Spolufinancováno Evropskou unií

MINISTERSTVO PRO MÍSTNÍ ROZVOJ ČR

SMLOUVA NA DODÁVKU SYSTÉMU DETEKCE SÍŤOVÉHO PROVOZU A ZAJIŠTĚNÍ SERVISNÍ PODPORY

č. MSP-34/2024 -MSP-CES

uzavřená podle § 2079 a násl. a § 1746 odst. 2 a násl. zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „**Občanský zákoník**“)

Smluvní strany:

Česká republika – Ministerstvo spravedlnosti
se sídlem: Vyšehradská 16, 128 10 Praha 2
IČO: 00025429
zastoupena: Ing. Bc. Radomír Daňhel, MBA, LL.M. náměstek člena vlády pověřený v oblasti ekonomické a správní
bankovní spojení: Česká národní banka
číslo účtu: [redacted]
(dále jen „**Objednatel**“)

a

NTT Czech Republic s.r.o.
se sídlem: Milevská 2095/5, 140 00 Praha 4
IČO: 26175738
DIČ: CZ26175738
zapsaná v Obchodním rejstříku vedeném Městským soudem v Praze Oddíl: C, vložka: 77064
zastoupena: Ing. Petrem Hüblem, jednatelem společnosti
bankovní spojení: HSBC Bank plc – pobočka Praha
číslo účtu: [redacted]
(dále jako „**Dodavatel**“)

(společně dále jen „**Smluvní strany**“) uzavírají níže uvedeného dne, měsíce a roku tuto Smlouvu na dodávku systému detekce síťového provozu a zajištění servisní podpory (dále jen „**Smlouva**“):

PREAMBULE

Smlouva je uzavírána v souladu se zákonem č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „**Zákon o zadávání veřejných zakázek**“) na základě

výsledku zadávacího řízení k nadlimitní veřejné zakázce s názvem „***Implementace a podpora systému detekce síťového provozu včetně dodávky kolektorů a sond***“ (dále jen „**Veřejná zakázka**“).

Plnění ze Smlouvy je součástí projektu “*Budování kapacit kybernetické bezpečnosti“, registrační číslo projektu: CZ.06.01.01/00/22_005/00002467 a je spolufinancované z Integrovaného regionálního operačního programu 2021-2027“* (dále jen „**Projekt**“).

Článek 1
Účel a předmět Smlouvy

1.1 Účelem Smlouvy je úprava a stanovení podmínek, za jakých Dodavatel dodá a zajistí pro Objednatele plnění specifikované v této Smlouvě, a podmínek, za jakých Objednatel řádně poskytnuté plnění dle této Smlouvy převezme a zaplatí za něj Dodavateli sjednanou cenu. Účelem Smlouvy je dodávka, instalace a implementace komplexního systému detekce síťového provozu včetně servisní podpory dodaných technologií na dobu 60 měsíců.

1.2 Předmětem Smlouvy je závazek Dodavatele

a) dodat Objednateli systém detekce síťového provozu specifikovaný v příloze č. 1 Smlouvy (*Technická specifikace*), včetně dodávky kolektorů, sond, úložišť a řídícího software, jež bude všechny komponenty spravovat, (společně i jednotlivě dále jen „**Zařízení**“ nebo „**Systém**“), přičemž dodávka Zařízení zahrnuje i instalaci a implementaci Zařízení do míst plnění dle článku 2.1 Smlouvy, konfiguraci a nastavení řídícího (analytického) Software Zařízení dle požadavku Objednatele, ověření plné funkčnosti Zařízení a zaškolení určených zaměstnanců Objednatele dle specifikace v příloze č. 1 Smlouvy (*Technická specifikace*) (dále jen „**Dodávka Zařízení**“). Součástí Dodávky Zařízení je i dodání veškerých dokladů, dokumentace skutečného provedení a licencí (oprávnění) k užívání Zařízení, s tím, že licenční oprávnění poskytnou Objednateli a jeho organizačním složkám uvedeným v příloze č. 3 Smlouvy (*Seznam míst plnění*) neomezená oprávnění ke všem činnostem, které jsou potřebné k efektivnímu využití Zařízení v souladu s účelem této Smlouvy.

b) zajistit pro Zařízení servisní podporu (dále jen „**Servisní podpora**“) zahrnující i podporu výrobce Zařízení (dále jen „**Výrobce**“) dle specifikace v příloze č. 5 Smlouvy (*Podmínky Servisní podpory*“) v souladu s Přílohou č. 1 Smlouvy (*Technická specifikace*) na dobu 60 měsíců (dále jen „**Podpora Výrobce**“) od podpisu akceptačního protokolu dle článku 2.3 Smlouvy s výrokem Objednatele „*bez výhrad*“ (dále jen „**Akceptační protokol**“). Vzor Akceptačního protokolu tvoří přílohu č. 4 Smlouvy (*Vzor Akceptačního protokolu*).

Specifikace požadované Servisní podpory, včetně Podpory Výrobce je uvedena v příloze č. 5 Smlouvy (*Podmínky Servisní podpory*)

(Dodávka Zařízení a Servisní podpora společně dále jen „**Předmět plnění**“),

1.3 Předmětem Smlouvy je dále závazek Objednatele uhradit Poskytovateli za řádně dodaný Předmět plnění cenu dle článku 3.1 Smlouvy.

1.4 Poskytovatel je povinen dodat Předmět plnění v souladu s předmětem Smlouvy a se všemi podmínkami a požadavky uvedenými ve Smlouvě a v souladu s platnými právními předpisy.

Článek 2
Místo a doba plnění

2.1 Místem plnění je sídlo Objednatele Vyšehradská 16, Praha 2 a dále místa plnění uvedená v příloze č. 3 Smlouvy (*Seznam míst plnění*).

2.2 Dodavatel se zavazuje zahájit plnění dle článku 1.2 písm. a) Smlouvy bezprostředně po nabytí účinnosti Smlouvy.

2.3 Plnění dle článku 1.2 písm. a) Smlouvy, včetně otestování funkčnosti Zařízení, odstranění veškerých vad Zařízení v rámci testovacího provozu a spuštění Zařízení v ostrém provozu, předání provozní dokumentace, a doklad o zajištění Podpory Výrobce, tzn. potvrzení vystavené Výrobcem či oficiálním zástupcem Výrobce v České republice o podpoře Výrobce či oficiálního zástupce Výrobce v České republice pro Zařízení na dobu 60 měsíců od podpisu Akceptačního protokolu, se Dodavatel zavazuje dodat Objednateli **nejpozději do 5 měsíců od účinnosti Smlouvy**. O této skutečnosti sepíšou oprávnění zástupci Smluvních stran Akceptační protokol.

2.4 Dodavatel se dále zavazuje realizovat školení v souladu s přílohou č. 1 Smlouvy (*Technická specifikace*) **do 3 měsíců** od účinnosti Smlouvy.

2.5 Plnění dle článku 1.2 písm. a) Smlouvy musí splňovat akceptační kritéria stanovená v příloze č. 1 (*Technická specifikace*) a považuje se za provedené podpisem Akceptačního protokolu bez výhrad Objednatele.

2.6 Dodavatel předá Objednateli neprodleně po nabytí účinnosti Smlouvy, nejpozději však do 3 dnů od účinnosti Smlouvy, ke schválení harmonogram instalace jednotlivých částí technologie Zařízení ve specifikovaných lokalitách, resp. v sídle Objednatele a v sídlech organizačních složek resortu justice dle přílohy č. 3 Smlouvy (*Seznam míst plnění*). Součástí harmonogramu bude rovněž seznam členů realizačního týmu Dodavatele, kteří budou instalaci v dané lokalitě provádět s uvedením jejich role a telefonního kontaktu. Na základě takto vypracovaného harmonogramu zajistí Objednatel Dodavateli přístup do místa instalace. Smluvní strany mohou harmonogram za účelem hladkého průběhu plnění

upravovat. Jakákoli změna harmonogramu podléhá vždy písemnému souhlasu ze strany Objednatele.

2.7 Dodavatel se zavazuje poskytovat Servisní podporu **po** dobu 60 měsíců od podpisu Akceptačního protokolu s výrokem Objednatele „*bez výhrad*“.

Článek 3
Cena a platební podmínky

3.1 Objednatel se zavazuje uhradit Dodavateli za Předmět plnění, tj. za řádnou Dodávku Zařízení a Servisní podporu (včetně Podpory Výrobce) na dobu 60 měsíců dle článku 1.2 písm. a) a písm. b) Smlouvy, cenu ve výši:

cena bez DPH	58 035 000,- Kč
sazba DPH:	21 %
výše DPH:	12 187 350,- Kč
Cena včetně DPH	70 222 350,- Kč

(dále jen „**Cena**“).

3.2 Cena je nepřekročitelná, nejvýše přípustná a zahrnuje veškeré náklady Dodavatele spojené s plněním dle této Smlouvy, včetně veškerého materiálu, práce, balení, poplatků, dopravy (doručení na místo dodání), atd.

3.3 Objednatel neposkytuje zálohy a ani jedna Smluvní strana neposkytla ani neposkytne druhé Smluvní straně závdavek.

3.4 Za účelem vyloučení pochybností smluvní strany uvádějí, že v Ceně je zahrnut záruční servis Dodavatele dle Článku 6 po dobu 60 měsíců od podpisu Akceptačního protokolu s výrokem Objednatele „*bez výhrad*“.

3.5 Změna Ceny je přípustná pouze v případě změny zákonem stanovené sazby DPH, na základě písemného dodatku, podepsaného k tomu oprávněnými zástupci obou Smluvních stran. Ke sjednané ceně bez DPH se připočte daň z přidané hodnoty ve výši stanovené právními předpisy platnými ke dni uskutečnění zdanitelného plnění. Za den uskutečnění zdanitelného plnění u Ceny se považuje den podpisu Akceptačního protokolu bez výhrad Objednatele.

3.6 Smluvní strany sjednávají, že Cena dle článku 3.1 Smlouvy bude uhrazena na základě daňového dokladu vystaveného Dodavatelem (faktury), s tím, že Dodavatel je oprávněn vystavit fakturu po provedení řádné Dodávky Zařízení, po předložení potvrzení o Podpoře

Výrobce a po podpisu Akceptačního protokolu podepsaného oběma Smluvními stranami dle článku 2.3 Smlouvy bez výhrad Objednatele.

3.7 Daňový doklad bude obsahovat:

a) náležitosti stanovené § 435 Občanského zákoníku,

b) náležitosti stanovené zákonem č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů,

c) číslo Smlouvy,

d) označení, že se jedná o plnění v rámci projektu "*Budování kapacit kybernetické bezpečnosti", registrační číslo projektu: CZ.06.01.01/00/22_005/00002467, spolufinancované z Integrovaného regionálního operačního programu 2021-2027*,

e) kopie Akceptačního protokolu s výrokem Objednatele „*bez výhrad*".

3.8 Splatnost daňového dokladu je sjednána na 30 dnů ode dne jeho doručení Objednateli.

3.9 Platba bude provedena bankovním převodem a za den úhrady se považuje den odepsání fakturované částky z účtu Objednatele ve prospěch účtu Dodavatele.

3.10 Nebude-li daňový doklad splňovat předepsané nebo sjednané náležitosti, je Objednatel oprávněn jej ve lhůtě splatnosti vrátit Dodavateli. Po doručení opraveného daňového dokladu Objednateli běží nová lhůta splatnosti.

3.11 V případě prodlení Objednatele s platbou faktury má Dodavatel právo požadovat úhradu úroku z prodlení dle zvláštního právního předpisu v platném znění (nařízení vlády č. 351/2013 Sb., ve znění pozdějších předpisů).

3.12 Vlastnické právo k Zařízení přechází na Objednatele akceptací bez výhrad (podpisem Akceptačního protokolu). Okamžikem předání/instalace Zařízení či jeho části přechází na Objednatele právo Zařízení nebo jeho danou část užívat.

Článek 4
Mlčenlivost a ochrana osobních údajů

4.1 Všechny informace, které se Dodavatel dozví v souvislosti s plněním dle Smlouvy, jsou důvěrné povahy. Dodavatel se zavazuje zachovávat o důvěrných informacích mlčenlivost a důvěrné informace používat pouze k plnění Smlouvy.

4.2 Povinnost zachovávat mlčenlivost znamená zejména povinnost zdržet se jakéhokoliv jednání, kterým by důvěrné informace byly sděleny nebo zpřístupněny třetí osobě nebo

by byly využity v rozporu s jejich účelem pro vlastní potřeby nebo pro potřeby třetí osoby, případně by bylo umožněno třetí osobě jakékoliv využití těchto důvěrných informací. Poskytovatel je povinen přijmout opatření k ochraně důvěrných informací a zajistit utajení těchto skutečností a důvěrných informací i u svých zaměstnanců, zástupců, jakož i u jiných spolupracujících třetích stran.

4.3 Povinností mlčenlivosti dle tohoto článku Smlouvy není dotčena povinnost Dodavatele sdělit nebo zpřístupnit důvěrné informace třetí osobě, která vyplývá z platných právních předpisů nebo z rozhodnutí orgánů veřejné moci, jakož i zpřístupnění důvěrných informací svému právnímu, účetními nebo daňovému poradci, kteří jsou vázáni povinností mlčenlivosti.

4.4 Dodavatel si je při plnění Smlouvy vědom povinností vyplývajících z platných právních předpisů upravujících ochranu osobních údajů, zejména ze zákona č. 110/2019 Sb., o zpracování osobních údajů, ve znění posledních předpisů (dále jen „**Zákon o zpracování osobních údajů**“) a z nařízení Evropského parlamentu a Rady (EU) 2016/679 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) (GDPR) (dále jen „**Nařízení**“). Dodavatel je oprávněn zpracovávat osobní údaje v rozsahu nezbytně nutném pro plnění předmětu Smlouvy, za tímto účelem je oprávněn osobní údaje zejména ukládat na nosiče informací, upravovat, uchovávat po dobu nezbytnou k uplatnění práv Dodavatele vyplývajících ze Smlouvy, předávat zpracované osobní údaje Objednateli, osobní údaje likvidovat, vše v souladu s platnými právními předpisy upravujícími ochranu osobních údajů, zejména s Nařízením a se Zákonem o zpracování osobních údajů.

4.5 Dodavatel učiní v souladu s platnými právními předpisy dostatečná organizační a technická opatření zabraňující přístupu neoprávněných osob k osobním údajům Objednatele a k důvěrným informacím, se kterými se seznámil v souvislosti s plněním předmětu Smlouvy.

4.6 Povinnost zachovávat mlčenlivost a ochrany osobních údajů trvá i po skončení tohoto smluvního vztahu.

Článek 5
Smluvní pokuty a úrok z prodlení

5.1 V případě prodlení Dodavatele s provedením Dodávky Zařízení nebo s doložením potvrzení o Podpoře Výrobce na 60 měsíců dle článku 2.3 Smlouvy, je Objednatel oprávněn požadovat po Dodavateli a Dodavatel je povinen uhradit smluvní pokutu ve výši 100.000,- Kč za každý započatý den prodlení.

5.2 V případě prodlení Dodavatele s odstraněním vad Předmětu plnění po termínu pro odstranění vady dle článku 6.12 Smlouvy, je Objednatel oprávněn požadovat po Dodavateli a Dodavatel je povinen uhradit smluvní pokutu ve výši 5.000,- Kč za každý započatý den prodlení.

5.3 V případě prodlení Dodavatele s poskytováním Servisní podpory, zejména s dodržením doby pro vyřešení závady HW nebo doby pro řešení SW problému uvedených v příloze č. 5 (*Podmínky Servisní podpory*), je Objednatel oprávněn požadovat po Dodavateli a Dodavatel je povinen uhradit smluvní pokutu ve výši 50.000,- Kč za každý započatý den prodlení.

5.4 V případě porušení závazku mlčenlivosti, ochrany důvěrných informací nebo ochrany osobních údajů dle článku 4 Smlouvy, je Objednatel oprávněn požadovat po Dodavateli a Dodavatel je povinen uhradit smluvní pokutu ve výši 100 000,- Kč za každý jednotlivý případ porušení.

5.5 Objednatel je oprávněn požadovat po Dodavateli smluvní pokutu za porušení kterékoli povinnosti stanovené v článcích 9.3 až 9.6 Smlouvy (souvisejících s realizačním týmem), ve výši 10 000,- Kč za každý jednotlivý případ porušení.

5.6 Opustí-li paměťové médium prostory Objednatele nebo organizační složky z důvodů na straně Dodavatele, zaplatí Dodavatel Objednateli smluvní pokutu ve výši 10 000,- Kč za každý jednotlivý případ.

5.7 V případě prodlení se splněním povinnosti Dodavatele dle článku 8.2 (doložení potvrzení o pojištění), je Dodavatel povinen uhradit Objednateli smluvní pokutu ve výši 3.000,-Kč za každý den prodlení se splněním této povinnosti.

5.8 Ujednáním o smluvních pokutách dle Smlouvy není dotčeno právo na náhradu majetkové i nemajetkové újmy (dále jen „**Újma**“) způsobené porušením povinnosti, pro kterou jsou smluvní pokuty sjednány, ani právo odstoupit od Smlouvy. Zaplacení smluvní pokuty nezbavuje Dodavatele povinnosti řádně dodat Předmět plnění dle Smlouvy ani povinnosti odstranit vady Předmětu plnění.

5.9 Splatnost smluvních pokut je 10 dnů ode dne doručení písemné výzvy k jejich úhradě druhé Smluvní straně.

5.10 Objednatel je oprávněn započíst pohledávku na úhradu smluvní pokuty vůči pohledávce Dodavatele na úhradu Ceny dle článku 3.1 Smlouvy, s čímž Dodavatel výslovně souhlasí.

Článek 6
Záruka, odpovědnost za vady

6.1 Dodavatel poskytuje na Předmět plnění, tj. na Dodávku Zařízení záruku za jakost **na dobu 60 měsíců**. Dohodnutá záruční doba běží ode dne podpisu Akceptačního protokolu s výrokem Objednatele „*bez výhrad*“ oběma smluvními stranami. Dodavatel se zaručuje, že Zařízení budou v záruční době plně způsobilá pro použití k účelu stanovenému v této Smlouvě a v zadávací dokumentaci k Veřejné zakázce, a není-li účel v této Smlouvě nebo v zadávací dokumentaci k Veřejné zakázce stanoven, k účelu obvyklému a dále, že si všechna Zařízení z Dodávky Zařízení zachovají vlastnosti stanovené touto Smlouvou, zadávací dokumentací k Veřejné zakázce a ustanoveními § 2095 a 2096 Občanského zákoníku (záruka za jakost). Zárukou za jakost nejsou dotčena práva a povinnosti z vadného plnění plynoucí ze zákona.

6.2 Nemá-li Předmět plnění vlastnosti stanovené touto Smlouvou, zadávací dokumentací k Veřejné zakázce a ustanoveními § 2095, 2096 a 2097 Občanského zákoníku, má vady. Za vady se považuje i dodání jiného plnění, než určuje tato Smlouva, resp. zadávací dokumentace k Veřejné zakázce. Vadou Předmětu plnění jsou kromě HW a SW rovněž vady v dokladech a licencích nutných k užívání Zařízení a prvotní konfiguraci Zařízení.

6.3 Uplatní-li Objednatel během záruční doby písemně vady, má se zato, že uplatňuje jejich bezplatné odstranění. Oznámením vady se staví běh záruční doby, a to tak, že o dobu od oznámení vady do termínu odstranění vady se sjednaná záruční doba prodlužuje.

6.4 Dodavatel se zavazuje, že po dobu záruky za jakost zajistí, aby byl Předmět plnění plně funkční a bude poskytovat servisní zásahy (odstranění vad) prostřednictvím kompetentních členů realizačního týmu, kteří splňují náležitosti dle článku 9.3 Smlouvy (dále jen „**Záruční servis**“). Dodavatel je povinen odstraňovat vady v rámci Záručního servisu ve lhůtách stanovených pro odstraňování závad HW a řešení SW problému v příloze č. 5 (*Podmínky Servisní podpory*)

6.5 Hlášení vad bude Dodavatelem umožněno Objednateli v pracovních dnech v době od 8:00 do 17:00 hodin. Pracovním dnem se rozumí dny pondělí až pátek kromě dnů pracovního klidu (tj. sobot a nedělí) a státem uznaných svátků (jak jsou tyto stanoveny zákonem č. 245/2000 Sb., o státních svátcích, o významných dnech a o dnech pracovního klidu, ve znění pozdějších předpisů).

6.6 Hlášení vad bude obsahovat tyto údaje:

- identifikace Zařízení a jeho umístění
- popis vady
- identifikace zaměstnance Objednatele (jméno, příjmení, pracovní pozici), který vadu hlásí (dále jen „**Ohlašovatel vady**“)
- kontaktní údaje Ohlašovatele vady (telefon a e-mail)

(dále jen „**Hlášení vady**”).

6.7 Hlášení vady může být provedeno kterýmkoliv z následujících způsobů (všechny dále uvedené způsoby mají stejnou váhu:

- e-mailem na e-mailovou adresu Dodavatele: [redacted],
- telefonicky na telefonické lince (dispečinku) Dodavatele – telefonní číslo: [redacted],
- pomocí automatizovaného systému pro řízení požadavků (servicedesk system) Dodavatele: [redacted]

6.8 Dodavatel je povinen potvrdit přijetí Hlášení vady nejpozději v těchto dobách:

- pokud bude Hlášení vady učiněno do 13:00 hodiny pracovního dne, potvrdí Dodavatel přijetí Hlášení vady do 4 hodin od přijetí Hlášení vady;
- pokud bude Hlášení vady učiněno po 13:00 hodině pracovního dne, Dodavatel potvrdí přijetí Hlášení vady do 8:00 hodiny následujícího pracovního dne.

6.9 Potvrzení přijetí Hlášení vady musí být vždy provedeno jedním z následujících způsobů:

- na e-mail Ohlašovatele vady uvedený v Hlášení vady a na e-mail kontaktní osoby Objednatele dle čl. 9.1 Smlouvy nebo
- automatizovaně prostřednictvím systému pro řízení požadavků (servicedesk systému) Dodavatele na e-mail Ohlašovatele vady uvedený v Hlášení vady a na e-mail kontaktní osoby Objednatele dle čl. 9.1 Smlouvy.

6.10 V případě, že Dodavatel nepotvrdí přijetí Hlášení vady dle čl. 6.8 a 6.9 Smlouvy, má za to, že potvrzení přijetí Hlášení vady provedl ve lhůtě dle čl. 6.8 Smlouvy a způsobem dle čl. 6.9 Smlouvy.

6.11 Odpovědný člen realizačního týmu Dodavatele je povinen nastoupit k odstranění vad nejpozději následující pracovní den po dni:

- kdy Dodavatel potvrdil Hlášení vady nebo
- kdy přijetí Hlášení vady měl Dodavatel nejpozději potvrdit.

6.12 Vady musí být odstraněny nejpozději do 24:00 hodiny (půlnoci) v den nástupu technika k odstranění vad, a to některým z těchto způsobů:

- opravou,
- dodáním nového Zařízení nebo nové součásti Zařízení nebo jiné části Předmětu plnění bez vady,
- dodáním chybějící části Předmětu plnění.

Tím nejsou dotčena ostatní práva Objednatele z vadného plnění plynoucí ze zákona.

6.13 Dodavatel prohlašuje, že na Předmětu plnění neváznou práva třetích osob, ze kterých by pro Objednatele vyplynuly jakékoliv další finanční nebo jiné nároky ve prospěch třetích stran. V opačném případě Dodavatel ponese veškeré důsledky takového porušení práv třetích osob.

6.14 Dodavatel nese veškeré náklady spojené s odstraňováním vad, a to včetně nákladů spojených s přepravou.

6.15 Veškeré výměny HW komponentů a řešení veškerých vad v rámci záruky musí být prováděno přímo kompetentními členy realizačního týmu dodavatele dle článku 9 Smlouvy a dle přílohy č. 2 (*Realizační tým*).

6.16 V případě, že vada se týká komponenty obsahující paměťové médium (pevný disk, paměťovou kartu, CD/DVD apod.), na kterém můžou být uložena data organizačních složek/Objednatele nebo záznamy z jednání organizační složky/Objednatele, nebo je vada detekována přímo na takovémto paměťovém médiu, zůstává tato paměťová média vždy bezúplatně Organizační složce/Objednateli; paměťové médium **nesmí** opustit prostory Organizační složky/Objednatele. Veškerá paměťová média (i při výměně HW) budou vždy protokolárně předána oprávněnému zástupci dané organizační složky nebo Objednatele (v místě instalace).

6.17 Při plnění dle Smlouvy prostřednictvím poddodavatele má Dodavatel odpovědnost, jako by plnil sám.

Článek 7
Ukončení Smlouvy

7.1 Smlouvu lze ukončit písemnou dohodou smluvních stran, odstoupením od Smlouvy nebo písemnou výpovědí.

7.2 Smluvní strany jsou oprávněny písemně odstoupit od Smlouvy v případě, kdy druhá Smluvní strana poruší podstatným způsobem své povinnosti stanovené zákonem či

Smlouvou. Odstoupení od Smlouvy ze strany Objednatele nesmí být spojeno s uložením jakékoliv sankce k jeho tíži.

7.3 Za porušení Smlouvy podstatným způsobem se považuje:

a) prodlení Dodavatele s dodáním Předmětu plnění dle článku 1.2 písm. a) Smlouvy delší než 14 kalendářních dní,

b) poruší-li Dodavatel povinnost mlčenlivosti dle Smlouvy,

c) prodlení Dodavatele s odstraněním vad Předmětu plnění dle čl. 6 Smlouvy o více jak 30 kalendářních dnů,

d) opakované porušení povinností Dodavatele vyplývajících ze Smlouvy (více než 3x).

7.4 Objednatel je oprávněn odstoupit od Smlouvy v případě, že

a) v insolvenčním řízení bude zjištěn úpadek Dodavatele (v souladu se zněním zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení (insolvenční zákon), ve znění pozdějších předpisů),

b) Dodavatel vstoupí do likvidace,

c) Dodavatel či jeho poddodavatel je nebo se v průběhu účinnosti Smlouvy stane osobou, na kterou se vztahuje zákaz zadání veřejné zakázky dle § 48a Zákona o zadávání veřejných zakázek, nebo

d) prokáže-li se, že zájmy osob ve smyslu § 44 odst. 2 písm. a) a b) Zákona o zadávání veřejných zakázek získat osobní výhodu nebo snížit majetkový nebo jiný prospěch Objednatele, ohrožují jejich nestrannost nebo nezávislost v souvislosti se zadávacím řízením.

7.5 Dojde-li

a) k přeměně společnosti Dodavatele nebo

b) ke změně vlastnické struktury společnosti Dodavatele nebo ke změně podílu na hlasovacích právech ve společnosti Dodavatele, v jejichž důsledku se změní ovládající osoba oproti dni uzavření Smlouvy,

je Dodavatel povinen písemně oznámit tuto skutečnost Objednateli ve lhůtě 10 kalendářních dnů od účinnosti této změny. Objednatel je v tomto případě oprávněn písemně vypovědět Smlouvu. Výpovědní doba činí 10 kalendářních dnů a počíná běžet dnem následujícím po jejím doručení Dodavateli.

7.6 Za den odstoupení od Smlouvy se považuje den, kdy bylo písemné oznámení o odstoupení oprávněné strany doručeno druhé Smluvní straně. Od Smlouvy je možné odstoupit pouze s účinky ex nunc (do budoucna).

7.7 Odstoupení od Smlouvy se nedotýká práva na zaplacení smluvní pokuty ani práva na náhradu Újmy vzniklé z porušení smluvní povinnosti.

7.8 Dojde-li k předčasnému ukončení Smlouvy, zavazují se Smluvní strany vypořádat své vzájemné nároky související s plněním dle Smlouvy.

Článek 8
Další ujednání

8.1 Dodavatel se zavazuje udržovat v platnosti po celou dobu trvání Smlouvy pojistnou smlouvu, jejímž předmětem je pojištění odpovědnosti za škodu způsobenou v souvislosti s výkonem činností, které jsou předmětem Smlouvy, s limitem pojistného plnění nejméně ve výši 50.000.000,-Kč, a to ze všech pojistných událostí vzniklých v 1 pojišťovacím roce v souvislosti se Smlouvou. Ve vztahu k pojištění dle tohoto ustanovení Smlouvy Dodavatel zajistí, že v případě vzniku pojistné události bude pojistné plnění placeno přímo Objednateli.

8.2 Dodavatel je povinen do 15 dnů od účinnosti Smlouvy a dále pak kdykoli v průběhu trvání Smlouvy nejpozději do 14 dnů ode dne doručení žádosti Objednatele předložit Objednateli platnou a účinnou pojistnou smlouvu dle odst. 8.1 tohoto článku, nebo pojistku ve smyslu § 2775 Občanského zákoníku či jiný pojistný certifikát.

8.3 Objednatel je oprávněn uveřejnit na svých webových stránkách a v registru smluv celý text Smlouvy, a to za předpokladu nebrání-li uveřejnění zvláštní právní předpis.

8.4 Dodavatel bere na vědomí skutečnost, že podle § 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, je osobou povinnou spolupůsobit při výkonu finanční kontroly prováděné v souvislosti s úhradou zboží nebo služeb z veřejných výdajů.

8.5 Dodavatel je povinen řádně uchovávat veškerou dokumentaci související s plněním Smlouvy a s realizací Projektu včetně účetních dokladů podle českých právních předpisů, minimálně však do 31.12.2035, a po tuto dobu poskytovat požadované informace a dokumentaci související s realizací Projektu zaměstnancům nebo zmocněncům pověřených orgánů (zejména Centra pro regionální rozvoj, Ministerstva vnitra ČR, Ministerstva financí ČR, Ministerstva průmyslu a obchodu ČR, Evropské komise, Evropského účetního dvora, Nejvyššího kontrolního úřadu, příslušného orgánu finanční správy a dalších oprávněných orgánů státní správy), vytvořit jim podmínky k provedení

kontroly vztahující se k realizaci Projektu a poskytnout jim při provádění kontroly součinnost. Předmětem případné kontroly může být zejména ověření toho, že plnění a skutečné vynaložení výdajů na realizaci Veřejné zakázky nejsou v rozporu.

8.6 Dodavatel prohlašuje, že:

a) je Výrobcem autorizován k Dodávce Zařízení a jeho součástí, instalaci, konfiguraci, zaškolení personálu, veškerému servisu a dalším činnostem v rozsahu dle této Smlouvy;

b) je držitelem oprávnění k podnikání v rozsahu odpovídajícímu účelu a předmětu této Smlouvy;

c) disponuje potřebnými odbornými znalostmi a praktickými zkušenostmi k řádnému splnění účelu a předmětu této Smlouvy, je odborníkem ve smyslu § 5 a § 2950 Občanského zákoníku.

8.7 Dodavatel je povinen na vyžádání Objednatele doložit doklady prokazující skutečnosti uvedené v čl. 8.6 písm. a) a b) Smlouvy.

8.8 Dodavatel prohlašuje, že Předmět plnění dle Smlouvy nebude zatížen právy třetích osob, ze kterých by pro Objednatele vyplynuly jakékoliv další finanční nebo jiné nároky ve prospěch třetích stran. V opačném případě Dodavatel ponese veškeré důsledky takového porušení práv třetích osob.

8.9 Dodavatel je povinen nahradit veškerou Újmu, kterou způsobil porušením ustanovení této Smlouvy nebo které vznikly v souvislosti s vadou Zařízení. Dodavatel bere na vědomí, že pokud neuvědomí Objednatele o jakékoli hrozící či vzniklé Újmě a neumožní tak Objednateli, aby učinil kroky k zabránění vzniku Újmy či k jejímu zmírnění, má Objednatel proti Dodavateli nárok na náhradu majetkové i nemajetkové Újmy, která tím Objednateli vznikla.

8.10 Dodavatel výslovně prohlašuje, že na sebe přebírá nebezpečí změny okolností ve smyslu ustanovení § 1765 odst. 2 Občanského zákoníku.

8.11 Komunikace mezi Dodavatelem a Objednatelem bude probíhat v českém jazyce.

Článek 9
Kontaktní osoby, realizační tým a poddodavatelé

9.1 Pro realizaci Smlouvy a vzájemnou komunikaci Smluvní strany určují tyto kontaktní osoby:

a. Objednatel:

i. [redacted], tel. [redacted], e-mail: [redacted] – je kontaktní osobou pro plnění Smlouvy z hlediska věcného, oprávněnou podepsat Akceptační protokol.

ii. [redacted] tel. [redacted], e-mail: [redacted], [redacted], e-mail: [redacted] – je kontaktní osobou ve všech ostatních záležitostech, které nespadají do působnosti kontaktní osoby pro věcné plnění podle předchozího bodu;

b. Dodavatel:

i. [redacted], tel. [redacted], e-mail: [redacted] – je kontaktní osobou pro plnění Smlouvy z hlediska věcného, oprávněnou podepsat Akceptační protokol.

ii. [redacted], tel. [redacted], e-mail: [redacted], tel. [redacted] e-mail: [redacted] – je kontaktní osobou ve všech ostatních záležitostech, které nespadají do působnosti kontaktní osoby pro věcné plnění podle předchozího bodu.

9.2 Případnou změnu kontaktních osob oznámí Smluvní strana bez zbytečného odkladu písemně druhé Smluvní straně. V tomto případě se nepoužije ustanovení čl. 10.3 Smlouvy.

9.3 Dodavatel bude provádět plnění dle Smlouvy a poskytovat služby Servisní podpory prostřednictvím členů realizačního týmu uvedených v příloze č. 2 Smlouvy (*Realizační tým*) tak, aby jednotliví členové realizačního týmu prováděli činnosti na pozicích dle jejich odbornosti (role) uvedené v příloze č. 2 Smlouvy (*Realizační tým*) a v rozsahu, který těmto rolím běžně odpovídá.

9.4 Členy realizačního týmu, jejichž prostřednictvím Dodavatel prokazoval kvalifikaci ve Veřejné zakázce, musí Dodavatel využívat při plnění Smlouvy po celou dobu jejího trvání v rozsahu, v jakém jimi prokazoval kvalifikaci, ledaže dojde ke změně člena realizačního týmu.

9.5 Využití nového člena realizačního týmu, změnu člena realizačního týmu nebo rozsahu jeho využití musí předem odsouhlasit Objednatel. Členy realizačního týmu, jimiž Dodavatel prokazoval kvalifikaci ve Veřejné zakázce, lze vyměnit, pouze pokud budou nahrazeni osobami splňujícími kvalifikaci požadovanou ve Veřejné zakázce ve stejném rozsahu jako nahrazovaní členové.

9.6 Poskytovatel musí bezodkladně, nejpozději však do 5 pracovních dnů, nahradit člena realizačního týmu na odůvodněnou žádost Objednatele v případě, že člen realizačního

týmu neplní své povinnosti podle Smlouvy nebo svou činností způsobil Objednateli Újmu.

9.7 Při změně realizačního týmu není nutné uzavírat písemný dodatek ke Smlouvě a Dodavatel po změně realizačního týmu (odsouhlasení změny Objednatelem) vypracuje a předá Objednateli v podobě elektronického dokumentu aktualizované znění přílohy č. 2 Smlouvy (*Realizační tým*), čímž dojde automaticky k jejímu nahrazení novým zněním.

9.8 Poskytovatel k plnění části předmětu Smlouvy smí využít třetí osobu realizující subdodávky pro Dodavatele v souvislosti s touto Smlouvou. V takovém případě je Dodavatel povinen předložit Objednateli k odsouhlasení seznam poddodavatelů, které bude Dodavatel využívat k realizaci Předmětu plnění, včetně informací o části Předmětu plnění, pro který budou příslušní poddodavatelé využíváni. Realizací subdodávek se rozumí i poskytnutí oprávnění (např. licence) Objednateli ze strany třetích osob.

9.9 Dodavatel v plném rozsahu odpovídá za zapojení a činnost poddodavatelů. Ohledně práv a povinností poddodavatelů, jejich zaměstnanců, členů a členů statutárního orgánu se dále obdobně použijí ustanovení této Smlouvy o právech a povinnostech Dodavatele a členů realizačního týmu podle tohoto článku 9.

9.10 Využití nového poddodavatele, změna poddodavatele či rozsahu jeho využití musí předem písemně odsouhlasit Objednatel. V těchto případech není nutné uzavírat dodatek ke Smlouvě.

9.11 Poddodavatelé, jejichž prostřednictvím Dodavatel prokazoval kvalifikaci ve Veřejné zakázce, je Dodavatel povinen využívat při plnění Smlouvy po celou dobu jejího trvání v rozsahu, v jakém jimi prokazoval kvalifikaci. Poddodavatele, jimiž Poskytovatel prokazoval kvalifikaci ve Veřejné zakázce, lze vyměnit, pouze pokud budou nahrazeni osobami splňujícími kvalifikaci požadovanou ve Veřejné zakázce ve stejném rozsahu jako nahrazovaní poddodavatelé.

9.12 Objednatel je oprávněn uzavřít jakékoliv smlouvy s příslušnými poddodavateli týkající se předmětu Smlouvy. Dodavatel se zavazuje, že ve smlouvách uzavřených s poddodavateli nevyloučí či neomezí oprávnění poddodavatelů vstoupit do smluvních vztahů s Objednatelem, a to také včetně jakéhokoli omezení případného jednání poddodavatelů s Objednatelem či třetími osobami o poskytnutí takových služeb v době trvání smluvního závazkového vztahu založeného Smlouvou.

Článek 10
Obecná a závěrečná ustanovení

10.1 Smlouva je podepsána vlastnoručně nebo elektronicky. Je-li Smlouva podepsána vlastnoručně, je vyhotovena ve čtyřech (4) stejnopisech v českém jazyce, z nichž každá

Strana obdrží po dvou (2) vyhotoveních. Je-li Smlouva podepsána elektronicky, je podepsána pomocí kvalifikovaného elektronického podpisu.

10.2 Smluvní strany prohlašují, že Smlouva obsahuje veškerý projev jejich shodné vůle a mimo ni neexistují žádná ujednání v jiné než písemné formě, která by ji doplňovala, měnila nebo mohla mít význam při jejím výkladu, a že se tedy žádná ze Smluvních stran nespoléhá na prohlášení druhé Smluvní strany, které není uvedeno ve Smlouvě, jejích přílohách či dodatcích. Tím není dotčen význam následné komunikace Smluvních stran.

10.3 Veškeré změny a doplňky Smlouvy musí být učiněny písemně ve formě číslovaného dodatku ke Smlouvě, podepsaného k tomu oprávněnými zástupci obou Smluvních stran.

10.4 Smluvní strany se zavazují vyvinout maximální úsilí k odstranění vzájemných sporů vzniklých na základě Smlouvy nebo v souvislosti se Smlouvou, včetně jejího výkladu a vynaloží úsilí k jejich vyřešení, zejména prostřednictvím jednání kontaktních osob nebo pověřených zástupců.

10.5 Smlouva a vztahy z ní vyplývající se řídí právním řádem České republiky.

10.6 Při rozhodování případných sporů, vzniklých ze závazkových vztahů založených Smlouvou, budou místně a věcně příslušné soudy České republiky.

10.7 Smluvní strany v souladu s ustanovením § 558 odst. 2 Občanského zákoníku vylučují použití obchodních zvyklostí na právní vztahy vzniklé ze Smlouvy.

10.8 Smluvní strany souhlasně prohlašují, že Smlouva není smlouvou uzavřenou adhezním způsobem ve smyslu ustanovení § 1798 a násl. Občanského zákoníku.

10.9 Dodavatel je povinen postupovat při plnění dle Smlouvy podle pravidel kybernetické bezpečnosti uvedených zejména v zákoně č. 181/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů, ve vyhlášce č. 82/2018 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů a v Instrukci Ministerstva spravedlnosti č. 5/2022 (č. j. 115/2022-OI-SP/1) o zajištění bezpečnosti informací v prostředí informačních a komunikačních technologií resortu spravedlnosti.

10.10 Objednatel se zavazuje poskytnout Dodavateli ke splnění Předmětu smlouvy nezbytnou součinnost.

10.11 Stane-li se některé ustanovení Smlouvy neplatným, zdánlivým či neúčinným, nemá tato skutečnost vliv na ostatní ustanovení Smlouvy, která zůstávají platná a účinná. Smluvní strany se v tomto případě zavazují písemnou dohodou nahradit ustanovení, které bylo shledáno neplatným, zdánlivým či neúčinným novým ustanovením, které po obsahové stránce nejlépe odpovídá zamýšlenému účelu původního ustanovení. Do té doby platí odpovídající úprava obecně závazných právních předpisů České republiky.

10.12 Vyskytnou-li se události, které jedné nebo oběma Smluvním stranám částečně nebo úplně znemožní plnění jejich povinností podle Smlouvy, jsou povinny se o tomto bez zbytečného odkladu informovat a společně podniknout kroky k jejich překonání. Nesplnění této povinnosti zakládá právo na náhradu Újmy pro stranu, která se porušení Smlouvy v tomto bodě nedopustila.

10.13 Smlouva nabývá platnosti dnem podpisu oběma Smluvními stranami a účinnosti dnem uveřejnění Smlouvy v registru smluv. Uveřejnění Smlouvy v registru smluv zajistí Objednatel.

10.14 Smluvní strany prohlašují, že Smlouva byla sjednána na základě jejich pravé, vážné a svobodné vůle, že si její obsah přečetly, bezvýhradně s ním souhlasí, považují jej za zcela určitý a srozumitelný, což níže stvrzují svými vlastnoručními podpisy.

10.15 Nedílnou součást Smlouvy tvoří tyto přílohy:

Příloha č. 1: Technická specifikace

Příloha č. 2: Realizační tým

Příloha č. 3: Seznam míst plnění

Příloha č. 4: Vzor Akceptačního protokolu

Příloha č. 5: Podmínky Servisní podpory

V Praze dne ……

Za Dodavatele:

[redacted]

……

NTT Czech Republic s.r.o.
Ing. Petr Hübl, jednatel společnosti

[redacted]

V Praze dne ……

Za Objednatele:

[redacted]

……

Česká republika – Ministerstvo spravedlnosti
Ing. Bc. Radomír Daňhel, MBA, LL.M.
náměstek člena vlády pověřený v oblasti ekonomické a správní

TECHNICKÁ SPECIFIKACE

Technická specifikace

Systém pro analýzu/detekci síťového provozu, který okamžitě identifikuje bezpečnostní rizika a události a který splňuje klíčové požadavky uvedené níže.

Nabízená technologie musí být 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 Objednatel (dále také „zadavatel“) přímo kontaktovat.

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

Obecné požadavky

Systém pro analýzu síťového provozu	Krátký komentář, doplňující údaje (parametr, popis), jak nabízené řešení splňuje požadavek.
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.	**Nabízené řešení postavené na kombinaci příslušné SW licence a HW monitoruje síťovou aktivitu v reálném čase, identifikuje hrozby, bezpečnostní rizika i anomální chování a vytváří upozornění o těchto událostech v reálném čase. Upozornění je odesláno okamžitě dle nastavení správce.**
Dodaný systém musí analyzovat síť na základě zrcadleného síťového provozu ze SPAN portů nebo TAPů (nikoliv jen na základě statistických protokolů typu NetFlow) a zároveň bez potřeby nasazovat agenty na koncové stanice nebo další zařízení v síti.	**Nabízené řešení analyzuje síť na základě zrcadleného síťového provozu ze SPAN portů nebo TAPů a nevyžaduje instalaci agentů na jakákoliv další zařízení v síti. V případě potřeby zadavatele dokáže analyzovat také statistické protokoly.**
Systém musí analyzovat obsah datových paketů v reálném čase a detekovat protokol nebo aplikaci na základě obsahu provozu prostřednictvím DPI (Deep Packet Inspection), nikoli pouze čísla portu.	**Nabízené řešení analyzuje obsah datových paketů v reálném čase a prostřednictvím Deep Packet Inspection**
Dodaný systém musí být schopen analyzovat síť také na základě zpracování statistických protokolů typu NetFlow, IPFIX, NetStream, Cisco NSEL a případně dalších.	**Nabízené řešení umožňuje analyzovat síť také na základě zpracování protokolů typu NetFlow, IPFIX, NetStream, Cisco NSEL a dalších dle potřeby zadavatele.**
Systém musí být plně funkční v offline prostředí objednatele bez využití cloudového prostředí pro sběr, ukládání a zpracování dat a veškeré konfigurace a reporting jsou k dispozici přímo v systému.	**Nabízené řešení lze provozovat zcela v offline prostředí zadavatele, konfiguraci může provést obsluha přímo v systému, stejně jako vytváření požadovaných reportů.**

	Sběr, ukládání a zpracování dat může probíhat lokálně v offline režimu.
Aktualizace systému musí být možné provádět uživatelsky v offline režimu.	**Aktualizaci nabízeného řešení je možné provádět v offline režimu dvěma způsoby - získáním dat z přenosného USB média nebo prostřednictvím interní transparentní proxy s funkcí diody. Takto jsou aktualizovány SW upgrady i znalostní aktualizace hrozeb. Vše lze uživatelsky nastavit v GUI.**
Zpracování a 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.	**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. Data jsou uložena v softwarově akcelerovaných databázích pro okamžitý přístup k datům. U všech toků jsou obsaženy volumetrické, statické a dynamické vlastnosti toku, a dále dle protokolu obsah aplikačních metadat nebo plný obsah protokolu. Nabízené řešení detailně (aplikační detail) zpracovává asi 70 protokolů, šifrovaných i nešifrovaných a uchovává až 2000 parametrů pro jeden síťový tok. Dále uživatel může nechat zaznamenávat definovanou velikost aplikačního obsahu nebo i celý aplikační obsah u každého toku.**
Požadované protokoly pro ukládání aplikačních metadat z jednotlivých transakcí jsou: 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, NFS, ARP, SSL/TLS zapouzdření.	**Nabízené řešení 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**
Je požadováno vysokorychlostní úložiště pro uchování historie datových toků na dobu minimálně 12 měsíců složené z SSD nebo NVMe disků.	**Nabízené řešení zahrnuje vysokorychlostní úložiště pro uchování datových toků po dobu minimálně 12 měsíců, složené z SSD disků. Každé jednotlivé zařízení je vybaveno odpovídající velikostí**

	úložiště s retencí 12 měsíců podle průměrného průtoku v daném segmentu sítě.
Analýza aplikačních a systémových logů Systém musí být schopen sbírat a analyzovat aplikační a systémové logy ve formátu syslog z dohledovaných zařízení a identifikovat nebezpečné nebo potenciálně škodlivé aktivity.	**Nabízené řešení z dohledovaných zařízení sbírá a analyzuje aplikační a systémové logy ve formátu syslog, detekuje nebezpečné a potenciálně škodlivé aktivity využitím všech aplikovaných metod identifikace uvedených dále ve specifikaci.**
Uživatelské 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.	**Nabízené řešení poskytuje jednotné grafické rozhraní pro uživatele a veškerou jejich práci se systémem; uživatel si může nastavit rozhraní se světlou nebo tmavou grafikou dle svých preferencí.**
Systém musí být schopen vytváření profilů a skupin uživatelů pro omezení funkcionality produktu a viditelnosti uložených dat s podporou minimálně:	**Administrátor nabízeného řešení má možnost vytvářet profily jednotlivých uživatelů a jejich skupin s definovanými oprávněními k funkcionalitám řešení a omezeným přístupem k datům. Administrátor nastavuje:**
● granulárního nastavení přístupu k analytickým i konfiguračním/administrativním komponentám Systému s definovanými úrovněmi přístupu (alespoň read, write, execute),	**- přístupy a omezení k analytickým a konfiguračním komponentám s požadovanou úrovní přístupu R/W/Execute**
● granulárního nastavení přístupu k datům z různých segmentů sítě organizace s definovanými úrovněmi přístupu (alespoň read, write, execute),	**- granulární přístupy k datům z jednotlivých segmentů sítě s požadovanými úrovněmi R/W/E**
● vytváření vlastních filtrů veškerých dat a jejich sdílení mezi uživateli a skupinami uživatelů,	**- filtry dat a jejich sdílení mezi jednotlivými uživateli a/nebo jejich skupinami**
● vytváření vlastních uživatelských pohledů, reportů, dashboardů apod.	**Uživatelé mohou vytvářet vlastní dashboardy, filtry a reporty v rámci svých oprávnění.**
Automatické hlášení (alerty) a reporting	
Systém musí být schopen upozorňovat uživatele prostřednictvím minimálně emailu a logu o všech identifikovaných událostech a dále o událostech filtrovaných minimálně dle IP a MAC adresy, podsítě, závažnosti události, kategorie události, země, uživatele, síťové služby, čísla portu, provozu do/z internetu.	**Nabízené řešení upozorňuje uživatele prostřednictvím přednastaveného typu komunikace, např. mailem na zvolené adresy a logy o všech identifikovaných událostech i o událostech filtrovaných dle IP a MAC adresy, podsítě, závažnosti a kategorie události, země, uživatele, síťové**

	služby, čísla portu, provozu z a do 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 Systému.	**Nabízené řešení dodává tyto aletry i ve strojově čitelném formátu pro využití v produktech třetích stran, například SIEM, obsahuje kompletní informace o detekované události včetně URL odkazu na událost v reportovaném období do grafického rozhraní.**
Systém musí mít možnost vytváření automatizovaných manažerských reportů o stavu kybernetické bezpečnosti z pohledu zprávy kybernetických incidentů ideálně dle oblastí jejich vzniků (např.: doména, web, email apod.).	**Nabízené řešení umožňuje vytvářet automatizované manažerské reporty o stavu kybernetické bezpečnosti z pohledu správy kybernetických incidentů dle oblasti jejich vzniku (doména, web, e-mail apod.)**
Je požadováno vytváření automatizovaných reportů v českém jazyce.	**Reporty lze vytvářet v českém jazyce.**
Integrace Systému	
Systém musí poskytovat hotové nástroje umožňující integraci se softwarem třetích stran bez použití API Systému, a to minimálně:	**Nabízené řešení disponuje hotovými nástroji pro integraci se SW třetích stran bez použití API, včetně:**
● syslog, CEF a LEEF pro export událostí včetně plné podpory filtrů (exportování pouze požadovaných dat)	**Syslog, CEF a LEEF pro export událostí včetně podpory filtrů**
● přímé url odkazy na libovolnou obrazovku grafického uživatelského rozhraní a filtrovaná zobrazení v grafickém uživatelském rozhraní	**Přímé URL odkazy na jakoukoliv obrazovku GUI a filtrovaná zobrazení v GUI**
● export informací o toku ve formátu IPFIX nebo podobném formátu včetně plné podpory filtrů (exportovat lze pouze požadovaná data)	**Export informací o toku ve formátu IPFIX a jemu podobných včetně podpory filtrů**
● integrace se službami identity uživatelů bez nutnosti konfigurace zasílání logů do Systému – minimálně Cisco ISE a Microsoft Active Directory	**Integraci se službami identity uživatelů bez nutnosti konfigurace zasílání logů, např. Cisco ISE, Microsoft Active Dircetory**
● integrace s firewally, alespoň Palo Alto, Fortinet a Checkpoint, pro automatické a manuální reakce vyvolané Systémem	**Integraci s firewally Palo Alto, Fortigate, Checkpoint a dalšími pro aktivní automatický i manuální response**
● integrace s nástroji pro řízení přístupu k síti minimálně Cisco ISE, pro automatickou a manuální reakci Systému.	**Integraci s nástroji pro řízení přístupu k síti, např. Cisco ISE, pro automatický i manuální response**
Podpora EDR	
Systém musí poskytovat nástroje umožňující přímou integraci se softwarem EDR třetích stran pro získání informací a zkvalitnění detekce.	**Nabízené řešení umožňuje přímou integraci s EDR nástroji třetích stran**

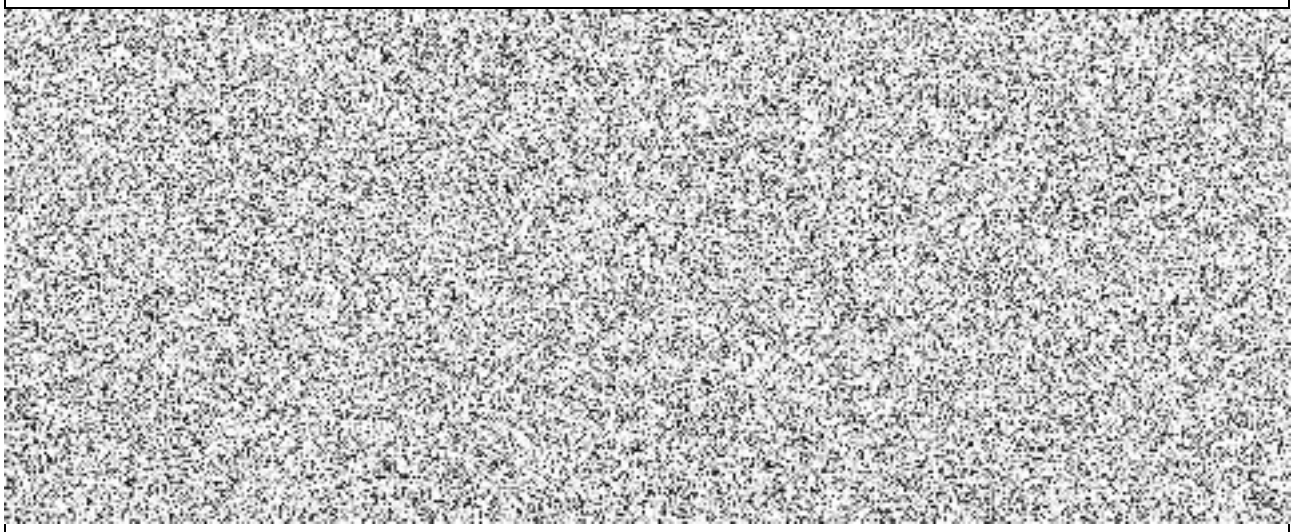
	pro získání informací a zkvalitnění detekce událostí.

Požadavky na architekturu nasazení

Požadované funkcionality/vlastnosti	**Krátký komentář, doplňující údaje (parametr, popis), jak nabízené řešení splňuje požadavek.**
Obecné požadavky pro nasazení	
Pro všechny HW komponenty senzor a kolektor je požadován formát 1U nebo 2U server o velikosti 19“.	**Všechny navržené HW komponenty senzor, kolektor i all-in-one jsou dodávány jako server formátu 1U nebo 2U o velikosti 19“.**
Pro všechny HW komponenty senzor a kolektor je požadován duální zdroj napájení se schopností hot-swap.	**Všechny HW servery jsou dodávány s duálním zdrojem napájení se schopností hot-swap.**
Pro všechny HW komponenty senzor a kolektor je požadováno samostatné síťové rozhraní pro vzdálenou správu serveru v případě výpadku Systému typu IPMI, IDRAC, ILO apod.	**Veškeré HW servery (senzory, kolektory i all-in-one) jsou dodávány se samostatným síťovým rozhraním pro vzdálenou správu serveru pro případ výpadku nabízeného řešení typu IDRAC.**
Požadavky pro pokrytí IT prostředí	
V síti je předpokládáno cca s průměrným . Je požadováno celkem a , a . V případě společného umístění sensoru/kolektoru lze řešit jedním nebo dvěma samostatnými HW boxy.	**Nabízené řešení zahrnuje , a , detailní rozpis kombinace je uveden dále. Celé řešení naplňuje požadavky na níže uvedenou architekturu nasazení.**
Je požadován o celkové propustnosti minimálně hostů s monitorovacím rozhraním 2x10/25GE a 4x1GE. Na zařízení je požadována dostupná historie dat minimálně 12 měsíců zpětně, uložená na rychlém úložišti typu SSD o velikosti alespoň 3TB. Požadován je minimálně RAID10 nebo RAID6 se schopností hot-swap.	**Nabízené řešení zahrnuje + o celkové propustnosti pro minimálně s monitorovacím rozhraním a , který je vybaven úložištěm typu o pro retenci dat měsíců, s + nebo s .**
Je požadován datový kolektor/sensor o celkové propustnosti minimálně s monitorovacím rozhraním 4x10/25GE a 2x1GE. Na zařízení je požadována dostupná historie dat minimálně 12 měsíců zpětně, uložená na rychlém úložišti typu SSD o velikosti alespoň . Požadován je minimálně RAID10 nebo RAID6 se schopností hot-swap.	**Nabízené řešení zahrnuje + o celkové propustnosti pro minimálně s monitorovacím rozhraním 4x10/25GE a 2x1GE, který je vybaven úložištěm typu pro retenci dat , s nebo s .**
Je požadován o celkové propustnosti minimálně s monitorovacím rozhraním 6x10/25GE. Na zařízení je požadována dostupná historie dat minimálně 12 měsíců zpětně, uložená na rychlém úložišti typu NVMe o velikosti . Požadován je minimálně RAID10 nebo RAID6 se schopností hot-swap	**Nabízené řešení zahrnuje + o celkové propustnosti s monitorovacím rozhraním 6x10/25GE, který je vybaven úložištěm typu o pro**

Spolufinancováno Evropskou unií

MINISTERSTVO PRO MÍSTNÍ ROZVOJ ČR

	měsíců, s nebo s .
Je požadován o celkové propustnosti minimálně s monitorovacím rozhraním .	**Nabízené řešení zahrnuje o celkové propustnosti s monitorovacím rozhraním**
Je požadován o celkové propustnosti minimálně 2Gbps s monitorovacím rozhraním a .	**Nabízené řešení zahrnuje o celkové propustnosti s monitorovacím rozhraním a .**
Je požadován o celkové propustnosti minimálně s monitorovacím rozhraním .	**Nabízené řešení zahrnuje o celkové propustnosti s monitorovacím rozhraním .**
Je požadován událostí (centrální konzole) pro centrální vyhodnocení událostí o celkové propustnosti .	**Nabízené řešení zahrnuje pro centrální o .**
Požadovaná architektura	
	

Požadavky na schopnost detekce bezpečnostních událostí

Požadované funkcionality/vlastnosti	**Krátký komentář, doplňující údaje (parametr, popis), jak nabízené řešení splňuje požadavek.**
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:	**Nabízené řešení identifikuje všechna zařízení připojená do sítě (koncových zařízení, serverů, IoT zařízení apod.) a identifikuje následující změny v síti:**
● změna IP/MAC adresy hosta,	**Změnu IP/MAC adresy hosta**
● duplicitní IP/MAC adresa,	**Duplicitní IP/MAC adresu**

● změna VLAN,	**Změnu VLAN**
● vytvoření nové podsítě,	**Vytvoření nové podsítě**
● připojení nového zařízení,	**Připojení nového zařízení**
● použití nebo vznik nové služby,	**Použití nebo vznik nové služby**
● nedostupnost dříve dostupné a komunikující služby nebo dříve dostupného a komunikujícího zařízení,	**Nedostupnost dříve dostupné a komunikující služby a dříve dostupného a komunikujícího zařízení**
● přístup nového zařízení ke službě či zařízení	**Přístupy nových zařízení ke službám a/nebo zařízením**
● ověřování platnosti interních certifikátu pro validní TLS šifrování u HTTPS a upozornění před datem jejich vypršení.	**Ověřování platnosti interních certifikátů pro validní TLS šifrování u HTTPS a upozornění před datem jejich vypršení**
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.	**Nabízené řešení umožňuje uživateli pomocí detekčních metod nastavovat bezpečnostní politiky pro různé segmenty sítě a různá zařízení a upozornit na jejich porušení.**
Samostatné učení behaviorálních aktivit a detekce anomálií	
Systém musí používat matematické metody samostatného učení pro analýzu síťové aktivity, vytvářet a v čase automaticky modifikovat modely chování na základě běžného chování jednotlivých zařízení a na nich provozovaných služeb v rámci celé organizace.	**Nabízené řešení používá matematické metody samostatného učení pro analýzu síťových aktivit, vytváří a automaticky v čase modifikuje modely chování na základě chování jednotlivých zařízení a provozovaných služeb v rámci celé organizace.**
Systém musí mít schopnost na základě matematického modelu daného zařízení a jeho služeb identifikovat nestandardní síťové chování, a to zejména odchylky od modelu normálního chování pro:	**Nabízené řešení identifikuje nestandardní síťové chování na základě matematického modelu daného zařízení a jeho služeb. Zejména detekuje následující odchylky od normálního chování:**
● odchylku od modelu pro přenos dat, toků a paketů,	**Odchylky pro přenos dat, toků a paketů**
● odchylku od modelu pro počet komunikačních partnerů,	**Odchylky pro počet komunikačních partnerů (naučený průměr a směrodatná odchylka)**
● odchylku od modelu entropie na komunikačních portech,	**Odchylky od modelu entropie na komunikačních portech (naučený průměr a směrodatná odchylka)**
● odchylku od modelu pro počet síťových toků a využitých síťových služeb,	**Odchylky od modelu pro počet síťových toků a využitých síťových**

	služeb (naučený průměr a směrodatná odchylka)
● odchylku od modelu výkonnosti sítě (rychlost přenosu) a aplikací (doba odezvy).	**Odchylky od modelu výkonnosti sítě a aplikací, tedy rychlosti přenosu a doby odezvy (naučený průměr a směrodatná odchylka)**
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.	**Nabízené řešení využívá metodu samostatného učení na všech síťových zařízeních a na nich provozovaných službách – porty 0 – 65535 u TCP a UDP, na IPv4 a IPv6, na dalších protokolech L3 a L4**
Identifikace neznámých hrozeb a podezřelých chování	
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:	**Nabízené řešení detekuje neznámé hrozby, které není možné odhalit pomocí detekčních signatur – trojské koně, botnety apod, zejména následující příznaky škodlivého chování:**
● průzkumné aktivity v síti,	**Průzkumné aktivity v síti - scany, multicastové průskumy, pingy apod.**
● detekce podezřelého strojového chování, které nevytvářejí lidští uživatelé sítě,	**Podezřelé strojové chování, které neodpovídá aktivitě lidských uživatelů sítě, též zvané jako beaconing.**
● detekce repetitivních vzorců chování na síti,	**Repetitivní vzorce chování v síti, tzn. periodicky se opakující a predikovatelnou komunikaci v časových intervalech 1 až 12 hodin**
● detekce botnetů a ovládání kompromitované stanice,	**Botnety a ovládání kompromitované stanice**
● detekce příznaků těžení kryptoměn,	**Příznaky těžby kryptoměn**
● útoky hrubou silou a enumerace dat,	**Útoky hrubou silou a enumerace dat**
● rozpoznání tunelovaného síťového provozu – alespoň IPv4 prostřednictvím IPv6 a DNS tunely.	**Tunelovaný síťový provoz IPv4 prostřednictvím IPv6 a DNS tunely**
Detekce na základě databáze známých hrozeb	
Systém musí být schopen identifikovat hrozby a reportovat události na základě	**Nabízené řešení identifikuje hrozby a reportuje události na základě:**
● detekční databáze známých hrozeb, tj. malware (trojské koně, viry, červy, rootkity, apod.), známých útoků (exploity) a zranitelností, porušení bezpečnostních pravidel a „best practices“ a dalších rizik,	**Detekční databáze známých hrozeb – malware, známých útoků a zranitelností, porušení bezpečnostních pravidel a best practices a dalších hrozeb**
● reputační databáze známých škodlivých IP adres, TLS certifikátů, záznamů DNS a hostname, URL adres a hashů souborů.	**Reputační databáze známých škodlivých IP adres, TLS certifikátů,**

	záznamů DNS a hostname, URL adres a hashů souborů
Tyto databáze musí být aktualizované minimálně na hodinové bázi. Nesmí se jednat pouze o volně dostupné/open-source databáze, ale musí se jednat o komerční databázi renomovaného vendora nebo poskytovatele těchto služeb.	**Nabízené řešení využívá profesionální licencovanou reputační databázi ProofPoint, která je aktualizovaná každou hodinu.**
Uživatel musí být schopen importovat vlastní záznamy.	**Nabízené řešení umožňuje uživateli importovat vlastní záznamy**
Systém musí využívat tuto 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 využívá tuto metodu detekce pro veškerý monitorovaný provoz v interní síti mezi všemi segmenty i na perimetru sítě.**
Databáze detekčních pravidel (signatur) musí být založena na pokročilých regulárních výrazech pro zpracování řetězců, které dokážou provádět inspekci veškeré síťové komunikace od L2 (Ethernet apod.) po L7. Systém musí detekovat události na základě vysokého počtu signaturních pravidel (minimálně několik desítek tisíc).	**Databáze detekčních pravidel v nabízeném řešení je založena na pokročilých regulárních výrazech pro zpracování řetězců, které provádí inspekci veškeré síťové komunikace od L2 po L7. Řešení detekuje události na základě více než 90 tisíc signaturních pravidel.**
Uživatel musí být schopen přidávat vlastní detekční pravidla v praktickém a obecně využívaném formátu. 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;)*	**Nabízené řešení umožňuje uživateli přidávat vlastní detekční pravidla v běžně využívaném formátu, jako je uvedený příklad, pro vytváření nabízí automatizovaný průvodce, nebo textovou konzoli.**
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.	**Nabízené řešení používá pro analýzu šifrované komunikace rovněž TLS fingerprinting a s tím spojenou detekci známých hrozeb.**
Asistované učení	
Je požadován uživatelsky přívětivý proces vytváření pravidel pro zpřesnění detekce a eliminaci falešně pozitivní detekce, a to na základě minimálně následujících parametrů:	**Nabízené řešení umožňuje uživatelsky snadné vytváření pravidel pro zpřesnění detekce a eliminaci falešně pozitivní detekce na základě následujících parametrů:**
● IP adresa,	**IP adresy**
● MAC adresa,	**MAC adresa**
● hostname,	**Hostname**
● segment sítě / podsíť,	**Segment sítě / podsíť**
● lokalita – ASN, země apod.	**Lokalita – ASN, země apod.**
● směr komunikace – určení klienta, nebo serveru,	**Směr komunikace, určení klienta a serveru**
● detekovaná událost – kategorie, název apod.	**Kategorie události, název apod.**

● použité služby, protokolu, portu,	**Služba, protokol, port…**
● libovolné kombinaci výše popsaných.	**Kombinace uvedených parametrů**
Systém musí být schopen eliminovat falešné alarmy i pro události detekované v historii.	**Nabízené řešení umí eliminovat falešné alarmy také pro události, které byly detekované v minulosti.**

Požadavky na zajištění síťové viditelnosti

Požadované funkcionality/vlastnosti	Krátký komentář, doplňující údaje (parametr, popis), jak nabízené řešení splňuje požadavek.
Vyhledávání, filtrování a vizualizace dat	
Systém musí být schopen okamžitého (v řádu vteřin) vyhledávání a vizualizace pro forenzní analýzu a podporu threat hunting bez zvláštního dotazovacího jazyka.	**Nabízené řešení vyhledává a vizualizuje výsledky pro forenzní analýzu a podporu threat hunting bez speciálního dotazovacího jazyka v řádu vteřin pro všechna uložená analyzovaná data**
Jedná se o možnost okamžitě filtrovat a vyhledávat v plné historii všech uložených dat, tj. bezpečnostních událostí, síťových toků a agregovaných síťových statistikách (tabulky a grafy), a to minimálně:	**Nabízení řešení bez časového zpoždění filtruje a vyhledává údaje v plné historii všech uložených dat (bezpečnostních událostí, síťových toků a agregovaných statistikách – tabulkách a grafech) podle následujících parametrů:**
● podle parametrů IP a MAC adresa, hostname, username (identita uživatele), příchozí a odchozí provoz, síťová služba, lokální nebo vzdálená služba (služba z pohledu klient nebo server), číslo portu, VLAN, země, ASN,	**IP a MAC adresa, hostname, identita uživatele, příchozí/odchozí provoz, síťová služba, lokální/vzdálená služba (z pohledu klinet/server), číslo portu, VLAN, země, ASN**
● prostřednictvím full-textového vyhledávání v datech a vyhledávání na základě definice směru (zdroj, cíl) a logických výrazů and, or, not.	**Full-text vyhledávání v datech a na základě definice zdroje/cíle a logických výrazů (AND/OR/NOT).**
Systém musí pro vyhledávání poskytovat již předpočítané hodnoty výkonnostních a behaviorálních charakteristik pro každé zařízení v síti a pro všechny na něm provozované služby, bez nutnosti zpracování surových dat ze síťových logů.	**Nabízené řešení poskytuje pro vyhledávání předpočítané hodnoty výkonnostních a behaviorálních charakteristik pro jednotlivá zařízení v síti a pro všechny na nich 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.	**Nabízené řešení filtruje a vizualizuje výsledky v grafech, výpočtových tabulkách a možností řazení a TOP N statistikách.**
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:	**Nabízené řešení ukládá a vyhledává aplikační metadata (dotaz i odpověď všech transakcí v toku)**

FTP, FTP-DATA, TFTP, TFTP-DATA, SSH, Telnet, SMTP, SMTPS, DNS, DHCP, HTTP, HTTPS, NTP, SMB, SNMP, LDAP, NFS, RDP, ARP, MS-SQL, SIP, Kerberos, SSL/TLS. Metadata jsou v tomto případě chápána jako přenášená aplikační metadata nebo vlastní data servisních protokolů. U protokolu HTTP například http hlavička s metodou, URI, host, user-agent, cookies apod. V odpovědi pak návratový kód a další http parametry.	**z protokolů: FTP, FTP-DATA, TFTP, TFTP-DATA, SSH, Telnet, SMTP, SMTPS, DNS, DHCP, HTTP, HTTPS, NTP, SMB, SNMP, LDAP, NFS, RDP, ARP, MS-SQL, SIP, Kerberos, SSL/TLS**
Systém umožnuje provádět uživatelsky jednoduché a okamžité vizualizace síťových prostupů mezi zařízeními a podsítěmi. Využitím uživatelského datového filtru lze vizualizační pohledy libovolně modifikovat.	**Nabízené řešení poskytuje uživateli možnost jednoduše a okamžitě vizualizovat síťové prostupy mezi zařízeními a podsítěmi, tyto vizualizační pohledy může uživatel libovolně upravovat díky uživatelskému datovému filtru dle vlastních potřeb.**
Kontextuální informace	
Systém musí být schopen pro každé zařízení získávat, vizualizovat a v jednom grafickém pohledu zobrazovat kontextuální informace:	**Nabízené řešení získává, vizualizuje a v jednom grafickém pohledu zobrazuje pro každé zařízení následující kontextuální informace:**
● jméno uživatele a další jeho parametry z doménového řadiče (MS Active Directory), včetně její historie	**Jméno uživatele a další parametry doménového řadiče – MS AD včetně historie**
● hostname zařízení a jeho historie na základě zpracování relevantních dat z DNS a DHCP provozu	**Hostname zařízení a jeho historii na základě zpracování relevantních dat z DNS a DHCP provozu**
● IP geolokace	**IP geolokaci**
● IP reputace, vč. údaje, jestli je IP adresa na blacklistu nebo podezřelá	**IP reputaci včetně informací, zda je IP adresa na blacklistu / podezřelá**
● historie použitých MAC adresa a výrobce zařízení	**Historii použitých MAC adres a výrobce zařízení**
● operační systém a jeho historie na zařízení	**Operační systém a jeho historii na zařízení**
● uživatelem zadané poznámky a informace k zařízení	**Uživatelsky zadané poznámky a informace o zařízení**
● automaticky přiřazené značky/tagy zařízení, které popisují jejich účel a chování – alespoň server doménového řadiče, webový server, poštovní server, server DNS, server SSH, databázový server, tiskárna, administrátorské zařízení, datové úložiště, aktivní dohledy, skenery zranitelností a technologické systémy.	**Automaticky přiřazené tagy zařízení popisující jejich účel a chování: server doménového řadiče, webový server, poštovní server, DNS, SSH, DB server, tiskárna, admin. zařízení, datové úložiště, aktivní dohledy, skenery zranitelností a technologické systémy.**
● seznam provozovaných a využívaných služeb (klient a server) u daného zařízení a množství na nich přenesených dat.	**Seznam provozovaných a využívaných služeb klient/server u zařízení a množství na nich přenesených dat.**

● seznam detekovaných bezpečnostních a provozních událostí daného zařízení.	**Seznam detekovaných bezpečnostních a provozních událostí daného zařízení.**
Zaznamenávání a ukládání plného provozu Je požadováno volitelné nahrávání plného síťového provozu (full packet capture) ve formátu PCAP na všech dodaných zařízeních minimálně na základě parametrů: cílová a zdrojová IP/MAC adresa, podsíť, využitý protokol, IPv4 nebo IPv6. Zaznamenávání je možno zapínat automaticky dle detekovaných událostí, nebo uživatelskou aktivací.	**Nabízené řešení umožňuje volitelné nahrávání plného síťového provozu – full packet capture ve formátu PCAP na všech dodaných zařízeních na základě parametrů: cílová a zdrojová IP/MAC adresa, podsíť, využitý protokol, IPv4 /IPv6. Zaznamenávání lze zapínat automaticky na základě detekovaných událostí nebo uživatelskou aktivací.**

Další požadované oblasti využití

Požadované funkcionality/vlastnosti	Krátký komentář, doplňující údaje (parametr, popis), jak nabízené řešení splňuje požadavek.
Monitorování politik kybernetické bezpečnosti	
Systém musí umožňovat vytváření komplexních komunikačních a bezpečnostních politik, a to minimálně:	**Nabízené řešení umožňuje vytváření komplexních komunikačních a bezpečnostních politik s následujícími parametry:**
● monitorovat definovanou komunikační matici a detekovat, kdy jsou tyto matice porušeny – alespoň jaké zařízení smí komunikovat s jakým zařízením, přes jaký protokol, v jakém čase.	**Monitorování definované komunikační matice a detekování v případě porušení – jaké zařízení má povoleno komunikovat s jakých zařízením, přes jaký protokol a v jakém čase**
● detekce změn v síti – přinejmenším nové komunikační vektory, nová nebo změněná zařízení a podsítě, obcházení perimetru.	**Detekci změn v síti – komunikační vektory, nová/změněná zařízení a podsítě, obcházení perimetru.**
Pro účely monitorování politik kybernetické bezpečnosti musí Systém poskytovat uživatelský rámec pro definování pravidel pomocí:	**Nabízené řešení poskytuje pro monitorování politik KB uživatelské prostředí pro definování pravidel pomocí následujících parametrů:**
● uživatelem definované podsítě na základě rozsahů IP adres	**Uživatelem definované podsítě na základě rozsahů IP adres**
● uživatelsky libovolně definovaných skupin zařízení	**Uživatelsky libovolně definovaných skupin zařízení**
● automaticky přiřazené značky/tagu zařízení, které popisují jejich účel a chování – alespoň server doménového řadiče, webový server, poštovní server, server DNS, server SSH, databázový server, tiskárna, administrátorské zařízení, datové úložiště, aktivní dohledy, skenery zranitelností a technologické systémy.	**Automaticky přiřazených tagů zařízení popisujících jejich účel a chování – server doménového řadiče, webový server, poštovní server, DNS, SSH, DB server, tiskárna, administrátorské zařízení, datové úložiště, aktivní dohledy,**

	skenery zranitelností a technologické systémy.
Management bezpečnostních událostí a incidentů	
Systém musí poskytovat funkcionalitu pro reporting bezpečnostních incidentů (prohlášení identifikované události za bezpečnostní incident), včetně:	**Nabízené řešení umožňuje reporting bezpečnostních incidentů (označení události za bezpečnostní incident) s následujícími parametry:**
● 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,	**Sdílení informací při analýze identifikovaných incidentů včetně souvisejícího workflow mezi uživateli s podporou automatizovaných oznámení o změně stavu události a přiřazení řešitele**
● jednoduché sdílení informací o bezpečnostních incidentech, včetně uživatelem zadaných komentářů,	**Sdílení informací o bezpečnostních incidentech včetně uživatelsky vložených 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.),	**Vyhledávání a filtrování nad všemi událostmi z pohledu workflow incidentu – report/ v řešení / vyřešená událost / událost v řešení zadaného uživatele atd.**
● možnost exportování dat do emailu, csv, pdf, syslogu a podobně,	**Exportování dat do e-mailu, csv, pdf, syslog**
● možnost exportu bezpečnostních událostí a incidentů do systémů typu ticket management třetích stran.	**Exportování bezpečnostních událostí a incidentů do ticketovacích systémů třetích stran**
Detekce úniku dat	
Systém musí být schopen detekovat přenosy citlivých souborů a dat definovaných pomocí jejich názvů, hashů, specifického binárního obsahu (vodoznaku) nebo regulárních výrazů (např. rodné číslo).	**Nabízené řešení detekuje přenosy citlivých souborů a dat definovaných jejich názvem, hashem, binárním obsahem nebo regulárními výrazy**
Systém musí být schopen detekovat přenosy citlivých souborů a dat alespoň u následujících protokolů: HTTP, FTP, SMTP, SMB, NFS.	**Nabízené řešení detekuje přenosy citlivých souborů a dat u protokolů HTTP, FTP, SMTP, SMB, NFS.**
V rámci historických metadat u HTTP, FTP, SMTP, SMB a NFS je požadováno ukládání informací o všech po síti přenášených souborech alespoň v rozsahu:	**Pro historická metadata u protokolů HTTP, FTP, SMTP, SMB a NFS jsou ukládány informace o všech přenášených souborech v síti v rozsahu:**
● název souboru,	**Název souboru**
● velikost souboru,	**Velikost souboru**
● HASH souboru.	**Hash souboru**
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) model normálního chování pro výkonnostní parametry minimálně:	**Nabízené řešení měří a automaticky vytváří model normálního chování v celé monitorované síti, mezi všemi zařízeními a na všech službách pro následující výkonnostní parametry:**
● přenosová rychlost sítě,	**Přenosová rychlost sítě**
● rychlost odezvy aplikace,	**Rychlost odezvy aplikace**
● odezva Systému z pohledu uživatele.	**Odezva z pohledu uživatele**
Výpočet uvedených výkonnostních parametrů a automatické detekce anomálií na základě odchylky od modelu normálního chování musí být prováděna pro:	**Nabízené řešení provádí výpočet výše uvedených výkonnostních parametrů a automatické detekce anomálií na základě odchylky od modelu normálního chování pro všechny:**
● všechny porty a služby TCP,	**Porty a služby TCP**
● pro všechny kombinace služeb a zařízení.	**Kombinace služeb a zařízení**
Systém musí v celé monitorované síti, mezi všemi zařízeními a na všech službách měřit informace o retransmission paketech, out of order paketech, TTL, QoS a komunikaci blokované firewally.	**Nabízené řešení měří informace o retransmission / out-of-order paketech, TTL, QoS a komunikacích blokovaných firewally v celé monitorované síti mezi všemi zařízeními a na všech službách.**
Monitoring cloudových služeb	
Systém musí být schopen monitorovat přístupy zařízení a uživatelů ke cloudovým službám, a to minimálně Google Workspace a Microsoft Office 365, vč. monitoringu operací se soubory, změn oprávnění a nastavení a neúspěšných přístupů.	**Nabízené řešení monitoruje přístupy zařízení a uživatelů je cloud službám Google Workspace a MS Office 365 včetně monitorování operací se soubory, změn oprávnění / nastavení a neúspěšných pokusů o přístup.**
Systém musí být schopen tyto informace autonomně a průběžně získávat z aplikačních rozhraní těchto cloudových služeb bez nutnosti využití řešení třetích stran.	**Nabízené řešení výše uvedené informace autonomně a průběžně získává z aplikačního rozhraní těchto cloud služeb bez potřeby využití řešení třetích stran**
Inventarizace sítě a grafický vizualizace topologie	
Systém musí být schopen zobrazit celý inventář monitorované sítě s počtem zařízení v jednotlivých lokalitách, segmentech, nebo podsítích. Včetně detailního přehledu zařízení.	**Nabízené řešení umožňuje zobrazit celý inventář monitorované sítě, počty zařízení v jednotlivých lokalitách, segmentech a podsítích včetně detailního přehledu zařízení.**
Systém musí být schopen graficky vykreslit celou topologii sítě, dle zaznamenané komunikace.	**Nabízené řešení umožňuje graficky vykreslit celou topologii sítě podle zaznamenané komunikace.**
Systém musí být schopen zobrazit inventář jednotlivých lokalit, přehledy zařízení, přehledy výrobců, tagy zřízení, uživatele.	**Nabízené řešení umožňuje zobrazit celý inventář jednotlivých lokalit**

	s přehledy zařízení, výrobců, tagy a uživateli zařízení.
Systém umožnuje všechny inventory informace řadit dle různých parametrů.	**Nabízené řešení umožňuje řadit veškeré inventarizační informace podle různých parametrů dle potřeby uživatele.**

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 trvání Smlouvy.

Dodavatel zajistí vyladění a nastavení detekce všech dodávaných systémů tak, aby nebyly detekované nežádoucí a falešně pozitivní události. Tato činnost bude provedena ve spolupráci s kompetentními osobami Objednatele. Dodavatel zajistí integraci nástroje s aktuálním log managementem Objednatele, dále pak nastavení aktivních alertů a reportů dle potřeb Objednatele.

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;

Objednatel 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 Objednatel povinen zabývat se všemi hrozbami, které prostřednictvím varování vydává NÚKIB a zohlednit je v analýze rizik. Objednatel 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 Objednatele znamenat žádné další náklady.

Produktová Podpora Výrobce

Dodavatel musí zajistit:

- softwarovou produktovou podporu řešení od Výrobce v délce 60 měsíců od podepsání Akceptačního protokolu po předání Systému.
- záruku na veškerá dodaná HW zařízení minimálně v rozsahu 5 let NBD ode dne akceptace (Next Business Day) On-Site.

Provozní dokumentace

Dokumentace bude zpracována a vydána jako ucelený dokument ve formátech DOCX a PDF. 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
-

Obsahem dokumentace bude minimálně:

- **Popis architektury řešení** (společné pro všechny lokality)
  - Popis návrhu architektury Dodavatelem navrženého řešení v nabídce pro veřejnou zakázku.
  - Popis musí obsahovat minimálně:
    - Schematický nákres zapojení nabízených prvků
    - Textový popis fungování řešení jako celku. Z popisu musí být zřejmé, jakou roli jednotlivé komponenty zajišťují, jak je zajištěna jejich dostupnost a jak do celku zapadají.
    - Popis závislostí mezi jednotlivými komponentami.

- **Popis skutečného stavu předávaného řešení pro každou lokalitu samostatně**
  - Popis musí obsahovat přehled všech hardwarových komponent, které jsou obsahem řešení. U každé komponenty musí být uvedeno minimálně:
    - Název zařízení v síti Objednatele (pokud to zařízení umožňuje)
    - Výrobce a typ zařízení.
    - Sériové číslo zařízení.
    - Specifikace portů, kterými je zařízení připojeno do LAN (přesná specifikace každé LAN), jejich počty a nakonfigurované rychlosti.
      - Pokud se jedná o port sondy specifikovat, který zdroj/zdroje je kam zapojen
  - Popis musí obsahovat přehled všech softwarových komponent, které jsou obsahem řešení. U každé komponenty musí být uvedeno minimálně:
    - Název komponenty.
    - Kompletní přehled dodaných a použitých licencí.
    - Přehled, jak jsou jednotlivé licence využity a na kterých HW prvcích.
  - Popis všech úprav vytvořených pro potřeby této zakázky

Přístup k managementu řešení – přehledová tabulka

  - Tabulka musí obsahovat přehled všech použitých komponent s možností managementu. U každé komponenty musí být uvedeno:
    - FQDN a IP komponenty pro vzdálený přístup.
    - Forma přístupu ke konfiguraci (webový prohlížeč, instalovaná aplikace pro správu apod.)
    - Použité rozhraní (RS232, USB a pod.)

- **Konfigurace LAN parametrů řešení – přehledová tabulka**

- Tabulka musí obsahovat:
  - přehled všech komponent připojených do LAN
  - název komponenty a její typ
  - přehled všech konfigurovaných IP adres a FQDN jmen tak, aby bylo zřejmé, jaké všechny IP adresy a jména zařízení využívá.

- **Přístupové údaje nastavené při implementaci – přehledová tabulka**
  - Tabulka musí obsahovat veškeré přístupové údaje k jednotlivým komponentám a jejich managementu tak, aby Objednatel měl po převzetí řešení neomezený přístup ke všem jeho částem.

- **Přístup k technické podpoře**
  - Popis musí obsahovat:
    - Kontaktní informaci na technickou podporu – jedno kontaktní místo (single point of contact).
    - Pravidla práce s technickou podporou (musí být v souladu s požadavky VZ).
    - Kontaktní informace na servisní pracoviště zajišťující podporu jednotlivých HW komponent.

- **Dokumentace k rozhraní (CLI/GUI)**
  - Musí obsahovat minimálně:
    - Uživatelskou dokumentaci základních operací s aplikační částí (např. přihlášení, nastavení, odhlášení, vytvoření filtrů, vytvoření pohledů,…)
    - Administrátorskou dokumentaci(např. propojení s LDAP, vytváření uživatelů,…)

Administrátorské školení

V rámci realizace je požadováno administrátorské školení pro zaměstnance Objednatele a zaměstnance organizačních složek v rozsahu nezbytném pro kvalifikovanou obsluhu včetně videozáznamu pro zpětné použití, který bude dostupný online na zabezpečeném úložišti Dodavatele a tematicky zahrnuje zejména:

- základy síťového provozu

úvod do analýzy síťového provozu – nástroje, techniky

- seznámení s uživatelským prostředím

úvodní nastavení Systému

- analýza událostí a false positives

vizualizace dat

- základy síťové komunikace (protokoly atd.)

typové druhy útoků a jejich detekce Systémem.

Dále je v rámci Servisní podpory dle přílohy č. 5 Smlouvy požadováno opakované proškolení administrátorů a určených uživatelů jednou ročně v rozsahu minimálně 1MD, včetně revize analýzy bezpečnostních událostí ve všech lokalitách.

Akceptační podmínky

Předpokladem pro předání řešení do provozu (akceptaci Dodávky Zařízení) bude splnění všech následujících akceptačních testů.

Akceptační kritérium	splňuje/nesplňuje
• 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 Objednatele.	
● Dochází k záznamu flow a zrcadleného provozu, informace jsou dostupné k zobrazení a dalšímu zpracování.	
● V Systému jsou zavedeny všechny Objednatelem dodané podsítě.	
● V Systému jsou automatizovaně označeny (otagovány) důležitá zařízení jako doménové kontroléry, mailové a webové servery apod.	
● Výsledná informace vyhledávání (graf nebo tabulka) definovaná libovolně nastaveným základním filtrem (např. IP adresa/y, podsíť/e, služba/y, událost/i, …) v 24hodinovém intervalu musí být zobrazena do 30s.	
● Funguje asistované učení při označení falešně pozitivní detekce.	
● Pro všechna zařízení v síti jsou okamžitě dostupné informace o zařízeních (název, mac adresy, IP adresa, uživatele, klientské služby, serverové služby, detekované události, …)	
● Systém korektně načítá VLAN-ID ze zrcadlené komunikace a umožňuje filtrování informací podle VLAN-ID.	
● Systém zobrazuje inventarizovanou grafickou topologii celé sítě, včetně počtu zařízení v jednotlivých segmentech sítě a jejich bezpečnostním rizikem.	
● 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 interface.	
● Systém detekuje známé hrozby na základě databáze známých hrozeb (je aktivně využíváno alespoň 50.000 detekčních pravidel/signatur a alespoň 100.000 záznamů typu Threat Intelligence).	
● Systém detekuje anomálie na základě dynamicky se měnících modelů chování jednotlivých zařízení, Systém má nastavené (samostatně naučené) prahové hodnoty, na základě kterých detekuje anomálie. Prahové hodnoty jsou jasně viditelné pro každé zařízení a každou jeho službu.	
● Byla vytvořena a dodána provozní dokumentace.	
● Bylo předloženo potvrzení o Podpoře výrobce na 60 měsíců	
● Bylo provedeno školení v požadovaném rozsahu a je dostupný videozáznam	

Budou-li splněna veškerá akceptační kritéria uvedená shora v tabulce, zástupci Objednatele potvrdí splnění všech akceptačních podmínek pro předání řešení do ostrého provozu (Dodávku Zařízení) v Akceptačním protokolu, podepsaném zástupci obou Smluvních stran.

Spolufinancováno Evropskou unií

MINISTERSTVO PRO MÍSTNÍ ROZVOJ ČR

Realizační tým

Role	Kontaktní údaje	Osoba Poddodavatele (ANO/NE)
1. Projektový manažer	Jméno a příjmení: [redacted] Telefon: [redacted] E-mail: [redacted]	Ne
2. Technický specialista 1	Jméno a příjmení: [redacted] Telefon: [redacted] E-mail: [redacted]	Ne
3. Technický specialista 2	Jméno a příjmení: [redacted] Telefon: [redacted] E-mail: [redacted]	Ne
4. Technický specialista 3	Jméno a příjmení: [redacted] Telefon: [redacted] E-mail: [redacted]	Ne
5. Servisní specialista	Jméno a příjmení: [redacted] Telefon: [redacted] E-mail: [redacted]	Ne
6. Architekt Kybernetické bezpečnosti	Jméno a příjmení: [redacted] Telefon: [redacted] E-mail: [redacted]	Ne

Spolufinancováno Evropskou unií

MINISTERSTVO PRO MÍSTNÍ ROZVOJ ČR

Dodavatel zajistí plnění Smlouvy prostřednictvím shora uvedených členů Realizačního týmu, u nichž doložil v rámci Zadávacího řízení osvědčení o vzdělání a odborné kvalifikaci. Tuto povinnost má Dodavatel i u všech nových členů Realizačního týmu na výše uvedených pozicích v době trvání Smlouvy. Příslušné doklady Dodavatel předloží Objednateli také vždy na vyžádání.

Seznam míst plnění

Označení organizace	Lokalita	Adresa lokality
		,
		,
	–	
		,
	. ,	
	–	
		218,
	–	, , I
		,
	–	,
		5
	. ,	
		,
	–	,
		,
		,
		,
		,
	KSZ Praha	,
		,
		,
	–	,
		,

Spolufinancováno Evropskou unií

MINISTERSTVO PRO MÍSTNÍ ROZVOJ ČR

[redacted]		
[redacted]		
[redacted]		
[redacted]		
[redacted]		
[redacted]		
[redacted]		
[redacted]		
[redacted]		
[redacted]		4
[redacted]		
[redacted]		

Použité zkratky:

[redacted]

Vzor Akceptačního protokolu

Akceptační protokol

dle Smlouvy na dodávku systému detekce síťového provozu a zajištění servisní podpory č. MSP-34 / 2024-MSP-CES

Dodavatel: **NTT Czech Republic** se sídlem: Milevská 2095/5, 140 00 Praha 4 IČO: 26175738	**Objednatel:** **Česká republika – Ministerstvo spravedlnosti** se sídlem: Vyšehradská 16, 128 10 Praha 2 IČO: 000 25 429
Předmět akceptace: … **Vyjádření Objednatele:** ***Akceptováno** / **Neakceptováno** vč. případného uvedení, v čem předmětný výstup dle Objednatele neodpovídá požadavkům uvedeným ve Smlouvě, anebo jaké obsahuje vady, a to spolu se stanovením lhůty k odstranění vad a nedostatků…*	
Za Dodavatele: Jméno a příjmení:	**Za Objednatele:** Jméno a příjmení:
dne: podpis:	dne: podpis:

Podmínky Servisní podpory

1 Všeobecné podmínky poskytování služeb Servisní podpory

V rámci nabízeného řešení se Dodavatel zavazuje po dobu 5 let poskytovat odborné záruky a servisní služby na programové vybavení (software) a technické vybavení (hardware) pro zajištění bezproblémového provozu celého řešení. Servisní podpora pro dodané řešení bude Dodavatelem zajištěna v celém rozsahu přímo u Výrobce technologie, tak aby řešení technických potíží a SW aktualizace, které je oprávněn vykonávat pouze Výrobce, bylo možno konzultovat přímo s ním, pokud Dodavatel není schopen servisní podporu provádět samostatně. Poskytování Servisní podpory bude po celou dobu trvání smluvního vztahu u Výrobce ověřitelné.

Nabízené služby se nebudou vztahovat na jiné vybavení, než bylo předmětem plnění Veřejné zakázky. Pracovníci Dodavatele k takovým úkonům nebudou oprávněni a Objednatel ani koncový uživatel na nich nebude takovéto činnosti vyžadovat. Za zajištění správné funkčnosti jiného vybavení, než je předmětem plnění podle Smlouvy bude zodpovědný Objednatel.

Termín, kdy bude poskytování nabízených služeb a podpory zahájeno, je určeno dnem podpisu Akceptačního protokolu.

Místem plnění Servisní podpory jsou místa instalace uvedená v Příloze č. 3 Smlouvy (Seznam míst plnění). Dodavatel bere na vědomí, že místa instalace se výjimečně mohou změnit (např. kvůli stěhování) a je povinen zajistit poskytování Servisní podpory za stejných podmínek i v novém místě instalace, které mu Objednatel v dostatečném časovém předstihu oznámí.

Dodavatel se zavazuje, že jeho pracovníci (členové realizačního týmu) budou při plnění závazků dodržovat příslušné interní akty řízení Objednatele. Objednatel se zavazuje před poskytováním služeb, podpory a údržby pracovníky Dodavatele prokazatelně seznámit s u něj platnými interními akty řízení.

Dodavatel se zavazuje spolupracovat na analýze problému a jeho vyřešení. V případě potřeby zajistí řešení problému přímo Výrobcem.

Dodavatel se zavazuje provádět řádnou provozní údržbu podporovaného technického vybavení servisním pracovištěm Dodavatele, a to bezodkladně v rozsahu a v termínech předepsaných Výrobci tohoto vybavení, nebo dle požadavků Objednatele.

Objednatel i Dodavatel se zavazují spolupracovat také při úpravách nebo rozšiřování systému Objednatele v zájmu zachování funkčnosti vybavení Objednatele podporovaného Dodavatelem.

Dodavatel bude odpovídat za veškerou způsobenou škodu.

Servisní podpora a údržba na celé řešení musí zahrnovat jediné kontaktní místo (single-point-of-contact) pro hlášení všech závad.

Součástí Servisní podpory a údržby na celé řešení musí být analýza všech nahlášených problémů. V případě, že bude podporou identifikována závada na některé z komponent, na níž řešení zajišťuje přímo servisní pracoviště Výrobce, zajistí podpora eskalaci závady na příslušné pracoviště a koordinaci při odstranění závady.

Služby, podpora a údržba budou zahrnovat postupně jeden nebo více způsobů postupů, kterými budou:

telefonická konzultace,

odborná pomoc prostřednictvím e-mailové korespondence,

odborná pomoc prostřednictvím webového prostředí Dodavatele,

zásah interaktivně po telefonu,

zásah Dodavatele osobně v místech instalace u Objednatele.

Novému požadavku bude přiděleno evidenční číslo, pod kterým bude u Dodavatele dále dokumentováno a bude užito pro identifikaci předávaných zpráv.

Průběh řešení požadavku koordinuje Dodavatel.

Veškerá komunikace v průběhu řešení jednotlivých případů musí být vedena pouze v českém jazyce.

1.1 HW servisní podpora

Součástí dodávané standardní záruky na HW komponenty musí být závazek vyřešení závady v rozsahu Next Business Day On-Site.

1.2 SW servisní podpora

Servisní podpora bude poskytována na veškeré dodávané SW komponenty. Servisní podporou se rozumí předávání nových verzí veškerých SW modulů programového vybavení s vylepšenými funkcemi tak, jak je výrobce programového vybavení dává k dispozici. Aktualizace programového vybavení zajišťují jeho kompatibilitu s ostatními SW a HW komponenty informačního systému v souvislosti s jejich vývojem.

Poskytování služeb SW Servisní podpory a technické podpory a údržby bude zahájeno bez zbytečného odkladu po přijetí požadavku. Všechny činnosti Dodavatele budou směřovat k zjištění příčin vzniku provozních potíží nebo závad a poruch funkčnosti vybavení Objednatele, k jejich odstranění a k obnovení funkčnosti servisovaného vybavení v nejkratší době, nejdéle však do doby uvedené v kap. 1.2.2.

1.2.1 Úrovně závažnosti SW problému

Závažnost hlášení o problému je definována následující tabulkou:

- **Kritické** problémy zcela zamezují účinné využití aplikace.
- **Důležité** problémy závažně snižují výkonové charakteristiky aplikace, pokud jde o její kvalitu a použitelnost pro uživatele.

- **Drobné** problémy jsou všechny ostatní softwarové nebo systémové problémy hlášené uživatelem.

1.2.2 Maximální doba řešení SW problému

Problémy v kódu/algoritmu jsou odstraněny s následujícími termíny:

- do 5 pracovních dnů pro **kritické** problémy
- do 15 pracovních dnů pro **důležité** problémy
- v příštím vydání softwaru pro **drobné** problémy

1.3 Podpora uživatelů

Standardní podpora začne ihned po předání dodávky a bude obsahovat:

- osobní návštěvy u administrátorů na celkem 8 hodin pro každou justiční složku / v místě plnění na každých 6 měsíců (uživatelskou podporu lze využít pro školení nových administrátorů, vyhodnocování událostí a další aktivity)
- vzdálená asistence (telefonická konzultace, odborná pomoc prostřednictvím e-mailové korespondence, odborná pomoc prostřednictvím webového prostředí Dodavatele) od 8. do 17. hod v pracovní dny

2 Školení uživatelů

Jedním dnem se myslí 1 manday (MD), tedy 1x 8 hodin.

2.1 Průběžné (opakované) školení administrátorů (uživatelů)

Průběžné školení jednotlivých administrátorů z organizačních složek justice navazuje na úvodní zaškolení administrátorů. Bude zahájeno po akceptaci celkového řešení Objednatelem. Opakované proškolení uživatelů jednou ročně v rozsahu minimálně 1MD, včetně revize analýzy bezpečnostních událostí bude tematicky zaměřené zejména na:

- analýzu událostí a false positives

řešení konkrétních událostí v justiční organizaci

- úpravy a ladění systému

2.2 Jednodenní společné školení administrátorů

Školení proběhne formou videokonference jednou za 1 rok. Školení bude obsahovat témata vyžádaná manažerem kybernetické bezpečnosti MSp. Může jít o zopakování témat z úvodního školení administrátorů, nebo témata nová, která vyplynula z provozu a potřeb organizačních složek justice.

3 Evidence poskytování služeb Servisní podpory a školení – Elektronický provozní deník

Dodavatel požaduje v rámci plnění dodání aplikaci pro evidenci servisních zásahů – elektronický provozní deník (dále jen „Deník“), řešení bude realizováno ve formě webové aplikace přístupné na prostředcích Dodavatele. Deník dále bude sloužit k čerpání uživatelské podpory, školení a všech dalších služeb v organizačních složkách justice.

rganizacích.odpory a dalších služeb v parterských

Deník bude minimálně umožňovat povinný zápis:

- identifikace pracovníka, který záznam provedl

data a času zápisu, případně zahájení činnosti

- data a času ukončení provádění činnosti

popisu provedené činnosti

- výsledek provedení činnosti

Záznamy v deníku budou opatřeny elektronickým podpisem a kvalifikovaným časovým razítkem.

V záznamech bude možno autorizovaně vyhledávat podle všech zaznamenávaných atributů.

Aplikace bude obsahovat administrátorské rozhraní pro stanovení rolí a přístupových práv. Oprávnění budou svázána s místem instalace. Předpokládané role a oprávnění:

- Administrátor sondy – jen zápis, čtení vlastních záznamů, možnost volby libovolných míst instalace
- Administrátor Dodavatele – zápis a čtení všech záznamů
- Administrátor Objednatele – zápis a čtení všech záznamů, plný přístup do administrátorského rozhraní deníku