daňovým dokladem – fakturou (dále také jen „**Faktura**"), která bude vystavena na základě Akceptačního protokolu podepsaného odpovědnými zástupci obou Smluvních stran.

6. Dodavatel výslovně prohlašuje, že je ve smyslu zákona č. 235/2004 Sb., o dani z přidané hodnoty, v platném znění, plátcem DPH, resp. pro oblast přijatého plnění osobou povinnou k dani. Dodavatel se zavazuje při účtování dodávky uvést na faktuře odpovídající kód nomenklatury celního sazebníku. V případě, že se na dodávku Předmětu plnění vztahuje přenesená daňová povinnost, uvede Dodavatel na faktuře pouze platnou sazbu DPH a sdělení, že výši daně je povinen vypočítat, doplnit a přiznat Odběratel, pro kterého je plnění uskutečněno (§92f)".

7. Splatnost Faktury se sjednává do **60** (slovy: šedesát) kalendářních dnů od doručení Faktury Odběrateli.

8. Faktura musí splňovat mimo náležitostí podle ust. § 28 zákona č. 235/2004 Sb., o dani z přidané hodnoty, dále níže uvedené náležitosti:

   a. předmět plnění je spolufinancován z prostředků Integrovaného regionálního operačního programu. Na Faktuře musí být vždy uveden:
      - název projektu: *„Kybernetická bezpečnost ICT Fakultní nemocnice Ostrava"*;
      - registrační číslo projektu: *CZ.06.3.05/0.0/0.0/15_011/0007023*;
      - věta *„Projekt je spolufinancován v rámci Integrovaného regionálního operačního programu"*.

   b. dále bude Faktura obsahovat:
      - IČ;
      - den splatnosti;
      - označení peněžního ústavu a číslo účtu, ve prospěch kterého má být provedena platba, konstantní a variabilní symbol;
      - odvolávka na smlouvu, číslo smlouvy, Dodavatele a Odběratele;
      - razítko a podpis osoby oprávněné k vystavení účetního dokladu;
      - přílohou Faktury bude kopie potvrzeného Akceptačního protokolu.

   Smluvní strany se v souladu s ust. § 26, odst. 3, zákona č. 235/2004 Sb., o dani z přidané hodnoty, dohodly, že Dodavatel bude zasílat Fakturu, včetně příloh výhradně e-mailem na adresu: efakturace-inv@fno.cz.

   Dodavatel se zavazuje při této komunikaci dodržovat následující pravidla:

   - v jednom e-mailu budou jako přílohy zaslány dokumenty vztahující se pouze k jedné Faktuře, platí tedy pravidlo "jeden e-mail = jedna faktura a související dokumenty";
   - všechny přiložené dokumenty budou výhradně ve formátu PDF a v pořadí dokladů: faktura, ostatní související dokumenty;
   - Odběratel se zavazuje akceptovat takto zasílané dokumenty, pokud splňují ostatní náležitosti dané zákonem.

   Pouze výjimečně je možné zasílat Fakturu v papírové podobě.

9. Za okamžik uhrazení Faktury se považuje datum, kdy byla předmětná částka odepsána z účtu Odběratele.

10. V případě, že Faktura nebude obsahovat výše uvedené náležitosti, je Odběratel oprávněn Fakturu vrátit do doby její splatnosti způsobem, který prokazuje, že do tohoto data Dodavatel vrácený daňový doklad od Odběratele převzal. V takovém případě je Dodavatel povinen Fakturu opravit a v případě, že by oprava činila

Fakturu nepřehlednou, vystavit Fakturu nový. Opravená nebo nová Faktura musí být znovu zaslán Odběrateli a začíná běžet nová lhůta splatnosti.

V.
Technická podpora

1. Dodavatel zajistí Technickou podporu po dobu prvních 2 (slovy: dvou) let trvání Záruční doby ve smyslu čl. VI. odst. 4.1 této Smlouvy a případného rozšíření doby Technické podpory až o další 3 (slovy: tři) roky (tj. na celkovou dobu 5 let) a to za cenu sjednanou v čl. IV. odst. 3 písm. B/ této Smlouvy. Odběratel si vyhrazuje právo nevyužít případné rozšíření doby Technické podpory o další 3 (slovy: tři) roky (tj. na celkovou dobu 5 let). V tomto případě odešle Odběratel v prvních 2 letech trvání Záruční doby sdělení Dodavateli, že o rozšířenou dobu Technické podpory již nemá zájem.
2. Technická podpora bude poskytnuta v režimu servis v místě instalace (tzv. on-site service).
3. Technická podpora bude poskytována v režimu 5 x 9 (5 dnů v týdnu a 9 hodin každého dne) na celé Řešení.
4. Odběratel bude hlásit požadavky na poskytnutí Technické podpory (dále také jen „**Požadavky**") přes helpdesk systém Dodavatele (dále také jen „**Helpdesk**") dostupný na internetové adrese [redacted], e-mailem na adrese [redacted] nebo telefonicky na telefonní číslo servisního střediska Dodavatele [redacted]. Dodavatel bude veškeré Požadavky evidovat v Helpdesku a Odběratel bude mít k evidenci Požadavků přístup.
5. Dodavatel je povinen reagovat na jednotlivé Požadavky do 8 (slovy: osmi) hodin od jejich nahlášení Dodavateli postupem dle odst. 4 tohoto článku výše (dále také jen „**Reakční doba**"). V rámci Reakční doby je Dodavatel povinen (i) potvrdit přijetí Požadavku, (ii) dostavit se na místo, kde je Implementována Síťová behaviorální analýza a (iii) začít s řešením Požadavku.
6. Dodavatel se zavazuje vyřešit Požadavek v následujících lhůtách:
   a) v případě, že Požadavek je zapříčiněn poruchou či závadou Hardware, zavazuje se Dodavatel k vyřešení Požadavků včetně odstranění případné závady (oprava) do následujícího pracovního dne od nahlášení Požadavku;
   b) v případě, že Požadavek je zapříčiněn jiným důvodem, než dle bodu a) výše, pokud se Smluvní strany nedohodnou jinak, bude Požadavek vyřešen do 14 (slovy: čtrnácti) kalendářních dnů ode dne jeho nahlášení, to vše pokud není v této Smlouvě stanoveno jinak.
7. Požadavek se považuje za vyřešený akceptací jeho řešení Odběratelem.
8. V případě, že Požadavek nebude vyřešen ve lhůtách sjednaných v tomto článku Smlouvy, je Odběratel oprávněn uplatnit požadavek na odstranění závady Řešení přímo u výrobce.

VI.
Vady Předmětu plnění, jejich uplatnění a záruka

1. Vady Předmětu plnění

1.1. Předmět plnění vykazuje vady, nemá-li vlastnosti sjednané v této Smlouvě včetně jejich příloh, tj. zejména neodpovídá-li Technické specifikaci.

2. Právní vady

2.1. Dodavatel odpovídá za to, že jím poskytnutá plnění dle této Smlouvy nebudou zatíženy právem třetí osoby.

2.2. V případě, že k plněním poskytnutým Odběrateli na základě této Smlouvy uplatní právo jakákoliv třetí osoba, zavazuje se Dodavatel nahradit Odběrateli veškerou újmu takto způsobenou, jakož i náklady vynaložené na

obranu práv Odběratele. Dodavatel se v takovém případě dále zavazuje na svůj náklad poskytnout Odběrateli veškerou možnou součinnost k ochraně jeho práv. Dodavatel je povinen na své náklady vypořádat veškeré nároky třetích osob uplatněné vůči Odběrateli z titulu právních vad plnění dodaného na základě této Smlouvy. V případě soudního sporu je Dodavatel povinen zajistit řádné a svědomité vedení takového sporu a činit veškeré potřebné úkony tak, aby práva Odběratele nebyla zpochybněna z důvodu nedostatečné procesní obrany; Odběratel se zavazuje poskytnout Dodavateli potřebnou součinnost při vedení takového sporu.

3. Reklamace vad

3.1. Jakákoliv reklamace vad Předmětu plnění musí být Odběratelem provedena bez zbytečného odkladu, nejpozději do 5 (slovy: pěti) pracovních dnů, co se Odběratel o vadě dozvěděl. Uplynutím této lhůty nedochází ke ztrátě nároků Odběratele z vad Předmětu plnění.

3.2. Reklamace bude prováděna písemně. Za písemnou formu pro účely reklamace vad Předmětu plnění považují Smluvní strany rovněž e-mailovou komunikaci.

3.3. V rámci písemné reklamace musí Odběratel sdělit popis reklamované vady včetně doložení případných fotografií, pokud je má Odběratel k dispozici.

4. Záruka za jakost a možnost rozšíření její doby

4.1. Záruka za jakost na Řešení a jeho dílčí části (dále také jen „**Záruka**") je 2 roky (dále také jen „**Záruční doba**") a začíná plynout ode dne převzetí Síťové behaviorální analýzy na základě podepsání Akceptačního protokolu Odběratelem. V případě, že dojde k rozšíření doby Technické podpory dle čl. V. odst. 1 této Smlouvy, prodlužuje se Záruční doba i na celou dobu trvání rozšířené doby Technické podpory.

4.2. Dodavatel se zavazuje, že po dobu trvání Záruky bude mít Síťová behaviorální analýza vlastnosti požadované Odběratelem v rámci Technické specifikace a vlastnosti obvyklé.

4.3. Případné náklady související s odstraněním vad Síťové behaviorální analýzy včetně dílů a materiálu pro jejich odstranění, jsou v případě odstranění vad v rámci Záruky, neseny Dodavatelem.

VII.
Sankční ustanovení

1. V případě, že Dodavatel nesplní povinnost dle čl. II. odst. 2 této Smlouvy, vzniká Odběrateli nárok vůči Dodavateli na smluvní pokutu ve výši 500.000,- Kč (slovy: pět set tisíc korun českých). Úhradou smluvní pokuty není dotčeno právo na náhradu škody. Rovněž porušení povinnosti zakládající nárok na smluvní pokutu dle tohoto odstavce představuje podstatné porušení této Smlouvy.

2. V případě, že v průběhu trvání Záruky Odběratel zjistí, že vlastnosti (zejména technické parametry) Hardware nebo Software jsou prokazatelně v rozporu s touto Smlouvou (zejména nesplňují minimální požadované parametry uvedené v Technické specifikaci uvedené v příloze č. 1 této Smlouvy), vzniká Odběrateli nárok vůči Dodavateli na smluvní pokutu ve výši 500.000,- Kč (slovy: pět set tisíc korun českých). Úhradou smluvní pokuty není dotčeno právo na náhradu škody. Rovněž porušení povinnosti zakládající nárok na smluvní pokutu dle tohoto odstavce představuje podstatné porušení této Smlouvy.

3. V případě prodlení Dodavatele s poskytnutím Technické podpory, tj. se splněním Reakční doby a/nebo splnění lhůty pro vyřešení Požadavku, delším než 2 (slovy: dva) pracovní dny, vzniká Odběrateli nárok na smluvní pokutu vůči Dodavateli ve výši 5.000,- Kč (slovy: pět tisíc korun českých) za každý den prodlení s poskytnutím Technické podpory.

4. Odběratel se zavazuje při prodlení se zaplacením ceny Předmětu plnění zaplatit Dodavateli úrok z prodlení ve výši stanovené zákonem č. 89/2012 Sb., občanským zákoníkem.

5. V případě prodlení Dodavatele s plněním Termínu plnění vzniká Odběrateli vůči Dodavateli nárok na smluvní pokutu ve výši 0,5% (slovy: pět desetin procenta) z ceny Předmětu plnění za každý započatý den prodlení. Úhradou smluvní pokuty není dotčeno právo na náhradu škody.

6. Smluvní pokuty dle tohoto článku Smlouvy jsou splatné 3. (slovy: třetí) den od doručení výzvy k jejich úhradě druhé Smluvní straně.

VIII.
Ochrana osobních údajů a důvěrných informací

1. Smluvní strany se zavazují při zpracování osobních údajů dodržovat nařízení Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 27. dubna 2016, obecného nařízení o ochraně osobních údajů (dále jen „**GDPR**"). Smluvní strany berou na vědomí, že cílem této Smlouvy není zpracování osobních údajů třetích osob (ve smyslu tohoto odstavce jsou třetími osobami chápáni i zaměstnanci smluvních stran). Za předpokladu, že se i přes tuto skutečnost dostane Dodavatel do kontaktu s osobními údaji třetích osob, zavazuje se tyto zpracovávat v minimálním možném rozsahu a v souladu s GDPR a případnou smlouvou o zpracování osobních údajů uzavřenou mezi Smluvními stranami.

2. Smluvní strany se vzájemně zavazují zachovávat mlčenlivost o všech podstatných skutečnostech získaných při své činnosti vyplývající z této Smlouvy (dále jen „**Povinnost mlčenlivosti**"), a to zejména o skutečnostech, které tvoří jejich obchodní tajemství ve smyslu ust. § 504 Občanského zákoníku a důvěrné informace (dále také jen „**Důvěrné informace**").

3. Za Důvěrné informace Odběratele Smluvní strany považují zejména (nikoliv výlučně):

   a) strukturu počítačových systémů a programů Odběratele;

   b) popis procesů Odběratele;

   c) přístupové údaje k počítačovým systémům a programů Odběratele;

   d) data Odběratele;

   e) informace o plánovém rozvoji struktury počítačových systémů a programů Odběratele.

4. Za Důvěrné informace Dodavatele Smluvní strany považují detailní funkční specifikaci Řešení.

5. Za Důvěrné informace kterékoliv Smluvní strany se dále považují informace a údaje, které poskytující Smluvní strana výslovně a zřetelně označí jako „důvěrné".

6. Za porušení Povinnosti mlčenlivosti je kvalifikováno jednání, jímž jedna smluvní strana jiné osobě neoprávněně sdělí, zpřístupní, pro sebe nebo pro jiného využije obchodní tajemství či Důvěrné informace získané při své činnosti od jiné Smluvní strany, pokud je to v rozporu se zájmy jiné Smluvní strany, a učiní tak bez jejího souhlasu.

7. Porušením závazku mlčenlivosti není:

   a) poskytnutí obchodního tajemství a/nebo Důvěrných informací v nezbytném rozsahu orgánům nebo osobám majícím ze zákona právo na tyto informace a kontrolu činnosti Smluvních stran;

   b) poskytnutí obchodního tajemství a/nebo Důvěrných informací osobám, které mají ze zákona uloženou povinnost mlčenlivosti (notář, advokát, daňový poradce);

   c) poskytnutí obchodního tajemství a/nebo Důvěrných informací Smluvní strany či umožnění přístupu k němu třetím osobám v souvislosti s plněním této Smlouvy, pouze však v nezbytném rozsahu, přičemž příslušná Smluvní strana je povinna poučit tyto třetí osoby o tom, že jde o obchodní tajemství a/nebo Důvěrné informace jiné Smluvní strany a zavázat takové třetí osoby k mlčenlivosti nejméně ve stejné rozsahu v jakém je k mlčenlivosti vázána dle této Smlouvy Smluvní strana, třetí osobě takové informace sdělující;

   d) použití obchodního tajemství a/nebo Důvěrných informací v souladu s touto Smlouvou nebo na základě výslovného souhlasu příslušné Smluvní strany, popř. jiné použití důvěrných informací, které se staly veřejně dostupnými nikoliv v důsledku porušení závazku mlčenlivosti povinnou Smluvní stranou;

e) použití a/nebo sdělení obchodního tajemství a/nebo Důvěrných informací Odběratelem třetí osobě za účelem správy, údržby, rozšíření, úprav, změn, oprav a dalšího nakládání se Software prováděného pro Odběratele takovou třetí osobou.

8. Veškeré důvěrné informace zůstávají výhradním vlastnictvím předávající Smluvní strany a přijímající Smluvní strana vyvine pro zachování jejich důvěrnosti a pro jejich ochranu stejné úsilí, jako by se jednalo o její vlastní důvěrné informace.

9. Povinností mlčenlivosti jsou Smluvní strany vázány po dobu trvání skutečností zakládajících tuto Povinnost mlčenlivosti, pokud nebudou mlčenlivosti zproštěny nebo se nestanou dané informace veřejně dostupnými jinak než porušením Povinnosti mlčenlivosti některou ze Smluvních stran.

10. V případě porušení Povinnosti mlčenlivosti Dodavatelem, vzniká Odběrateli nárok na smluvní pokutu ve výši 100.000,- Kč (slovy: sto tisíc korun českých) za každé jednotlivé porušení Povinnosti mlčenlivosti. Tato smluvní pokuta je splatná do 10 (slovy: deseti) kalendářních dnů od doručení výzvy k její úhradě. Úhradou této smluvní pokuty není dotčen nárok Odběratele na náhradu škody ani nárok na případné sankce ze závislých smluv na této Smlouvě.

IX.
Ukončení Smlouvy

1. Odběratel je oprávněn od této Smlouvy odstoupit kromě podmínek daných zákonem č. 89/2012 Sb., občanským zákoníkem a případů sjednaných v této Smlouvě, rovněž v následujících případech, které se považují za podstatné porušení této Smlouvy:

   a) prodlení Dodavatele s dodáním Hardware, Licencí nebo jiných plnění dle této Smlouvy, které je delší než 60 (slovy: šedesát) kalendářních dnů;

   b) prodlení s Technickou podporou o více než 7 (slovy: sedm) kalendářních dnů.

2. V případě odstoupení od Smlouvy jsou si Smluvní strany povinny vrátit vše, co si v souvislosti s touto Smlouvou plnily, přičemž Smluvní strany se dohodly, že dojde-li k odstoupení v druhém nebo dalším roce trvání platnosti této Smlouvy, není Dodavatel povinen vracet tu část uhrazené Ceny, po jaký počet měsíců trvala tato Smlouva s tím, že tato částka, kterou nebude Dodavatel povinen vracet, bude určena z ceny Technické podpory dle čl. IV. odst. 3 písm. B/ jako její poměrná část.

3. Zánikem Smlouvy z důvodu odstoupení od Smlouvy nezanikají nároky na smluvní pokuty sjednané v čl. VII. této Smlouvy, stejně jako nezaniká právo na náhradu škody.

X.
Závěrečná ustanovení

1. Pohledávky vyplývající z této Smlouvy nemohou být postoupeny třetí osobě bez předchozího písemného souhlasu druhé Smluvní strany.

2. V souladu s ustanovením § 2 písm. e) zákona č. 320/2001 Sb., o finanční kontrole, je Dodavatel osobou povinnou spolupůsobit při výkonu finanční kontroly. Tato povinnost se vztahuje na právnickou nebo fyzickou osobu, podílející se na dodávkách zboží nebo služeb hrazených z veřejných rozpočtů nebo z veřejné finanční podpory.

3. Dodavatel je povinen archivovat veškerou dokumentaci související s realizací Předmětu plnění, zejména originální vyhotovení Smlouvy, její dodatky, originály účetních dokladů a dalších dokladů vztahujících se k realizaci Předmětu plnění této Smlouvy po dobu 10 (slovy: deseti) let od zániku závazku vyplývajícího ze Smlouvy a po tuto dobu je Dodavatel rovněž povinen umožnit kontrolu těchto dokladů osobám oprávněným k výkonu kontroly Předmětu plnění a vytvořit těmto osobám podmínky k provedení kontroly vztahující se k realizaci Předmětu plnění a poskytnout jim při provádění kontroly součinnost.

4. Smluvní strany se dohodly, že v souladu se zákonem č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), tuto Smlouvu, včetně případných dodatků, v Registru smluv uveřejní Odběratel.
5. Veškeré změny a doplňky této Smlouvy je možné činit písemně, a to formou číslovaných dodatků.
6. Tato Smlouva se uzavírá písemně elektronickými prostředky, a to zaručeným elektronickým podpisem oprávněných zástupců obou smluvních stran.
7. Veškeré právní vztahy touto Smlouvou neupravené se řídí obecně závaznými právními předpisy České republiky, zejména zákona č. 89/2012 Sb., občanským zákoníkem.
8. Tato Smlouva nabývá platnosti podpisem obou Smluvních stran a účinnosti od data zveřejnění v Registru smluv.
9. Jestliže jednotlivá ustanovení této Smlouvy jsou nebo se stanou zcela nebo částečně neplatnými nebo jestliže v této Smlouvě nějaké ustanovení zcela chybí, není tím dotčena platnost ostatních ustanovení. Namísto neplatného či chybějícího ustanovení dohodnou Smluvní strany takové platné ustanovení, které nejvíce odpovídá smyslu a účelu neplatného či chybějícího ustanovení.

Přílohy:

Příloha č. 1 - Technická specifikace Předmětu plnění;
Příloha č. 2 – Položkový rozpočet Předmětu plnění
Příloha č. 3 – Realizační tým dodavatele

V Ostravě, dne: dle elektronického podpisu

MUDr. Jiří Havrlant

Digitálně podepsal MUDr. Jiří Havrlant
Datum: 2020.11.11 11:35:21 +01'00'

Fakultní nemocnice Ostrava
MUDr. Jiří Havrlant, MHA
Ředitel

V Brně, dne: dle elektronického podpisu

Ing. Michal Drozd

Digitally signed by Ing. Michal Drozd
Date: 2020.11.09 15:45:11 +01'00'

GreyCortex s.r.o.
Ing. Michal Drozd
jednatel

1 POPIS POŽADAVKU

1.1 MOTIVACE POŽADAVKU

Globální zavedení síťové behaviorální analýzy včetně podpory sběru a vyhodnocování síťového provozu, zajištění diagnostiky výkonnostních problémů sítě a aplikací, a detekce anomálií a pokročilých kybernetických hrozeb.

Řešení tak napomáhá splnění požadavků daných § 18, 23 a 25 Vyhlášky o kybernetické bezpečnosti č. 82 /2018 Sb.

1.2 POPIS SOUČASNÉHO STAVU

1.2.1 Lokalita FNO – hlavní datová centra

V prostředí Fakultní nemocnice Ostrava (dále také jen "**FNO**" nebo "**Zadavatel**") jsou nyní provozovány dvě nezávislá datová centra DC1 a DC2. LAN konektivita je postavena na dvou chassis Cisco 6509 zapojených v režimu Virtual switching (VSS) a tvoří jádro sítě celé lokality zajišťující L2/L3 funkcionalitu.

Připojování koncových bezdrátových zařízení je zajišťováno jednotným řešením pro ověřování identit a řízení přístupu k síti – Cisco Identity Services Engine (ISE). Stejné Network Access Control (NAC) řešení by mělo být dle předpokladu FNO v nejbližší době využito i pro ověřování identit a zařízení připojených do drátové sítě.

Připojení do sítě Internet zajišťuje dvojice firewallů Cisco ASA5585-X zapojených v režimu vysoké dostupnosti.

1.2.2 Lokalita LDN

V rámci lokality jsou provozována 2 datová centra vzájemně propojená na druhé vrstvě modelu OSI.

Připojení do sítě Internet zajišťuje dvojice firewallů Cisco ASA5506-X zapojených v režimu vysoké dostupnosti.

Lokalita LDN je propojena s FNO pomocí site to site VPN navázanou přes WAN s garantovanou konektivitou 100 Mbit/s.

Firewally v obou lokalitách jsou centrálně spravovaná pomocí Cisco Firepower Management Center (FMC).

1.3 POPIS POŽADOVANÉHO ŘEŠENÍ

Systém pro analýzu síťového provozu a bezpečnostní monitoring, který okamžitě identifikuje bezpečnostní rizika a události a který splňuje všechny požadavky uvedené níže.

Při definici technických požadavků jsou všechny uvedené požadavky závazné. Je-li definice požadavku „umožňuje, lze, je možné, možnost, ..." je uvedený parametr závazný a požadovaná funkcionalita musí být v rámci Systému dodána/naimplementována a případně licencována. Tyto technické požadavky jsou minimálně možné a Dodavatel může nabídnout charakteristiky (funkce) lepší.

Systém bude dodán včetně instalace, implementace, plné konfigurace, uvedení do provozu, zajištění technické podpory, zajištění záruky výrobce a zajištění dostupnosti softwarových aktualizací, a to na všechny části a komponenty dodaného systému (HW, SW i licence) po dobu pěti let.

Systém bude nasazen v datových centrech umístěných ve dvou lokalitách – FN Ostrava a LDN Klokočov. Propojení mezi lokalitami je zajištěna symetrickým VPN tunelem o rychlosti 100 Mbit/s.

1.3.1 Obecné požadavky a parametry

- Veškeré dodávané HW a SW produkty byly získány legálně a umožňují využití těchto produktů Zadavatelem, jako koncovým zákazníkem, v souladu s distribučními a licenčními podmínkami výrobce zařízení;

- V případě dodání HW a SW produktů Zadavateli, jako koncovému zákazníkovi, nebude Zadavatel nijak omezen ve svých nárocích vyplývajících ze záruky výrobce dodávaného zařízení a z produktové podpory, kterou tento výrobce k dodávaným HW a SW produktům poskytuje. Uvedené musí zahrnovat i nárok Zadavatele na přístup k relevantním SW releases a novým verzím SW po celou dobu trvání podpory výrobce;
- Musí být umožněn online přístup Zadavatele k dokumentaci výrobce HW/SW a znalostní bázi, kterou výrobce v rámci své podpory poskytuje;
- Zadavatel musí mít možnost eskalovat závady přímo k technické podpoře výrobce HW/SW, včetně možnosti si sám a přímo otevřít požadavek na technickou podporu, provádět změny priority požadavků a případné eskalace pracovníky Zadavatele. A to po celou dobu požadované podpory;
- V databázi výrobce musí být Zadavatel veden jako první uživatel zboží a licencí/subscripcí/operačních systémů. Zadavatel požaduje originální a nová zařízení určená pro evropský trh. Před převzetím zboží si Zadavatel vyhrazuje právo kontroly dle sériových čísel u výrobce. Pokud v databázi výrobce bude uveden jiný koncový uživatel než Zadavatel, bude se jednat o porušení podmínky originálního a nového zařízení;
- Dodavatel garantuje, že v případě dodání zboží Zadavateli, jako koncovému zákazníkovi, bude Dodavatelem poskytnuta k dodávanému zařízení záruka výrobce a produktová podpora v plném, výrobcem poskytovaném rozsahu;
- Součástí všech zařízení musí být dodávka operačního systému a SW v aktuální verzi;
- Součástí dodávky musí být poskytnutí práva užívat software (dále též jen „**licence**");

1.3.2 Technická specifikace

1.3.2.1 Obecné požadavky

- **Systém pro analýzu síťového provozu**
  Systém složený z hardwarových zařízení musí monitorovat síťovou aktivitu v reálném čase a identifikovat potenciální kybernetické hrozby, bezpečnostní rizika a anomální chování, a musí o nich v reálném čase vytvářet upozornění.

  Systém zajišťuje detailní viditelnost do síťové komunikace s drill down prokliky na veškerá uložená data. Všechny komponenty systému musí být instalované v interním prostředí Zadavatele („on premise") a použití externích komponent nebo cloudových služeb se nepřipouští.

- **Analýza plného síťového provozu**
  Dodaný systém musí analyzovat síť na základě zrcadleného síťového provozu (nikoliv jen na základě statistických protokolů typu NetFlow) a to bez potřeby nasazovat agenty na koncové stanice nebo další zařízení v síti.

  Systém musí být schopen získávat data zrcadlené komunikace ze SPAN/RSPAN/ERSPAN portů a síťových TAPů.

  Systém musí být zcela pasivní vzhledem k monitorovanému provozu, monitorovaný provoz přes něj neprochází.

- **Analýza protokolů typu NetFlow**
  Dodaný systém musí analyzovat síť na základě zpracování statistických protokolů typu NetFlow, IPFIX, NetStream, Cisco NSEL a případně dalších.

- **Ukládání síťových toků**
  Systém ukládá síťové toky ve formátu, který umožní analýzu síťové komunikace na úrovni jednotlivých toků, včetně dohledání informací o aplikačních transakcích a jejich metadatech z L2 až L7, obsažených v daném síťovém toku.

  Požadované protokoly pro ukládání aplikačních metadat z jednotlivých transakcí jsou: DHCP, DNS, SMB, HTTP, HTTPS, SMTP, POP3, IMAP, SSH, LDAP, KERBEROS, SNMP, CIFS, SMTPS, MSSQL, RDP, SIP, TELNET, FTP, FTP-DATA, TFTP, TFTP-DATA, SSL/TLS zapouzdření.

- **Uchování a vyhledávání síťových toků**

Je požadováno vysokorychlostní úložiště pro uchování datových toků na dobu minimálně **180 dnů** složené z **SSD** disků o celkové kapacitě alespoň **45 TB**.

Dále je požadováno, aby uživatel mohl v reálném čase volně filtrovat a vyhledávat v plné historii uložených síťových toků, dat a agregovaných síťových statistik na základě minimálně těchto parametrů:

- IP host/net a MAC adresa, PostNAT/NATT IP/port
- Hostname
- Username
- příchozí a odchozí provoz
- síťová služba
- lokální nebo vzdálená služba (klient nebo server)
- číslo portu
- VLAN id
- Země
- ASN

- **Automatická identifikace důležitých systémů**
  Je požadována automatická detekce přítomnosti klíčových služeb monitorované infrastruktury, jako jsou doménové řadiče, webové, emailové a databázové služby apod.

  Systém musí být schopen upozornit na vznik nových služeb v interní síti a sledovat jejich změny, a to minimálně v rozsahu následujících služeb: DHCP, DNS, MS Active Direktory služby, HTTP, HTTPS, SMTP, POP3, IMAP, SSH, CIFS, SMTPS, POP3S, IMAPS, MSSQL, TELNET, FTP, TFTP, a to i v případě, že nebudou využívat standardních „well known" portů.

1.3.2.2 Specifika nasazení v jednotlivých lokalitách

- **FN Ostrava**
  Je požadován **1 x HW** datový kolektor a sensor o celkové propustnosti alespoň **10 Gbps** s monitorovacím rozhraním **4 x 1GE RJ45 a 8 x 10GE SFP+ včetně 6x 10Gb LR Transceiver a 2x 10Gb SR Transceiver**.

  Minimální celková disková kapacita úložiště je **45 TB SSD** disků.

  Šasi pro montáž do standardního racku (800 x 800 mm) o velikosti max. 2U.

- **LDN Klokočov**
  Je požadován **1 x HW** datový kolektor a sensor o celkové propustnosti alespoň **200 Mbps** s monitorovacím rozhraním **2 x 1GE RJ45**.

  Minimální celková disková kapacita úložiště je **4 TB** disků.

  Šasi pro montáž do standardního racku (800 x 800 mm) o velikosti max. 2U.

1.3.2.3 Schopnosti detekce bezpečnostních událostí

- **Monitorování zařízení, segmentů sítě a využívaných síťových služeb**
  Dodaný systém musí identifikovat všechna zařízení připojená do sítě včetně koncových zařízení, serverů, IoT zařízení apod. Zároveň musí být systém schopen identifikovat změny v síti – minimálně:

  - změna IP/MAC adresy hosta,
  - duplicitní IP/MAC adresa,
  - změna VLAN,
  - vytvoření nové podsítě,
  - připojení nového zařízení,
  - použití nové služby,
  - nedostupnost dříve dostupné a komunikující služby nebo dříve dostupného a komunikujícího zařízení,
  - přístup nového zařízení ke službě či zařízení.

  Systém musí uživateli umožnit pomocí těchto detekčních metod nastavovat bezpečnostní politiky pro různé segmenty sítě a pro různá zařízení a na porušení těchto politik reagovat upozorněním.

- **Detekce síťových služeb**
  Systém musí být schopen detekovat síťové služby na základě síťových metadat získaných prostřednictvím DPI (Deep Packet Inspection), nikoliv pouze čísla portu.

- **Samostatné učení behaviorálních aktivit a detekce anomálií**
  Systém musí používat matematické metody samostatného učení (např. strojové učení) pro analýzu síťové aktivity, musí vytvářet a v čase automaticky modifikovat modely chování na základě běžného chování jednotlivých zařízení a na nich provozovaných služeb v rámci celé organizace.

- **Identifikace nestandardního síťového chování na základě modelu daného zařízení a jeho služeb:**
  Systém musí mít schopnost identifikovat zejména následující nestandardní síťové chování:

  - odchylku od modelu pro přenos dat, toků a paketů,
  - odchylku od modelu pro počet komunikačních partnerů a entropie na komunikačních portech,
  - odchylku od modelu pro počet síťových toků a využitých síťových služeb,
  - odchylku od modelu výkonnosti sítě (rychlost přenosu) a aplikací (doba odezvy).

  Samostatné učení je požadováno na všech síťových zařízeních a na nich provozovaných službách (port číslo 0 až 65535 u TCP i UDP) na IPv4 a IPv6 a dalších protokolech L3 a L4 síťové vrstvy.

- **Identifikace neznámých hrozeb, podezřelých chování na síti a porušení politik**
  Systém musí být schopen detekovat neznámé hrozby, které nelze identifikovat prostřednictvím detekčních signatur, jako jsou trojské koně, botnety apod.

  Zejména musí být identifikovány tyto příznaky potenciálně škodlivého chování:

  - průzkumné aktivity v síti,
  - potenciální úniky dat,
  - detekce podezřelého strojového chování, které nevytvářejí lidští uživatelé sítě,
  - detekce repetitivních vzorců chování na síti,
  - detekce botnetů a ovládání kompromitované stanice,
  - detekce příznaků těžení kryptoměn,
  - útoky hrubou silou a enumerace dat,
  - rozpoznání tunelovaného síťového provozu – alespoň IPv4 prostřednictvím IPv6 a DNS tunely.

- **Detekce na základě databáze známých hrozeb (signaturní detekce)**
  Systém musí být schopen identifikovat a reportovat události na základě detekční databáze malware, známých útoků a zranitelností, porušení bezpečnostních pravidel a „best practices" a dalších rizik. Tato databáze musí být aktualizovaná minimálně na hodinové bázi. Nesmí se jednat o volně dostupnou/open source databázi, ale musí se jednat o komerční databázi renomovaného vendora nebo poskytovatele těchto služeb.

  Databáze detekčních pravidel (signatur) musí být založena na pokročilých regulárních výrazech pro zpracování řetězců, které dokáží provádět inspekci veškeré síťové komunikace od L2 (Ethernet apod.) po L7.

  Příklad možné syntaxe detekčního pravidla:

  ```
  alert tcp $HOME_NET any -> any any (msg:"Command Shell Access";
  content:"C:\\Users\\Administrator\\Desktop\\hfs2.3b"; sid:1000001; rev:1;)
  ```

  Systém musí využívat tuto signaturní detekci pro veškerý monitorovaný provoz (na perimetru i v interní síti mezi všemi segmenty), nikoliv pouze pro omezený segment nebo podmnožinu celkové komunikace.

  Systém musí detekovat události na základě vysokého počtu signaturních pravidel (minimálně několik desítek tisíc).

  Uživatel musí být schopen přidávat vlastní detekční pravidla v praktickém a obecně využívaném formátu.

- **Detekce přenosu škodlivých souborů**

Systém musí být schopen v monitorovaném provozu porovnávat hash zachycených souborů s databázemi známých hashů škodlivých souborů.

- **Analýza šifrované komunikace**
  Vedle samostatného učení musí systém používat další metody pro analýzu šifrované komunikace, minimálně TLS fingerprinting a s ní spojenou detekci známých hrozeb.

- **Kontrola platnosti certifikátů**
  Ověřování platnosti interních certifikátu pro validní TLS šifrování u HTTPS a upozornění před datem jejich vypršení.

- **Asistované učení a korelace událostí**
  Systém musí být schopen korelace jakýchkoliv detekovaných událostí ze všech detekčních metod a úpravy samostatného učení a dalších detekčních metod tak, aby byly v maximální míře eliminovány falešné alarmy. Systém musí být schopen eliminovat falešné alarmy i pro události detekované v historii.

  Systém musí být schopen zobrazovat zařízení podle souhrnné kritičnosti identifikovaných událostí – minimálně v rozsahu kritické a důležité.

- **Aktuální databáze blacklistů**
  Systém musí být schopen hodnotit IP adresy, se kterými komunikují vnitřní hosté v síti prostřednictvím minimálně denně aktualizovaných reputačních databází. Uživatel musí být schopen importovat vlastní reputační databáze.

1.3.2.4 Požadavky na zajištění síťové viditelnosti

- **Vyhledávání, filtrování a vizualizace všech dat**
  Systém musí být schopen okamžitého vyhledávání a vizualizace pro forenzní analýzu a podporu threat hunting bez zvláštního dotazovacího jazyka a bez hlubokých znalostí konkrétních komunikačních protokolů.

  Jedná se o možnost okamžitě filtrovat a vyhledávat v plné historii všech zpracovávaných dat, tj. bezpečnostních událostí a zaznamenaných síťových toků, a to minimálně podle parametrů: IP a MAC adresa, hostname, username, příchozí a odchozí provoz, síťová služba, lokální nebo vzdálená služba (služba z pohledu klient nebo server), číslo portu, VLAN, země, ASN.

  Systém musí pro vyhledávání poskytovat již předpočítané hodnoty výkonnostních a behaviorálních charakteristik pro každé zařízení a pro všechny na něm provozované služby, bez nutnosti zpracování surových dat ze síťových logů.

  Systém musí být schopen filtrovat a vizualizovat výsledky v grafech, výčtových tabulkách s možností řazení a TOP N statistikách.

- **Ukládání a vyhledávání aplikačních metadat**
  Systém musí být schopen ukládat a následně vyhledávat aplikační metadata (vždy dotaz i odpověď všech transakcí v toku) minimálně z následujících protokolů, které jsou nebo mohou být využívány ve vnitřní síti organizace: FTP, FTP-DATA, TFTP, TFTP-DATA, SSH, Telnet, SMTP, SMTPS, DNS, DHCP, HTTP, HTTPS, NTP, SMB, SNMP, LDAP, NFS, MS-SQL, SIP, Kerberos, SSL/TLS, ARP, MODBUS.

  V rámci metadat u HTTP, SMTP, SMB a NFS je požadováno ukládání informací o po síti přenášených souborech alespoň v rozsahu:

  - název souboru,
  - velikost souboru,
  - HASH souboru

- **Kontextuální informace**
  Systém musí být schopen pro každé zařízení získávat, vizualizovat a integrovat v jednotném grafickém rozhraní kontextuální informace:

  - jméno uživatele a další jeho parametry z doménového řadiče (MS Active Directory), včetně její historie,

- hostname zařízení a jeho historie na základě zpracování relevantních dat z DNS a DHCP provozu,
- IP geolokace,
- IP reputace, vč. údaje, jestli je IP adresa blacklistovaná nebo podezřelá,
- historie použitých MAC adresa a výrobce zařízení,
- operační systém a jeho historie na zařízení,
- uživatelem zadané poznámky a informace k zařízení

- **Monitoring výkonu aplikací a sítě**
  Systém v celé monitorované síti, mezi všemi zařízeními a na všech službách měří a vytváří automaticky (bez nutnosti nastavovat manuálně limitní hodnoty nebo jiné parametry) model normálního chování pro výkonnostní parametry minimálně:

  - přenosová rychlost sítě,
  - rychlost odezvy aplikace,
  - odezva systému z pohledu uživatele,
  - informace o retransmission a out of order paketech.

  Výkonnostní anomálie na jednotlivých zařízeních a jejich službách jsou reportovány uživateli.

- **Zaznamenávání a ukládání plného provozu**
  Je požadováno volitelné nahrávání plného síťového provozu (full packet capture) na všech dodaných zařízenich minimálně na základě parametrů: cílová a zdrojová IP/MAC adresa, podsíť, využitý protokol, IPv4 nebo IPv6.

1.3.2.5 Správa systému

- **Jednotné grafické rozhraní**
  Systém musí poskytovat jednotné grafické uživatelské rozhraní pro veškerou práci uživatelů, včetně všech detekcí, analýzy síťových statistik, nastavení systému, konfiguraci alertů, reportů a dashboardů.

- **Uživatelské profily a nastavení**
  Systém musí být schopen vytváření profilů a skupin uživatelů pro omezení funkcionality produktu a viditelnosti uložených dat s podporou minimálně:

  - granulární nastavení přístupu k analytickým i konfiguračním/administrativním komponentám systému s definovanými úrovněmi přístupu (alespoň read, write, execute),
  - granulární nastavení přístupu k datům z různých segmentů sítě organizace s definovanými úrovněmi přístupu (alespoň read, write, execute),
  - vytváření filtrů veškerých dat a jejich sdílení mezi uživateli a skupinami uživatelů,
  - vytváření vlastních uživatelských pohledů, reportů, dashboardů apod.

1.3.2.6 Požadavky na zpracování kybernetických událostí, integraci, reporting a alerting

- **Management bezpečnostních událostí a incidentů**
  Systém musí poskytovat integrované rozhraní pro:

  - reporting bezpečnostních incidentů (prohlášení identifikované události za bezpečnostní incident),
  - spolupráci a sdílení informací při analýze identifikovaných bezpečnostních incidentů včetně potřebného workflow mezi jednotlivými uživateli s podporou automatizovaných oznámení o změně stavu události či přiřazení řešitele,
  - jednoduché sdílení informací o bezpečnostních incidentech, včetně uživatelem zadaných komentářů,
  - možnost vyhledávání a filtrování nad všemi událostmi z pohledu workflow bezpečnostního incidentů (reportovaná událost, událost v řešení, vyřešená událost, události v řešení daného uživatele apod.).

- **Integrace**
  Systém musí být schopen rychlé a jednoduché uživatelské integrace s nástroji třetích stran:

  - nástrojem typu SIEM prostřednictvím minimálně syslog, CEF a LEEF,

- nástroji pro generování nebo zpracování síťových statistik ve formátu IPFIX/NetFlow, včetně možnosti filtrovat IPFIX/NetFlow exportované statistiky dle všech filtrovaných parametrů jako výše,
- s dalšími nástroji prostřednictvím okamžitě definovatelných a jednoduše použitelných odkazů (URL) na požadované pohledy v nástroji.

- **Automatické bezpečnostní hlášení (alerty)**
  Systém musí být schopen upozorňovat uživatele prostřednictvím minimálně emailu a logu o:

  - všech identifikovaných událostech,
  - událostech filtrovaných minimálně dle IP a MAC adresy, podsítě, závažnosti události, kategorie události, země, uživatele, síťové služby, čísla portu, provozu do/z internetu.

  Tyto alerty musí být systém schopen dodávat i ve strojově čitelném formátu pro vyžití v nástrojích typu SIEM a musí obsahovat minimálně kompletní informace o detekované události včetně URL odkazu na danou událost v reportovaném období do grafického rozhraní aplikace.

- **Možnost automatizovaného reportingu**
  Možnost vytváření automatizovaných manažerských reportů o stavu kybernetické bezpečnosti z pohledu zprávy kybernetických incidentů ideálně dle oblastí jejich vzniků (např.: doména, web, email apod.).

  Je požadováno vytváření reportů v českém jazyce.

1.3.3 Řízení přístupu do sítě LAN

- Systém musí umožňovat napojení na zařízení pro řízení přístupu Cisco ISE za účelem předávání informací a vynucení „Change of Authorization" aktivního připojení síťového zařízení, u kterého byla detekována anomálie síťového provozu ukazující s vysokou pravděpodobností na nákazu malware.
- Kritéria zajišťující vynucení „Change of Authorization" musí být uživatelsky konfigurovatelná

1.3.4 Řízení přístupu do sítě Internet

- Systém musí umožňovat napojení na firewally Zadavatele nebo na jejich centrální management za účelem předávání informací a vynucení blokování přístupu síťového zařízení do sítě Internet, u kterého byla detekována anomálie síťového provozu ukazující s vysokou pravděpodobností na nákazu malware.
- Kritéria zajišťující vynucení blokování přístupu do sítě Internet musí být uživatelsky konfigurovatelná

1.4 IMPLEMENTACE

Všechna Dodavatelem instalovaná zařízení nebo komponenty musí být Dodavatelem profesionálně nainstalovány a zprovozněny a po jejich nasazení řádně dokumentovány a otestovány, vč. prokázání, že tato zařízení plní všechny požadované a výkonnostní parametry.

Všechna Dodavatelem instalovaná zařízení budou zabezpečena a nebudou obsahovat zjevná rizika a zranitelnosti, a to po celou dobu provozu služby.

Řešení musí splňovat bezpečnostní kritéria podle zákona č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů, a nebude v rozporu s požadavky Národního úřadu pro kybernetickou a informační bezpečnost (dále jen „NÚKIB") pro provoz významných informačních systémů;

Zadavatel je povinen dle § 5 vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), ve znění pozdějších předpisů, provádět analýzu rizik a identifikovaná rizika řídit. Současně je Zadavatel povinen zabývat se všemi hrozbami, které prostřednictvím varování vydává NÚKIB a zohlednit je v analýze rizik. Zadavatel proto provedl, s přihlédnutím k vydanému "varování" NÚKIB, analýzu rizik a v hodnocení se řídil pokyny uvedenými v dokumentu NÚKIB "Metodika k varování ze dne 17. prosince 2018". Veškerá bezpečnostní opatření, která bude nutné u dodaného řešení na základě výsledků analýzy rizik přijmout, nesmí pro zadavatele znamenat žádné další náklady.

1.5 SERVISNÍ SLUŽBY

- Systém musí zahrnovat standardní záruční (servisní) podporu výrobce zařízení, software a Dodavatele systému po dobu 2 let a její rozšíření na celkovou dobu 5 let.
- Požadovaná úroveň podpory na celé řešení (Systém) je 5x9 s reakční dobou 8 hodin po celé období 5 let.
- Na dodaný HW je požadovaná úroveň podpory 5x9 s reakční dobou 8 hodin a garantovanou opravou NBD (Next Business Day on-site) po celé období 5 let.
- V případě, že porucha je zapříčiněna jiným důvodem než poruchou HW, bude požadavek vyřešen do 14 kalendářních dnů ode dne jeho nahlášení, pokud nebude dohodnuto jinak.

1.6 ZAŠKOLENÍ

Zaškolení administrátorů systému v rozsahu nutném pro zvládnutí každodenní správy v minimálním rozsahu 8 hodin pro 5 lidí. Školení bude probíhat v prostorách FNO a v termínech stanovených FNO.

1.7 PROVOZNÍ DOKUMENTACE

V rámci realizace řešení služeb bude Dodavatelem zpracována a předána dokumentace řešení minimálně v tomto rozsahu:

- Provozně-technická dokumentace v rozsahu požadovaném vyhláškou č. 529/2006 Sb. § 10 a § 11.
- Plán zálohování a obnovy včetně doporučení pravidel pro pravidelné ověřování jednotlivých postupů.
- Bezpečnostní dokumentace dle zákona 181/2014 Sb. o kybernetické bezpečnosti, včetně jeho novel a jeho prováděcích právních předpisů, především pak analýza aktiv ve vazbě na interní metodiku a plán obnovy.
- Integrační dokumentace popisující jednotlivá aplikační rozhraní (WS a API služby) používaná k integraci Informačních Systémů na jednotlivé funkce včetně funkčních prototypů volání jednotlivých funkcí.
- Schéma zapojení a síťové nastavení protilehlých zařízení.

2 AKCEPTAČNÍ TESTY

Předpokladem pro předání řešení do provozu bude splnění následujících akceptačních testů.

- Veškeré komponenty systému jsou řádně licencované
- Byly dodány fyzické zařízení dle požadované technické specifikace
- Všechny HW i SW komponenty systému jsou nainstalovány a napojeny na infrastrukturu FNO
- Dochází k záznamu netflow a zrcadleného provozu, informace jsou dostupná k zobrazení a dalšímu zpracování
- Výsledná informace definovaná základním filtrem s jedním parametrem (např. IP adresa, podsíť, služba, událost, ...) v 24hodinovém intervalu musí být zobrazena do 30s.
- Systém korektně načítá VLAN-ID ze zrcadlené komunikace a umožňuje filtrování informací podle VLAN-ID
- Systém zobrazuje netflow na základě adres nebo portů po překladu NAT
- Systém graficky znázorňuje skutečně přenesená data (In/Out) filtrovaná podle jednotlivých zdrojů flow nebo fyzických/logických interfaces
- Systém detekuje známé hrozby na základě databáze známých hrozeb, systém detekuje anomálie na základě dynamicky se měnících modelů chování jednotlivých zařízení
- Na základě detekce anomálií síťového provozu došlo k zablokování přístupu nakaženého síťového zařízení od sítě Internet
- Byla vytvořena a dodána provozní dokumentace
- Bylo provedeno školení v požadovaném rozsahu.

Příloha č. 2

Položkový rozpočet předmětu plnění

Popis plnění	*Cena*
HW a SW pro lokalitu FN Ostrava	
1 x DELL HW datový kolektor a sensor, celková propustnost 10 Gbps, monitorovací rozhraní 4 x 1GE RJ45 a 8 x 10GE SFP+ včetně 6x 10Gb LR Transceiver a 2x 10Gb SR Transceiver. Celková disková kapacita úložiště je 45 TB SSD disků. Šasi pro montáž do standardního racku (800 x 800 mm) o velikosti max. 2U. Neomezená licence SW GREYCORTEX Mendel, ser. č. MA-SC-10k-SW Podpora na dodaný HW 5x9 s reakční dobou 8 hodin a garantovanou opravou NBD (Next Business Day on-site) po celé období 5 let Servisní podpora a rozšířená technická podpora k SW na období 5 let.	**2 614 000**
HW a SW pro lokalitu LDN Klokočov	
1 x DELL HW datový kolektor a sensor o celkové propustnosti 200 Mbps s monitorovacím rozhraním 2 x 1GE RJ45. Celková disková kapacita úložiště je 4 TB disků. Šasi pro montáž do standardního racku (800 x 800 mm) o velikosti max. 2U. Neomezená licence SW GREYCORTEX Mendel, ser. č. MA-SC-200-SW Podpora na dodaný HW 5x9 s reakční dobou 8 hodin a garantovanou opravou NBD (Next Business Day on-site) po celé období 5 let Servisní podpora a rozšířená technická podpora k SW na období 5 let.	**350 000**
Instalace a implementace	**75 000**
Zaškolení a zhotovení dokumentace	**160 000**

Příloha č. 3

Realizační tým dodavatele

Označení role	Jméno a příjmení	Kontaktní údaje (telefon, e-mail)
IT specialista na systémy analýzy síťového provozu – hlavní architekt	[redacted]	
IT specialista na systémy analýzy síťového provozu		