[redacted]

SMLOUVA O POSKYTOVÁNÍ SLUŽBY

Číslo smlouvy Zadavatele: CES/2021/0548

Smluvní strany:

Městská část Praha 1

se sídlem:	Vodičkova 681/18, 115 68, Praha 1
zastoupená:	Ing. Petrem Hejmou, starostou
IČ:	00063410
DIČ:	CZ00063410

(dále jen „**Zadavatel**")

a

Rexonix s.r.o.

Se sídlem:	Pod višňovkou 1661/35, Krč, 140 00 Praha 4
Zastoupený:	Michaelem Pechmanem, provozním ředitelem
IČ:	04493982
DIČ:	CZ04493982
bankovní spojení:	Česká spořitelna a.s.
č. účtu	4071125319/0800
Zapsaný v obchodním rejstříku vedeném	u Městského soudu v Praze oddíl C vložka 248598

(dále jen „**Poskytovatel**")

(Zadavatel a Poskytovatel dále společně též jako „smluvní strany")

se níže uvedeného dne, měsíce a roku, v souladu s ustanoveními § 1746 odst. 2 zákona č. 89/2012 Sb., občanského zákoníku, s přihlédnutím k ust. § 2586 a násl. zákona č. 89/2012 Sb., občanského zákoníku, dohodly na základě usnesení Rady MČ Praha 1 č. UR21_0495 ze dne 4. 5. 2021 a vzájemného konsenzu o všech dále uvedených ustanoveních tak, jak stanoví tato:

SMLOUVA O POSKYTOVÁNÍ SLUŽBY

I.
Preambule

1. Tato smlouva je uzavírána na základě výsledků výběrového řízení pro zakázku malého rozsahu v souladu s ustanovením § 31 zákona č. 134/2016 Sb. o zadávání veřejných zakázek, s názvem „Monitoring sítě".
2. Poskytovatel prohlašuje, že se náležitě seznámil se všemi zadávacími podmínkami veřejné zakázky (dále jen „Zadávací dokumentace"), a které stanovují požadavky na předmět plnění Smlouvy, a že je odborně způsobilý ke splnění všech jeho závazků podle Smlouvy. Poskytovatel dále prohlašuje, že se detailně seznámil s rozsahem a povahou předmětu plnění, že jsou mu známy veškeré relevantní technické, kvalitativní a jiné podmínky nezbytné k realizaci předmětu plnění, a že disponuje takovými kapacitami a odbornými znalostmi, které jsou nezbytné pro realizaci předmětu plnění za dohodnutou maximální smluvní cenu uvedenou ve Smlouvě. Poskytovatel prohlašuje, že nemůže nastat změna skutečností, které by plnění předmětu plnění dle této

smlouvy podstatně ztěžovala. Poskytovatel prohlašuje, že pokud by v rámci plnění vznikla potřeba jiného úsilí nebo jiných nákladů, než bylo předpokládáno, nemá to vliv na cenu sjednanou v této smlouvě.

3. V případě jakékoliv nejistoty ohledně výkladu jednotlivých ustanovení Smlouvy budou tato ustanovení vykládána tak, aby v co nejširší míře zohledňovala účel a cíle Veřejné zakázky vyjádřený a vyplývající ze Zadávací dokumentace a této Smlouvy.

II.
Předmět smlouvy

1. Předmětem plnění je řádné poskytování služeb specifikovaných v Příloze č. **D01 – Technická specifikace předmětu veřejné zakázky** Poskytovatelem a závazek Zadavatele zaplatit za tyto služby Poskytovateli odměnu uvedenou v čl. III odst. 1 této smlouvy.

III.
Cena plnění a způsob fakturace

1. Celková cena plnění

   Celková cena plnění za služby podle čl. II za období od 1. 5. 2021 do 30. 4. 2024 je nabídkovou cenou uchazeče vzešlou z výsledků výběrového řízení veřejné zakázky „Monitoring sítě" a představuje částku:

	Cena bez DPH v Kč	**Výše PDH 21% v Kč**	**Cena s DPH v Kč**
Poskytnuté řešení na 36 měsíců	1 236 077,00 Kč	259 576,17 Kč	1 495 653,17 Kč
Implementace, konfigurace, školení	37 500,00 Kč	7 875,00 Kč	45 375,00 Kč
Služby bezpečnostního dohledu na 1 až 6 měsíc	175 680,00 Kč	36 892,80 Kč	212 572,80 Kč
Služby bezpečnostního dohledu na 7. až 36 měsíc	340 630,00 Kč	71 532,30 Kč	412 162,30 Kč
Celková cena (za 36 měsíců)	**1 789 887,00 Kč**	**375 876,27 Kč**	**2 165 763,27 Kč**

   Tato částka se stanovuje jako nejvýše přípustná a obsahuje veškeré náklady poskytovatele, včetně ostatních prací spojených s poskytováním plnění a nezbytné míry zisku.

2. Harmonogram plateb

   Fakturace bude probíhat měsíčně na základě akceptačního protokolu podepsaného oprávněnou osobou zadavatele.

3. Zadavatel neposkytuje dle této smlouvy zálohy.

4. Oprávněně vystavený daňový doklad musí mít veškeré náležitosti daňového dokladu (faktury) dle zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů. Dále musí obsahovat i tyto údaje:

   - pořadové číslo faktury, datum vystavení a datum splatnosti faktury, datum uskutečnění zdanitelného plnění;
   - identifikaci poskytovatele podle Obchodního rejstříku, pakliže je v něm zapsán;
   - označení banky a čísla účtu poskytovatele dle této smlouvy;

- celkovou fakturovanou částku bez DPH, vyčíslení sazby a výše DPH a celkovou cenu vč. DPH;
- evidenční údaje akce („název veřejné zakázky malého rozsahu");
- vlastnoruční podpis vystavitele, včetně kontaktního telefonního čísla;
- Akceptační protokol.

5. Délka splatnosti daňových dokladů (faktur) je 30 dnů od jejich doručení zadavateli.

6. V případě, že faktura nebude obsahovat potřebné náležitosti uvedené v předešlém odstavci, nebo bude obsahovat chybné či neúplné údaje (vč. chybně účtované ceny) či nebude připojen oboustranně podepsaný Akceptační protokol se zhodnocením kvalitativních parametrů za uplynulý kalendářní měsíc, je zadavatel oprávněn ji vrátit poskytovateli k opravě či doplnění s uvedením důvodu vrácení. Vrácení faktury musí být provedeno do data její splatnosti. Po vrácení faktury (nové či opravené) počíná běžet nová lhůta splatnosti uvedená v čl. III odst. 6 této smlouvy.

7. Zadavatel je oprávněn pozastavit či jednostranně započíst proti pohledávkám poskytovatele kteroukoli z plateb z důvodu (1) škody způsobené zadavateli, (2) opakovaného neplnění ze strany poskytovatele, (3) v případě existence jakýchkoliv oprávněných finančních či jiných nároků zadavatele vůči poskytovateli, nebo (4) uplatnění smluvních pokut. V případě, že taková pohledávka neexistuje, bude faktura uhrazena v souladu a ve výši dle předchozích odstavců tohoto článku. Poskytovatel není oprávněn započíst žádnou svou pohledávku proti pohledávce zadavatele z této smlouvy.

8. Smluvní strany se dohodly, že stane-li se poskytovatel nespolehlivým plátcem nebo daňový doklad poskytovatele bude obsahovat číslo bankovního účtu, na který má být plněno, aniž by bylo uvedeno ve veřejném registru spolehlivých účtů, je zadavatel oprávněn z finančního plnění uhradit daň z přidané hodnoty přímo místně a věcně příslušnému správci daně poskytovatele.

9. Fakturovaná částka se považuje uhrazenou okamžikem jejího odepsání z účtu zadavatele.

IV.

Doba plnění

1. Doba poskytování plnění dle této smlouvy je od nabytí účinnosti smlouvy po dobu 36 měsíců.

V.

Způsob poskytování plnění služby, povinnosti smluvních stran

1. Poskytovatel je povinen poskytnout zadavateli plnění definované v čl. II. této smlouvy za podmínek sjednaných v této smlouvě, na svou odpovědnost a po sjednanou dobu.

2. Poskytovatel se zavazuje, že bude při poskytování plnění postupovat s odbornou péčí, podle svých nejlepších znalostí a schopností a sledovat a chránit oprávněné zájmy zadavatele. Poskytovatel se dále zavazuje dodržovat obecně závazné předpisy, technické normy a ustanovení této smlouvy.

3. Poskytovatel je povinen vykonávat své povinnosti podle podmínek této Smlouvy v souladu s legislativním rámcem této Smlouvy a interními předpisy zadavatele, se kterými bude poskytovatel seznámen. O seznámení musí být učiněn písemný zápis. Legislativní rámec tvoří:

   - splnění požadavků legislativy ČR, vztahující se k předmětu plnění této Smlouvy,
   - splnění metodik vydávaných pro územní samosprávné celky (vydávají centrální a jimi pověřené orgány a Magistrátu hl. města Prahy (MHMP)), se kterými bude poskytovatel seznámen,
   - splnění metodik zadavatele, se kterými bude poskytovatel seznámen.

4. Poskytovatel je povinen po celou dobu platnosti smlouvy zajistit pro zadavatele dostupnost služeb, a to v souladu s přílohou D01 Technická specifikace předmětu veřejné zakázky.

5. Poskytovatel má povinnost zadavateli nabízet řešení, která umožní zajistit bezporuchový běh celého spravovaného a podporovaného systému.

6. Poskytovatel je povinen informovat zadavatele na jeho žádost o průběhu plnění předmětu smlouvy a akceptovat jeho doplňující pokyny a připomínky k plnění předmětu smlouvy. Poskytovatel je však povinen bez zbytečného odkladu písemně upozornit zadavatele na nevhodnou povahu věci, kterou mu zadavatel k provedení plnění předal, nebo příkazu (pokynu), který mu zadavatel dal. To neplatí, nemohl-li nevhodnost zjistit ani při vynaložení potřebné péče.

7. Poskytovatel je povinen v průběhu poskytování služby zajistit bezpečnost informací Objednavatele, s kterými přichází do styku a/nebo se seznámí při poskytování služby. Dále je Poskytovatel povinen řídit se platnými směrnicemi týkající se bezpečnosti informací a provozu

8. Poskytovatel se zavazuje provádět plnění předmětu této Smlouvy tak, aby nebyla ohrožena realizace těch činností zadavatele, pro jejichž podporu je předmět této Smlouvy určen.

9. Veškeré odborné práce musí vykonávat pracovníci poskytovatele mající příslušnou kvalifikaci. Doklad o příslušné kvalifikaci pracovníků je poskytovatel na požádání zadavatele povinen doložit. Poskytovatel odpovídá za to, že bude mít pro své zaměstnance poskytující plnění veškerá potřebná školení a platná kvalifikační potvrzení.

10. Zadavatel je povinen předat a bude předávat poskytovateli všechny potřebné informace a údaje, které má zadavatel a které jsou nutné, aby poskytovatel mohl vykonávat služby podle této Smlouvy. Zároveň se zavazuje zodpovídat dotazy poskytovatele ve vztahu k plnění podle této Smlouvy, a to do 2 dnů od obdržení dotazu, nedohodnou-li se smluvní strany v konkrétním případě jinak.

11. Zadavatel se zavazuje umožnit přístup pracovníkům poskytovatele do objektů zadavatele a k systémům v rozsahu nezbytném pro plnění předmětu této smlouvy a dle potřeby Poskytovatele umožnit vzdálený přístup ke spravovanému systému.

12. Poskytovatel se zavazuje, že zajistí, aby jeho pracovníci podílející se na plnění podle této Smlouvy při pobytu na pracovištích zadavatele dodržovali vnitřní předpisy, pokyny a směrnice zadavatele, dodržovali předpisy zadavatele upravující pohyb na pracovištích, pro požární bezpečnost, pro ochranu zdraví při práci a další předpisy, se kterými bude poskytovatel seznámen, přičemž poskytovatel zajistí, že o takovém seznámení bude pořízen písemný zápis.

13. Poskytovatel není oprávněn bez souhlasu zadavatele, s výjimkou příslušných ustanovení zákona č. 89/2012 Sb. Občanský zákoník a zákona č. 90/2012 Sb. O obchodních korporacích týkajících se přeměny společnosti, postoupit svá práva a závazky vyplývající z této Smlouvy na třetí osoby, a to včetně postoupení pohledávky, dluhu, ručení, zástavy i jakéhokoli zajištění závazku.

14. Pokud budou Poskytovateli předány informace a údaje, které budou obsahovat osobní údaje, je Poskytovatel povinen dodržovat zásady a pravidla ochrany těchto osobních údajů v souvislosti s jejich zpracováním v souladu s Nařízením Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) a se zákonem č. 110/2019 S., o zpracování osobních údajů.

VI.

Místo plnění

Místem plnění poskytovatele je sídlo zadavatele a všechna jeho pracoviště v Praze.

VII.

Součinnost smluvních stran

1. Smluvní strany se zavazují poskytnout druhé smluvní straně dohodnutou součinnost

umožňující řádné plnění této smlouvy.

2. Smluvní strany se zavazují úzce spolupracovat, zejména si poskytovat úplné, pravdivé a včasné informace potřebné k řádnému plnění svých závazků, přičemž v případě změny podstatných okolností, které mají nebo mohou mít vliv na plnění prováděcí smlouvy, jsou povinny o takové změně informovat druhou smluvní stranu nejpozději do deseti pracovních dnů po provedení takové změny.
3. V zájmu optimálního plnění této smlouvy jsou smluvní strany povinny plnit řádně a včas své závazky tak, aby nedocházelo k prodlení s jejich plněním. Pokud se některá ze smluvních stran dostane do prodlení s plněním svých závazků, je povinna oznámit bez zbytečného odkladu druhé smluvní straně důvod prodlení a předpokládaný termín a způsob jeho odstranění.
4. Smluvní strany se zavazují plnit své závazky v souladu se všemi příslušnými obecně závaznými legislativními předpisy.
5. Žádná ze smluvních stran není odpovědna za prodlení způsobené prodlením s plněním závazků druhé smluvní strany.
6. Komunikace smluvních stran probíhá na úrovni oprávněných osob a jejich zástupců. Zástupci oprávněných osob přitom oprávněnou osobu zastupují v rámci její působnosti. Za tím účelem se stanovují následující osoby:

Zadavatel	Jméno a příjmení	Kontaktní telefon	Kontakt - email
oprávněná osoba	[redacted]		
zástupce oprávněné osoby			
Poskytovatel			
oprávněná osoba			
zástupce oprávněné osoby			

7. Stanovením kontaktních osob a jejích zástupců není dotčena možnost smluvních stran komunikovat prostřednictvím svých statutárních orgánů.
8. Všechny dokumenty mající vztah k plnění této smlouvy, představující vícestranné či jednostranné úkony smluvních stran, například protokoly, výzvy, výpovědi, upozornění, žádosti a jiná oznámení, musí být vyhotoveny písemně a podepsány oprávněnými osobami.
9. Dokumenty uvedené v předchozím odstavci se vždy doručují druhé smluvní straně, a to některým ze způsobů dále uvedených:
   - osobně oproti potvrzení o převzetí,
   - doporučeným dopisem či jinou formou registrovaného poštovního styku. V tomto případě se dokumenty považují za doručené dnem jejich převzetí adresátem, nebo v případě, že adresát nebyl zastižen dnem doručení zpět odesílateli a dále dnem, kdy adresát převzetí zásilky odmítl,
   - Prostřednictvím datové schránky nebo elektronickou poštou. V tomto případě se dokumenty považují za doručené okamžikem, kdy odesílatel obdrží od příslušného technického zařízení potvrzení o úspěšném odeslání nebo potvrzení o doručení.
10. V případě doručování dokumentů v elektronické formě smluvní strany zavazují používat formát „.doc(x)", nebo „.pdf". Dokumenty v elektronické formě lze doručovat prostřednictvím

elektronické pošty, prostřednictvím datové schránky nebo na dohodnutém datovém médiu.

11. Dokumenty se doručují na adresu poskytovatele uvedenou v záhlaví této smlouvy, není-li stanoveno nebo dohodnuto jinak.

12. Další požadavky na součinnost mohou písemně dohodnout oprávněné osoby smluvních stran

VIII.

Ochrana důvěrných informací

1. Smluvní strany se zavazují zachovávat mlčenlivost ohledně skutečností, které se v souvislosti s plněním této Smlouvy dozvěděly, a to v rozsahu sjednaném v tomto článku Smlouvy. Za důvěrné informace jsou považovány jednak veškeré informace bez ohledu na formu jejich zachycení, které nebyly označeny jako veřejné a které se týkají Smlouvy, předmětu Smlouvy v ní sjednaného (zejména informace o právech a povinnostech smluvních stran, jakož i informace o cenách) či porušení zmíněné Smlouvy, dále (zejména, nikoliv však výlučně) obchodní tajemství, informace o činnosti příslušné smluvní strany, struktuře, hospodářských výsledcích, know-how), nebo případné informace, pro nakládání s nimiž je stanoven právními předpisy zvláštní režim utajení (osobní údaje, aj.), jednak informace, které byly jako důvěrné výslovně příslušnou smluvní stranou označeny; za důvěrné informace se však nepovažují informace, které se staly veřejně přístupnými, pokud se tak nestalo porušením povinnosti jejich ochrany jednou ze smluvních stran, dále informace získané na základě postupu nezávislého na této smlouvě, pokud je příslušná smluvní strana schopna tuto skutečnost doložit, a konečně informace poskytnuté třetí osobou, která takové informace nezískala porušením povinnosti jejich ochrany některé ze smluvních stran (dále jen jako „Důvěrné informace").

2. Poskytovatel je povinen Důvěrné informace ochránit proti úniku či neoprávněnému užití. Důvěrné informace mohou být Poskytovatelem využívány výlučně pro přípravu a poskytování předmětu smlouvy dle Smlouvy, není-li ve Smlouvě uvedeno jinak. Poskytovatel se zavazuje zachovávat mlčenlivost o Důvěrných informacích a zavazuje se, že přijme odpovídající opatření k ochraně Důvěrných informací.

3. Poskytovatel se zavazuje, že Důvěrné informace, které v souvislosti s poskytováním předmětu Smlouvy nebo při přípravě poskytování předmětu Smlouvy Poskytovateli poskytne Zadavatel, nebude bez písemného souhlasu Zadavatele žádným způsobem rozmnožovat (kromě potřebných kopií pro poskytnutí předmětu Smlouvy) a kdykoliv je na požádání vrátí Zadavateli, včetně všech případně vzniklých kopií a nosičů Důvěrných informací, nebo je na základě požadavku této smluvní strany zničí, včetně všech případně vzniklých kopií a nosičů Důvěrných informací.

4. Poskytovatel se zavazuje, že bez písemného souhlasu Zadavatele neposkytne Důvěrné informace v žádné formě třetím osobám. Poskytovatel je povinen zajistit, že jeho případný subdodavatel bude zachovávat mlčenlivost o Důvěrných informacích. Poruší-li subdodavatel Poskytovatele povinnost mlčenlivosti ve vztahu k Důvěrným informacím, považuje se to za porušení povinnosti mlčenlivosti Poskytovatele.

5. Za porušení povinnosti mlčenlivosti se nepovažuje, je-li Poskytovatel, jeho zaměstnanec, spolupracující osoba, zástupce nebo další osoba v obdobném postavení povinen Důvěrnou informaci sdělit na základě zákonem stanovené povinnosti.

6. Poskytovatel je povinen uvědomit Zadavatele o porušení povinnosti mlčenlivosti nebo ochrany Důvěrných informací podle Smlouvy bez zbytečného odkladu poté, co se o takovém porušení dozví.

7. Povinnost mlčenlivosti a ochrany Důvěrných informací podle Smlouvy trvá po dobu účinnosti Smlouvy a dále 3 (slovy: tři) roky po jejím ukončení.

8. Vzhledem k veřejnoprávnímu charakteru Zadavatele Poskytovatel výslovně prohlašuje, že je s touto skutečností obeznámen, že žádné ustanovení této Smlouvy nepodléhá z jeho strany obchodnímu tajemství a souhlasí se zveřejněním smluvních podmínek obsažených ve Smlouvě, včetně jejích příloh a případných dodatků Smlouvy za podmínek vyplývajících z příslušných právních předpisů, zejména zák. č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů a zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákona o registru smluv).

IX.
Pojištění

1. Poskytovatel se zavazuje, že po celou dobu poskytování svých služeb podle této smlouvy bude pojištěn pro případy škody vyplývající z výkonu svojí podnikatelské činnosti na částku předmětného pojištění alespoň 5.000.000 Kč s max. 10% spoluúčastí. Kopie pojistné smlouvy (či pojistný certifikát) je pak přílohou č. D03 této smlouvy. Poskytovatel je povinen být pojištěn i proti případným odcizením, ztrátám či poškození věcí Zadavatele.

X.
Odpovědnost za způsobenou škodu, záruka za jakost plnění, vady plnění

1. Smluvní strany se zavazují k vyvinutí maximálního úsilí k předcházení škodám a k minimalizaci vzniklých škod. Smluvní strany nesou odpovědnost za škodu dle platných právních předpisů a Smlouvy.
2. Poskytovatel odpovídá za škodu rovněž v případě, že část plnění poskytuje prostřednictvím subdodavatele. Poskytovateli se zavazuje uhradit zadavateli či orgánu veřejné moci veškeré finanční částky, které budou poskytovateli ve správním, soudním či jiném obdobném řízení uloženy jako pokuty či jiné majetkoprávní sankce za poskytovatelem způsobené porušení právních povinností.
3. Žádná ze smluvních stran není odpovědná za škodu nebo prodlení způsobené okolnostmi vylučujícími odpovědnost ve smyslu Občanského zákoníku. Smluvní strany se zavazují upozornit druhou smluvní stranu bez zbytečného odkladu na vzniklé okolnosti vylučující odpovědnost a bránící řádnému plnění Smlouvy. Smluvní strany se zavazují k vyvinutí maximálního úsilí k odvrácení a překonání okolností vylučujících odpovědnost.
4. Poskytovatel přebírá závazek a odpovědnost za jím způsobené vady předmětu smlouvy, jež bude mít v době jeho předání zadavateli a dále za vady, které se na předmětu Smlouvy vyskytnou v průběhu záruční doby. Poskytovatel v souvislosti s odpovědností za vady plnění poskytuje zadavateli záruku, která skončí uplynutím 24 (slovy: dvacet čtyři) měsíců od zahájení plnění, na to, že předmět Smlouvy bude mít vlastnosti stanovené Smlouvou, bude plně funkční a způsobilé pro použití ke smluvenému účelu, bude odpovídat sjednané funkční a technické specifikaci a parametrům uvedeným ve Smlouvě a bude bez jakýchkoliv nedodělků či vad. Záruka se vztahuje na všechny části plnění, včetně jeho příslušenství a pokrývá všechny součásti plnění předmětu Smlouvy, včetně produktů či činností třetích stran, které byly využity při realizaci plnění dle Smlouvy.
5. Poskytovatel je povinen poskytovat plnění dle Smlouvy v nejvyšší dostupné kvalitě a odpovídá za to, že případné vady plnění poskytnutého dle Smlouvy řádně odstraní, případně nahradí plněním bezvadným, v souladu se Smlouvou a jejími přílohami.

XI.

Zánik smlouvy

1. Tato smlouva primárně zaniká uplynutím doby, na kterou je uzavřena. Před uvedeným datem smluvní strany dále mohou ukončit smluvní vztah písemnou dohodou obou smluvních stran. Tato smlouva může také zaniknout i jednostrannou výpovědí či odstoupením od smlouvy.
2. Zadavatel je oprávněn odstoupit od této smlouvy:
   - v případě, že probíhá insolvenční řízení proti majetku poskytovatele, v němž bylo vydáno rozhodnutí o úpadku nebo insolvenční návrh byl zamítnut proto, že majetek poskytovatele nepostačuje k úhradě nákladů insolvenčního řízení, nebo byl konkurs zrušen proto, že majetek poskytovatele byl zcela nepostačující;
   - v případě podstatného porušení této smlouvy poskytovatelem, zejména v případě kdy poskytovatel využil k plnění předmětu této smlouvy subdodavatele v rozporu s nabídkou poskytovatele v rámci výběrového řízení nebo bez předchozího souhlasu zadavatele,
   - v případě, že poskytovatel nepředloží objednateli nový platný originál potvrzení, že poskytovatel je akreditovaným - autorizovaným poskytovatelem produktu GREYCORTEX Mendel a souvisejících služeb a podpory (Příloha č. D02 této smlouvy), a to ve lhůtě 7 pracovních dnů od pozbytí platnosti původního potvrzení.
3. Zadavatel je také oprávněn odstoupit od této smlouvy v případě, kdy vyjde najevo, že poskytovatel uvedl v rámci výběrového řízení nepravdivé či zkreslené informace, které by měly zřejmý vliv na výběr poskytovatele pro uzavření této smlouvy.
4. Smluvní strany jsou oprávněny od této smlouvy dále odstoupit za podmínek stanovených občanským zákoníkem nebo jinými právními předpisy.
5. Odstoupení od smlouvy musí být učiněno písemným oznámením o odstoupení od této smlouvy druhé straně, účinky odstoupení nastávají dnem doručení oznámení druhé straně. V pochybnostech se má za to, že odstoupení bylo doručeno do 10 dnů od jeho odeslání v poštovní zásilce s dodejkou, resp. do 10 dnů od jeho odeslání prostřednictvím informačního systému datových schránek.
6. Zadavatel je oprávněn smlouvu vypovědět písemnou výpovědí s 3 měsíční výpovědní lhůtou. Výpovědní lhůta začíná běžet dnem doručení výpovědi poskytovateli.
7. Strany se dohodly, že po ukončení smlouvy trvají a zůstávají v platnosti ujednání stran týkající se odpovědnosti za vady, záruk za jakost a záruční lhůty, smluvních pokut, náhrady škody a cenová ujednání obsažená v této smlouvě.

XII.

Sankce, nárok na slevu při nedodržení SLA služby

1. Pro případ že poskytovatel nezahájí plnění dle této smlouvy řádně, ve sjednaném rozsahu a v termínu dle čl. IV odst. 1 smlouvy, zavazuje se zadavateli zaplatit smluvní pokutu ve výši 5.000,--Kč za každý den prodlení.
2. Poruší-li poskytovatel kteroukoli povinnost mlčenlivosti uvedenou čl. VIII. odst. 1 až čl. VIII. odst. 4 smlouvy, zavazuje se zadavateli uhradit smluvní pokutu ve výši 100.000,--Kč za každý jednotlivý případ porušení povinnosti
3. Pro případ, že Poskytovatel nezačne řešit nahlášenou závadu monitorovacího systému do 24 hodin od nahlášení (resp. Zadavatel ve stanovené lhůtě neobdrží notifikační email o zahájení řešení), zavazuje se Zadavateli uhradit smluvní pokutu ve výši 500,--Kč za každý jeden den prodlení.

4. Pro případ, že Poskytovatel do 72 hodin od nahlášení závady monitorovacího systému nevyřeší nahlášenou závadu, zavazuje se Zadavateli neúčtovat pronájem služby (systému) do doby jejího odstranění.
5. Uplatněné smluvní pokuty se nezapočítávají na náhradu škody, která zadavateli vznikla nedodržením ustanovení této smlouvy či platných zákonů ze strany poskytovatele.
6. Při prodlení zadavatele s úhradou jakékoli dlužné částky je poskytovatel oprávněn účtovat zadavateli úrok z prodlení v zákonné výši, stanovené nařízením vlády č. 351/2013 Sb., ve znění pozdějších předpisů.
7. Smluvní pokuty jsou splatné do 30 dnů od dne obdržení příslušného vyúčtování.
8. Pokud závazek provést plnění dle této smlouvy zanikne řádným ukončením plnění, nezaniká nárok na smluvní pokutu, která souvisí s dřívějším porušením povinností.
9. Při prodlení poskytovatele s úhradou sankce proti sjednanému termínu úhrady je zadavatel oprávněn účtovat úrok z prodlení ve výši 0,05% z dlužné částky za každý, i započatý den prodlení.
10. Sankci (smluvní pokutu, úrok z prodlení) vyúčtuje oprávněná strana straně povinné písemnou formou. Ve vyúčtování musí být uvedeno to ustanovení smlouvy, které k vyúčtování sankce opravňuje a způsob výpočtu celkové výše sankce.
11. Strana povinná se musí k vyúčtování sankce vyjádřit nejpozději do deseti dnů ode dne jeho obdržení, jinak se má za to, že s vyúčtováním souhlasí. Vyjádřením se v tomto případě rozumí písemné stanovisko strany povinné. Nesouhlasí-li strana povinná s vyúčtováním sankce, je povinna písemně ve sjednané lhůtě sdělit oprávněné důvody, pro které vyúčtování sankce neuznává.

XIII.
Kontrola

1. Zadavatel je oprávněn zmocnit třetí osobu za účelem provádění průběžné kontroly plnění povinností poskytovatele, včetně kontroly systému řízení služeb poskytovatele formou zákaznického auditu. Poskytovatel je povinen poskytnout třetí osobě součinnost nezbytnou pro provádění kontroly.
2. Bude-li zadavatel provádět jakýkoliv audit, atestaci nebo certifikaci, je poskytovatel povinen poskytnout zadavateli potřebnou součinnost a dokumentaci. Odpovědnost za atestaci dle legislativy (např. ISVS a další) nese zadavatel. Poskytovatel je povinen poskytnout součinnost k atestaci a současně poskytovat služby v souladu s těmito parametry tak, aby zadavatel mohl atestaci úspěšně absolvovat.
3. Poskytovatel je povinen při kontrole poskytnout na vyžádání kontrolnímu orgánu daňovou evidenci v plném rozsahu. Poskytovatel je podle ustanovení § 2 písm. e) zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole), ve znění pozdějších předpisů, osobou povinnou spolupůsobit při výkonu finanční kontroly prováděné v souvislosti s úhradou zboží nebo služeb z veřejných výdajů.

XIV.
Rozhodné právo, řešení sporů

1. Právní vztahy vyplývající z této smlouvy o dílo se řídí zákony České republiky, zejména zákonem č. 89/2012 Sb., občanským zákoníkem.
2. Smluvní strany se zavazují vyvinout maximální úsilí k smírnému odstranění a vyřešení sporů vzniklých z této smlouvy operativně, a to zejména prostřednictvím oprávněných osob nebo

statutárních orgánů. První smírčí jednání se musí uskutečnit do dvou pracovních dnů, nedohodnou-li se smluvní strany jinak.

3. V případě, že spor nebude vyřešen konsensem podle předchozího odstavce, smluvní strany se dohodly řešit spor před soudem. Soudem příslušným pro všechny spory vzniklé z této smlouvy mezi zadavatelem a poskytovatelem je obecný soud zadavatele, v případě právního nástupce zadavatele nebo osoby, na níž byla převedena práva a povinnosti zadavatele ze smlouvy obecný soud této osoby.

XV.

Závěrečná ustanovení

1. Poskytovatel souhlasí se zveřejněním údajů uvedených ve smlouvě v souladu se zákonem č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů.
2. Poskytovatel souhlasí se zveřejněním této smlouvy včetně všech příloh a případných dodatků.
3. Tato Smlouva nabývá platnosti v den podpisu této Smlouvy druhou smluvní stranou a účinnosti dnem uveřejnění v registru smluv Ministerstva vnitra ČR, 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), včetně důsledků porušení této povinnosti. Povinnost uveřejnit smlouvu v registru smluv MV ČR náleží městské části Praha 1.
4. Smluvní strany výslovně souhlasí s tím, aby tato smlouva byla uvedena v Centrální evidenci smluv **(CES) vedené zadavatelem, která je veřejně přístupná a obsahuje údaje o smluvních stranách, předmětu Smlouvy**, číselné označení této Smlouvy a datum jejího podpisu i v případné evidenci smluv zadavatele.
5. Veškeré změny či doplnění této Smlouvy lze učinit pouze na základě písemné dohody smluvních stran. Takové dohody musí mít podobu datovaných, číslovaných a oběma smluvními stranami podepsaných dodatků Smlouvy.
6. Tato Smlouva je vyhotovena ve dvou vyhotoveních, z nichž zadavatel obdrží jedno vyhotovení a poskytovatel také jedno vyhotovení.
7. Tímto se osvědčuje v souladu s ustanovením § 43 zákona č. 131/2000 Sb., o hlavním městě Praze, v platném znění., že návrh na uzavření této smlouvy byl projednán a schválen Radou městské části Praha 1 dne 4. 5. 2021 usnesením č. UR21_0495.

Nedílnou součástí této Smlouvy jsou následující přílohy:

Číslo	Příloha
D01	Technická specifikace předmětu veřejné zakázky
D02	Potvrzení výrobce
D03	Pojistná smlouva či pojistný certifikát

[redacted]

Příloha D01 – Technická specifikace předmětu veřejné zakázky

Systém služby a technologie pro analýzu síťového provozu a bezpečnostní monitoring, který okamžitě identifikuje bezpečnostní rizika a události a který splňuje klíčové požadavky uvedené níže.
Nabízená technologie musí být dodána jako služba určená pro český trh. HW a SW licence a jejich PN (produktové číselné označení) musí být dostupné přímo v oficiálním ceníku výrobce pro český trh. Podpora na licence ve všech úrovních musí být zajištěna přímo jejich výrobcem, kterého může Zadavatel přímo kontaktovat.
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, účastník zadávacího řízení (dále jen „Účastník") může nabídnout charakteristiky (funkce) lepší.

Řešení musí splňovat **VŠECHNY** níže uvedené požadavky:

Popis nabízených komponent musí účastník zadávacího řízení zpracovat podle následujících podmínek:

1.1 Ve 2. sloupci následujících tabulek v každém řádku účastník zadávacího řízení potvrdí, že splňuje požadované technické podmínky uvedené v 1. sloupci tabulky slovem „ANO" či jiným slovem např. „SPLŇUJE" apod., a uvede konkrétní technickou hodnotu stěžejního nabízeného parametru a popis způsobu splnění technického požadavku, který je součástí nabízeného řešení. Z vyjádření v posledním sloupci u každého řádku musí být zřejmé, že účastník zadávacího řízení splňuje anebo překračuje požadované technické podmínky.

1.2 Údaje stanovené zadavatelem v 1. sloupci tabulky nesmí být měněny, vynechány nebo jinak přeskupeny.

1.3 Výčet požadované konfigurace může účastník zadávacího řízení doplnit o další řádky na konci tabulky s užitečnými údaji nebo parametry o nabízené komponentě.

Pokud komentář k některému z řádků v tabulce přesáhne možnosti 2. sloupce tabulky, pak účastník zadávacího řízení uvede v příslušném řádku tabulky jen základní anotaci odpovědi a uvede zde odkaz na konkrétní číslo kapitoly a strany své nabídky obsahující podrobnější údaje.

Obecné požadavky

Požadované funkcionality/vlastnosti	**Nabízené řešení splňuje/nesplňuje (doplní účastník)** **Včetně vysvětlení jak je zadání splněno**
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.	**ANO, nabízené řešení splňuje zadavatelem definované parametry** Nabízené HW + SW řešení monitoruje síťovou aktivitu v reálném čase a identifikuje potenciální kybernetické hrozby, bezpečnostní rizika a anomální chování, v reálném čase o nálezech vytváří 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.	Všechny komponenty systému jsou instalované v interním prostředí zadavatele („on premise").
Analýza plného síťového provozu Dodaný systém musí analyzovat síť na základě zrcadleného síťového provozu (nikoliv jen na základě statistických protokolů typu NetFlow) a zároveň bez potřeby nasazovat agenty na koncové stanice nebo další zařízení v síti. Systém musí být schopen získávat data zrcadlené komunikace ze SPAN portů a síťových TAPů. Systém je zcela pasivní vzhledem k monitorovanému provozu, monitorovaný provoz přes něj neprochází.	**ANO, nabízené řešení splňuje zadavatelem definované parametry** Nabízené řešení analyzuje síť na základě zrcadleného síťového provozu (ne pouze na základě statistických protokolů typu NetFlow) a současně nevyužívá jakékoliv agenty na koncových stanicích a dalších zařízeních v síti. Systém získává data zrcadlené komunikace ze SPAN portů a síťových TAPů. Systém je 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.	**ANO, nabízené řešení splňuje zadavatelem definované parametry** Nabízené řešení analyzuje 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 .	**ANO, nabízené řešení splňuje zadavatelem definované parametry** Nabízené řešení ukládá síťové toky ve formátu, který umožňuje 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. Využívá pro ukládání aplikačních metadat z jednotlivých transakcí následující protokoly: DHCP, DNS, SMB , HTTP, HTTPS, SMTP, SMTPS, POP3, IMAP, SSH, LDAP, LDAPS, KERBEROS, SNMP, CIFS, 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. 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 a MAC adresa, hostname, username, příchozí a odchozí provoz, síťová služba, lokální nebo vzdálená služba (klient nebo server), číslo portu, VLAN, země, ASN.	**ANO, nabízené řešení splňuje zadavatelem definované parametry** Nabízené řešení zahrnuje vysokorychlostní úložiště pro uchování datových toků na dobu minimálně 180 dnů složené z SSD disků. Uživatel může v reálném čase volně filtrovat a vyhledávat v plné historii uložených síťových toků, dat a agregovaných síťových statistik na základě parametrů: IP a MAC adresa, hostname, username, příchozí a odchozí provoz, síťová služba, lokální nebo vzdálená

	služba (klient nebo server), číslo portu, VLAN, země, ASN a dalších.
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.	**ANO, nabízené řešení splňuje zadavatelem definované parametry** Nabízené řešení automaticky detekuje přítomnost klíčových služeb monitorované infrastruktury, jako jsou doménové řadiče, webové, emailové a databázové služby apod. Systém je schopen upozornit na vznik nových služeb v interní síti a sleduje jejich změny v rozsahu služeb: DHCP, DNS, MS Active Direktory služby, HTTP, HTTPS, SMTP, SMTPS, POP3, IMAP, SSH, CIFS, POP3S, IMAPS, MSSQL, TELNET, FTP, TFTP, a to i v případě, že nevyužívají standardních „well known" portů.

Požadavky na architekturu nasazení

Požadované funkcionality/vlastnosti	**Nabízené řešení splňuje/nesplňuje (doplní účastník)** **Včetně vysvětlení jak je zadání splněno**
Požadavky pro nasazení do datového centra Je požadován 1x HW datový koletor/sensor o celkové propustnosti alespoň 1Gbps s monitorovacím rozhraním 4x 1GE a 2x 10GE. Je požadována dostupná historie dat minimálně 6 měsíců zpětně. V síti je předpokládáno cca 2500 aktivních zařízení s průměrným celkový průtokem do 1Gbps.	**ANO, nabízené řešení splňuje zadavatelem definované parametry** Nabízené řešení obsahuje 1x HW datový koletor/sensor o celkové propustnosti minimálně 1Gbps s monitorovacím rozhraním 4x 1GE a 2x 10GE. Řešení zajistí dostupnou historii dat nejméně 6 měsíců zpětně za předpokladu cca 500 aktivních zařízení s průměrným celkový průtokem do 1Gbps, ve špičce do 5Gbps.
Záruka na HW a SW Záruku na veškerá dodaná HW zařízení požadujeme minimálně v rozsahu Next Business Day on-site.	**ANO, nabízené řešení splňuje zadavatelem definované parametry** Záruka na nabízené HW zařízení je zajištěna v rozsahu 5 let v rozsahu NBD (Next Business Day) On-Site.

Požadavky na schopnost detekce bezpečnostních událostí

Požadované funkcionality/vlastnosti	**Nabízené řešení splňuje/nesplňuje (doplní účastník)** **Včetně vysvětlení jak je zadání splněno**
Monitorování zařízení, segmentů sítě a využívaných síťových služeb Dodaný systém musí identifikovat všechna zařízení připojená do sítě včetně koncových zařízení, serverů, IoT	**ANO, nabízené řešení splňuje zadavatelem definované parametry** Nabízené řešení identifikuje všechna zařízení připojená do sítě včetně koncových zařízení,

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.	serverů, IoT zařízení apod. Systém je 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 umožňuje uživateli pomocí těchto detekčních metod nastavovat bezpečnostní politiky pro různé segmenty sítě a pro různá zařízení a na porušení těchto politik reaguje 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.	**ANO, nabízené řešení splňuje zadavatelem definované parametry** Nabízené řešení je schopné 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 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. Systém musí mít schopnost na základě modelu daného zařízení a jeho služeb identifikovat nestandardní síťové chování, a to zejména: • 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	**ANO, nabízené řešení splňuje zadavatelem definované parametry** Nabízené řešení používá matematické metody samostatného učení pro analýzu síťové aktivity, vytváří a automaticky modifikuje v čase modely chování na základě běžného chování jednotlivých zařízení a na nich provozovaných služeb v rámci celé organizace. Systém umožňuje na základě modelu daného zařízení a jeho služeb identifikovat nestandardní síťové chování, a to zejména: 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 probíhá 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.

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.	**ANO, nabízené řešení splňuje zadavatelem definované parametry** Nabízené řešení detekuje neznámé hrozby, které nelze identifikovat prostřednictvím detekčních signatur, jako jsou trojské koně, botnety apod. Identifikuje následující příznaky potenciálně škodlivého chování: průzkumné aktivity v síti, potenciální úniky dat, podezřelé strojové chování, které nevytvářejí lidští uživatelé sítě, detekuje repetitivní vzorce chování na síti, botnety a ovládání kompromitované stanice, detekuje příznaky těžby kryptoměn, útoky hrubou silou a enumerace dat, rozpoznává tunelovaný síťový provoz 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.	**ANO, nabízené řešení splňuje zadavatelem definované parametry** Nabízené řešení identifikuje a reportuje události na základě detekční databáze malware, známých útoků a zranitelností, porušení bezpečnostních pravidel a „best practices" a dalších rizik. Databáze je aktualizovaná minimálně na hodinové bázi. Jedná se o komerční databázi ProofPoint, v nabízeném řešení není využita volně dostupná/open-source databáze. Databáze detekčních pravidel (signatur) je založena na pokročilých regulárních výrazech pro zpracování řetězců, které dokáží provádět inspekci veškeré síťové komunikace od L2 (Ethernet apod.) po L7. Nabízený systém využívá uvedenou signaturní detekci pro veškerý monitorovaný provoz (na perimetru i v interní síti mezi všemi segmenty), nikoliv pouze pro omezený segment nebo podmnožinu celkové komunikace. Nabízené řešení detekuje události na základě vysokého počtu signaturních pravidel (minimálně několik desítek tisíc).

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.	Uživatel má možnost 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.	**ANO, nabízené řešení splňuje zadavatelem definované parametry** Nabízené řešení umožňuje 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.	**ANO, nabízené řešení splňuje zadavatelem definované parametry** Nabízené řešení umožňuje kromě samostatného učení také používání dalších metod pro analýzu šifrované komunikace, např. 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.	**ANO, nabízené řešení splňuje zadavatelem definované parametry** Nabízené řešení ověřuje platnost interních certifikátů pro validní TLS šifrování u HTTPS a upozorňuje 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.	**ANO, nabízené řešení splňuje zadavatelem definované parametry** Nabízené řešení umožňuje korelovat jakékoliv detekované události ze všech detekčních metod a úpravy samostatného učení a dalších detekčních metod s cílem v maximální míře eliminovat falešné alarmy. Systém je schopen eliminovat falešné alarmy i pro události detekované v historii. Nabízené řešení umožňuje zobrazovat zařízení podle souhrnné kritičnosti identifikovaných událostí - kritické, důležité, střední, nízké, informativní.
Aktuální databáze blacklistů Systém musí být schopen hodnotit IP adresy, se kterými komunikují vnitřní hosté v sítí prostřednictvím minimálně denně aktualizovaných reputačních databází. Uživatel musí být schopen importovat vlastní reputační databáze.	**ANO, nabízené řešení splňuje zadavatelem definované parametry** Nabízené řešení vyhodnocuje IP adresy, se kterými komunikují vnitřní hosté v sítí prostřednictvím denně aktualizovaných reputačních databází. Uživatel má možnost importovat vlastní reputační databáze.

Požadavky na zajištění síťové viditelnosti

Požadované funkcionality/vlastnosti	Nabízené řešení splňuje/nesplňuje (doplní účastník) Včetně vysvětlení jak je zadání splněno
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.	**ANO, nabízené řešení splňuje zadavatelem definované parametry** Nabízené řešení umožňuje okamžité vyhledávání a vizualizaci pro forenzní analýzu a podporu threat hunting, k tomu nevyužívá žádný specifický dotazovací jazyka a nevyžaduje hluboké znalosti konkrétních komunikačních protokolů. Umožňuje okamžité filtrování a vyhledávání v plné historii všech zpracovávaných dat, tj. bezpečnostních událostí a zaznamenaných síťových toků 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 a dalších. Nabízené řešení poskytuje pro vyhledávání již předpočítané hodnoty výkonnostních a behaviorálních charakteristik pro každé zařízení a pro všechny na něm provozované služby, nevyžaduje zpracování surových dat ze síťových logů. Systém je schopen filtrovat a vizualizovat výsledky v grafech, výčtových tabulkách, umožňuje řazení a TOP N statistiky.
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.	**ANO, nabízené řešení splňuje zadavatelem definované parametry** Nabízené řešení umožňuje ukládání a následné vyhledávání aplikačních metadat (vždy dotaz i odpověď všech transakcí v toku) z 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 jsou informace ukládány souborech přenášených po síti v rozsahu: název souboru, velikost souboru, HASH souboru.
Kontextuální informace	**ANO, nabízené řešení splňuje zadavatelem definované parametry** Nabízené řešení umožňuje pro každé zařízení získávat, vizualizovat a integrovat v jednotném

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	grafickém rozhraní následující kontextuální informace: • Jméno uživatele a další jeho parametry z doménového řadiče (MS Active Directory), včetně historie • Hostname zařízení a jeho historie na základě zpracování relevantních dat z DNS a DHCP provozu • IP geolokace • IP reputace, včetně údaje, zda je IP adresa na blacklistu 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.	**ANO, nabízené řešení splňuje zadavatelem definované parametry** Nabízené řešení v celé monitorované síti, mezi všemi zařízeními a na všech službách měří a vytváří automaticky (bez nutnosti nastavovat manuálně limitní hodnoty a jiné parametry) model normálního chování pro výkonnostní parametry: 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 zařízeních minimálně na základě parametrů: cílová a zdrojová IP/MAC adresa, podsíť, využitý protokol, IPv4 nebo IPv6.	**ANO, nabízené řešení splňuje zadavatelem definované parametry** Nabízené řešení umožňuje nahrávat plný síťový provoz (full packet capture) na všech dodaných zařízeních na základě parametrů: cílová a zdrojová IP/MAC adresa, podsíť, využitý protokol, IPv4 nebo IPv6.
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.	**ANO, nabízené řešení splňuje zadavatelem definované parametry** Nabízené řešení poskytuje 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.	**ANO, nabízené řešení splňuje zadavatelem definované parametry** Nabízené řešení umožňuje vytváření profilů a skupin uživatelů s cílem omezit funkcionality produktu a viditelnosti uložených dat s podporou: granulárního nastavení přístupu k analytickým i konfiguračním / administrativním komponentám systému s definovanými úrovněmi přístupu (read, write, execute); granulárního nastavení přístupu k datům z různých segmentů sítě zadavatele s definovanými úrovněmi přístupu (read, write, execute); vytváření filtrů veškerých dat a jejich sdílení mezi uživateli a skupinami uživatelů; vytváření vlastních uživatelských pohledů, reportů, dashboardů atd.

Požadavky na procesní zpracování kybernetických událostí

Požadované funkcionality/vlastnosti	**Nabízené řešení splňuje/nesplňuje (doplní účastník)** **Včetně vysvětlení jak je zadání splněno**
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.).	**ANO, nabízené řešení splňuje zadavatelem definované parametry** Nabízené řešení poskytuje integrované rozhraní pro: • reporting bezpečnostních incidentů (označení identifikované události jako 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 atd.).

Požadavky na integraci, reporting a alerting

Požadované funkcionality/vlastnosti	Nabízené řešení splňuje/nesplňuje (doplní účastník) Včetně vysvětlení jak je zadání splněno
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.	**ANO, nabízené řešení splňuje zadavatelem definované parametry** Nabízené řešení umožňuje rychlou a jednoduchou uživatelskou integraci s nástroji třetích stran: s nástrojem typu SIEM prostřednictvím syslog, CEF a LEEF; s nástroji pro generování nebo zpracování síťových statistik ve formátu IPFIX/NetFlow, včetně možnosti filtrovat IPFIX/NetFlow exportované statistiky dle všech filtrovaných parametrů uvedených v předchozím textu; 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.	**ANO, nabízené řešení splňuje zadavatelem definované parametry** Nabízené řešení upozorňuje uživatele prostřednictvím zvoleného typu komunikace, alespoň emailu a logu o všech identifikovaných událostech, o událostech filtrovaných dle IP a MAC adresy, podsítě, závažnosti události, kategorie události, země, uživatele, síťové služby, čísla portu, provozu do/z internetu. Tyto alerty řešení dodává také ve strojově čitelném formátu pro vyžití v nástrojích typu SIEM a obsahuje 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.	**ANO, nabízené řešení splňuje zadavatelem definované parametry** Nabízené řešení vytváří automatizované manažerské reporty o stavu kybernetické bezpečnosti z pohledu správy kybernetických incidentů dle oblastí jejich vznik, např.: doména, web, email apod. Reporty jsou vytvářeny v českém jazyce.

Požadavky na služby bezpečnostního dohledu

Požadované funkcionality/vlastnosti	Nabízené řešení splňuje/nesplňuje (doplní účastník) Včetně vysvětlení jak je zadání splněno

Služby bezpečnostního dohledu na 1 až 6 měsíc • Dohled produktu 8x5 s proaktivním hlášením kritických bezpečnostních událostí a incidentů, v případě incidentů do 24 hodin. • Update software a denní updaty databází Threat Intelligence • Technický helpdesk. • Hardwarová podpora (DELL On-site NBD support). • Pravidelný dohled přesnosti detekce, správného nastavení a používání, včetně pravidelných školení security týmu. • Podpora cyber sercurity analityka (Po-Pá 9:00-17:00). • Měsíční report o stavu sítě z pohledu bezpečností - přehled bezpečnostních incidentů z pohledu identifikace a popisu nálezu, souvisejícího rizika doporučení k jeho eliminaci nebo odstranění.	**ANO, nabízené řešení splňuje zadavatelem definované parametry** Součástí nabízených služeb v prvních 6 měsících je: • Dohled produktu 8x5 s proaktivním hlášením kritických bezpečnostních událostí a incidentů, v případě incidentů do 24 hodin. • Update software a denní updaty databází Threat Intelligence • Technický helpdesk – zadávání tiketů na **ticket.rexonix.cz** • Hardwarová podpora (DELL On-site NBD support). • Pravidelný dohled přesnosti detekce, správného nastavení a používání, včetně pravidelných školení security týmu. • Podpora cyber sercurity analytika (Po-Pá 9:00-17:00). • Měsíční report o stavu sítě z pohledu bezpečností - přehled bezpečnostních incidentů z pohledu identifikace a popisu nálezu, souvisejícího rizika doporučení k jeho eliminaci nebo odstranění.
Služby bezpečnostního dohledu na 7. až 36 měsíc • Čtvrtletní report o stavu sítě z pohledu bezpečností - přehled bezpečnostních incidentů z pohledu identifikace a popisu nálezu, souvisejícího rizika doporučení k jeho eliminaci nebo odstranění. • Update software a denní updaty databází Threat Intelligence • Technický helpdesk • Hardwarová podpora (DELL On-site NBD support) • Pravidelný dohled přesnosti detekce, správného nastavení a používání, včetně pravidelných školení security týmu • Podpora cyber sercurity analityka (Po-Pá 9:00-17:00, měsíční limity)	**ANO, nabízené řešení splňuje zadavatelem definované parametry** Součástí nabízených služeb od 7. do 36. měsíce smlouvy je: • Čtvrtletní report o stavu sítě z pohledu bezpečnosti - přehled bezpečnostních incidentů z pohledu identifikace a popisu nálezu, souvisejícího rizika doporučení k jeho eliminaci nebo odstranění. • Update software a denní updaty databází Threat Intelligence • Technický helpdesk – zadávání tiketů na **ticket.rexonix.cz** • HW podpora (DELL On-site NBD support) • Pravidelný dohled přesnosti detekce, správného nastavení a používání, včetně pravidelných školení security týmu • Podpora cyber sercurity analityka (Po-Pá 9:00-17:00, v rámci měsíčního limitu)

Implementační služby

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.

Produktová podpora výrobce

Dodavatel musí zajistit produktovou podporu řešení v délce 60 měsíců od zahájení poskytování služeb.

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 IS na jednotlivé funkce včetně funkčních prototypů volání jednotlivých funkcí.

Administrátorské školení

V rámci realizace bude Dodavatelem realizováno administrátorské školení pro zaměstnance Zadavatele v rozsahu 1 člověkoden pro max 5 zaměstnanců Zadavatele.

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 zadavatele
- Dochází k záznamu flow a zrcadleného provozu, informace jsou dostupná k zobrazení a dalšímu zpracování
- Výsledná informace (graf nebo tabulka) definovaná libovolně nastaveným základním filtrem s parametrem (např. IP adresa, podsíť, služba, událost, ...) v 24hodinovém intervalu musí být zobrazena do 20s.
- 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, systém má nastavené (samostatně naučené) prahové hodnoty, na základě kterých detekuje anomálie
- Byla vytvořena a dodána provozní dokumentace
- Bylo provedeno školení v požadovaném rozsahu.

Příloha D02 – potvrzení výrobce

GREYCORTEX

GreyCortex s.r.o. potvrzuje, že uchazeč je akreditovaným – autorizovaným poskytovatelem produktu GREYCORTEX Mendel a souvisejících služeb a podpory.

Rexonix s.r.o.

Sídlo:	Pod Višňovkou 1661/35, 140 00 Praha 4
Právní forma:	Společnost s ručením omezeným
IČO:	04493982
DIČ:	CZ04493982
Obchodní rejstřík:	C 248598 vedená u Městského soudu v Praze

[redacted]

Platnost: 1. 3. 2021 – 28. 2. 2022

Příloha D03 – pojistná smlouva (pojistný certifikát)

direct pojišťovna

Potvrzení o pojištění odpovědnosti
Liability Insurance Certificate
Haftpflichtversicherungszertifikat

Pojištěný Insured Versichert	**Rexonix s.r.o.** Pod višňovkou 1661/35, 140 00 Praha 4 - Krč IČ: 044 93 982
Pojistná smlouva č. Policy No. Versicherungsvertag Nr.	900000032036
Ze dne Dated Datum der Verhandlung	02.03.2021
Doba pojištění od Insured period from Beginn der Versicherungszeit	10.03.2021
Doba pojištění do Insured period till Ende der Versicherungszeit	09.03.2022
Limit pojistného plnění základního rozsahu General Limit of Indemnity Grundversicherungslimit	100 000 000 CZK
Územní rozsah Territorial validity Territoriale Gultigkeit	**Česká republika** Czech Republic Tschechien

Direct pojišťovna, a.s. potvrzuje, že s pojištěným uzavřela pojistnou smlouvu s výše uvedenými parametry. Toto potvrzení nenahrazuje pojistnou smlouvu ani její přílohy.

EN	Direct pojišťovna, a.s. confirms concluding insurance contract of parameters named above. This certificate does not effect the contract neither its attachments
DE	Direct pojišťovna, a.s. bestätigt, mit dem Versicherten einen Versicherungsvertrag mit den oben genannten Parametern abgeschlossen zu haben. Diese Bestätigung ersetzt nicht den Versicherungsvertrag oder dessen Anhänge

Datum vystavení Date of issue Ausstellungsdatum	18.03.2021	**Vypracoval** Issued by Erstellt	[redacted]