KUPNÍ SMLOUVA

ČÍSLO 0006/0/OIN/22

uzavřená níže uvedeného dne, měsíce a roku dle ustanovení § 1746 odst. 2 a § 2079 a násl. zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „**Občanský zákoník**"), mezi níže uvedenými smluvními stranami (dále jen „**Smlouva**"):

(1) **Městská část Praha 5,**
se sídlem: Praha 5, Smíchov, náměstí 14. října 1381/4
zastoupená: Mgr. Renátou Zajíčkovou, starostkou
IČ: 00063631
DIČ: CZ00063631
(dále jen „**Kupující**")

a

(2) **ICZ a.s.**
se sídlem: Na hřebenech II 1718/10, Nusle, 140 00 Praha 4
Zastoupená: Ing. Marianem Arbetem, ředitelem sekce Infrastruktura, na základě plné moci ze dne 18. 12. 2018
IČO: 25145444
~~DIČ: CZ25145444~~ CZ 699000372 [redacted]
Bankovní spojení: [redacted] UniCredit Bank Czech Republic and Slovakia, a.s.
zapsaná v obchodním rejstříku vedeném pod sp. Zn. B 4840 u Městského soudu v Praze
(dále jen „**Prodávající**")

(Kupující a Prodávající společně dále jen „**Smluvní strany**" nebo jednotlivě též jen „**Smluvní strana**")

1 ÚVODNÍ UJEDNÁNÍ

1.1 Kupující realizuje nákup na základě zadávacího řízení na veřejnou zakázku malého rozsahu na dodávky s názvem „**Systém pro identifikaci a zastavení pokročilých bezpečnostních hrozeb - Fidelis Elevate** ", přičemž základním hodnotícím kritériem byla nejnižší nabídková cena (dále jen „**Zadávací řízení**").

1.2 Nabídka Prodávajícího byla Kupujícím, jakožto zadavatelem veřejné zakázky, vyhodnocena jako nejvhodnější. Smluvní strany tak za níže uvedených podmínek uzavírají tuto Smlouvu.

2 PŘEDMĚT SMLOUVY

2.1 Prodávající se zavazuje, že Kupujícímu dodá systém pro identifikaci a zastavení pokročilých bezpečnostních hrozeb - **Fidelis Elevate**, vč. maintenance na dobu 12 měsíců pro potřeby Úřadu městské části Praha 5 v rozsahu blíže specifikovaném v příloze č. 1 této Smlouvy (dále jen „**Systém proti bezpečnostním hrozbám**"), a převede na něj vlastnické právo k předmětu plnění dle této Smlouvy; Prodávající se též zavazuje poskytovat i příslušnou maintenance. Lhůta k poskytování maintenance začne běžet dnem předání Systému proti bezpečnostním hrozbám Kupujícímu bez vad a nedodělků, případně dnem odstranění a předání vytknutých vad a nedodělků.

2.2 Kupující se zavazuje, že dodaný Systém proti bezpečnostním hrozbám a služby od Prodávajícího převezme a zaplatí za ně Prodávajícímu cenu, to vše v rozsahu a za podmínek dle této Smlouvy.

2.3 Prodávající se zavazuje, že dodaný Systém proti bezpečnostním hrozbám bude ke dni předání nový, originální, nepoužitý, nerepasovaný, určený pro trh v EU a zadavatele. V databázi výrobce, pokud taková existuje, musí být zadavatel veden jako první uživatel zboží.

2.4 Dodávaný Systém proti bezpečnostním hrozbám musí být pokryt oficiální podporou výrobce tak, aby v případě závady, kterou není účastník schopen odstranit, mohl zadavatel tuto závadu eskalovat přímo k technické podpoře výrobce. Zadavatel musí mít možnost si sám legálně stahovat bezpečnostní záplaty i nové verze SW/FW na základě zaregistrování čísla aktivovaného servisního kontraktu.

2.5 Prodávající je povinen Kupujícímu dodat veškeré licence a oprávnění nezbytná k řádnému užívání systému, který je součástí dodávky dle této Smlouvy, a které jsou vyžadovány závaznými právními předpisy nebo jiným způsobem. Cena za poskytnutí takových licencí a oprávnění je zahrnuta v kupní ceně dle čl. 4.1 této Smlouvy.

2.6 Prodávající je povinen převést všechna užívací práva Systému proti bezpečnostním hrozbám na Kupujícího a prohlašuje, že tato práva nejsou zatížena jinou vazbou.

3 MÍSTO A TERMÍN DODÁNÍ

3.1 Místem dodání je Úřad Městské části Praha 5 na adrese Štefánikova 13-15, Smíchov, Praha 5 (dále jen „**Místo plnění**").

3.2 O předání a převzetí Systému proti bezpečnostním hrozbám bude vyhotoven a oprávněnými zástupci Smluvních stran podepsán předávací protokol, v němž bude uveden den dodání, specifikace dodaného Rozšíření zálohování, specifikace dodaných dokladů a popř. nezbytných kódů (dále jen „**Předávací protokol**").

3.3 Jakékoli vady Systému proti bezpečnostním hrozbám zjištěné při jeho předání a převzetí musí být uvedeny v Předávacím protokolu. Prodávající je povinen tyto odstranit ihned, nejpozději však do dvou pracovních dnů ode dne podpisu Předávacího protokolu, nedohodnou-li se Smluvní strany v Předávacím protokolu s ohledem na povahu vady jinak.

3.4 Systém proti bezpečnostním hrozbám v plném rozsahu dodá Prodávající Kupujícímu nejpozději do 30 dnů od účinnosti této Smlouvy.

4 CENA A PLATEBNÍ PODMÍNKY

4.1 Smluvní stany se dohodly na ceně dodávky Systému proti bezpečnostním hrozbám, vč. maintenance v rozsahu uvedeném v příloze č.1 této Smlouvy. Cena za dodávku činí

1 898 293,00 Kč bez DPH (slovy: ***jeden milion osm set devadesát osm tisíc dvě stě devadesát tři korun českých***) (dále jen „**cena**").

4.2 Prodávající prohlašuje, že cena sjednaná v čl. 3.1této Smlouvy plně pokrývá veškeré jeho náklady spojené s dodávkou Systému proti bezpečnostním hrozbám a zavazuje se vůči Kupujícímu nevznášet jakékoli nároky nad její rámec.

4.3 Cena bude uhrazena Prodávajícímu na základě daňového dokladu vystaveného Prodávajícím po řádném dodání Systému proti bezpečnostním hrozbám.

4.4 Faktura bude mít veškeré náležitosti daňového dokladu v souladu se zákonem č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, a její přílohou bude Předávací protokol. Daňový doklad bude dále obsahovat také následující údaje:

(i) číslo Smlouvy Kupujícího, a případně označení dodatků této Smlouvy;

(ii) počet kusů a dobu trvání dle přílohy č. 1 této Smlouvy.

4.5 Daňový doklad vystavený Prodávajícím podle této Smlouvy Prodávající ve 2 vyhotoveních zašle Kupujícímu.

4.6 Splatnost daňového dokladu bude činit vždy 30 kalendářních dnů ode dne jejího doručení Kupujícímu. Za den úhrady daňového dokladu bude považován den odepsání fakturované částky z účtu Kupujícího.

4.7 Kupující je oprávněn vrátit Prodávajícímu daňový doklad do data jeho splatnosti, nebude-li obsahovat veškeré údaje vyžadované závaznými právními předpisy nebo touto Smlouvou nebo v něm budou uvedeny nesprávné údaje anebo k němu nebude přiložen Předávací protokol nebo potvrzení Kupujícího o poskytnutí Služeb. V takovém případě začne běžet lhůta splatnosti daňového dokladu až doručením řádně opraveného daňového dokladu Kupujícímu.

5 Práva a povinnosti Smluvních stran

5.1 Smluvní strany jsou povinny vzájemně spolupracovat a poskytovat si veškerou nutnou součinnost potřebnou pro řádné splnění této Smlouvy, vzájemně se informovat o veškerých skutečnostech, které jsou nebo mohou být důležité pro splnění této Smlouvy.

5.2 Kupující je povinen vytvořit vhodné podmínky pro Systém proti bezpečnostním hrozbám a předat Prodávajícímu informace nezbytné pro dodání.

5.3 Prodávající je povinen postupovat při plnění této Smlouvy s náležitou odbornou péčí a podle pokynů Kupujícího. Při tom je Prodávající povinen upozorňovat Kupujícího na nevhodnost jeho pokynů, které by mohly mít za následek újmu na právech Kupujícího nebo vznik újmy. Pokud Kupující i přes upozornění Prodávajícího na splnění svých pokynů trvá, Prodávající neodpovídá za případnou újmu tím vzniklou.

5.4 Prodávající je oprávněn k plnění této Smlouvy použít jiných třetích osob, než uvedl ve své nabídce v Zadávacím řízení, jen s předchozím písemným souhlasem Kupujícího.

5.5 Prodávající není oprávněn bez předchozího písemného souhlasu Kupujícího (i) provádět jakékoli zápočty svých pohledávek za Kupujícím z této Smlouvy proti jakýmkoli pohledávkám Kupujícího za Prodávajícím ani (ii) postupovat jakákoli svoje práva a pohledávky z této Smlouvy za Kupujícím na jakoukoli třetí osobu.

5.6 V případě, že se vyskytne jakákoli překážka, zejména

(i) prodlení Kupujícího s poskytnutím objektivně nezbytné součinnosti, které by podmiňovalo plnění Prodávajícího,

(ii) mimořádná nepředvídatelná a nepřekonatelná překážka vzniklá nezávisle na vůli Prodávajícího, jak je vymezena v ustanovení § 2913 odst. 2 Občanského zákoníku,

která by mohla mít jakýkoli dopad na řádné a včasně splnění této Smlouvy, má Prodávající povinnost o této překážce Kupujícího písemně informovat, a to nejpozději do 3 kalendářních dnů od okamžiku, kdy se tato překážka vyskytla. Pokud Prodávající Kupujícího v této 3denní lhůtě o překážkách písemně neinformuje, zanikají veškerá práva Prodávajícího, která se na existenci příslušné překážky váží, zejména Prodávající nebude mít nárok na jakékoli posunutí termínů plnění této Smlouvy.

6 ODPOVĚDNOST ZA VADY A ZÁRUKA ZA JAKOST

6.1 Prodávající odpovídá za to, že dodávaný Systém proti bezpečnostním hrozbám bude prostý jakýchkoliv vad a plně funkční po dobu platnosti maintenance, a po tuto dobu poskytuje záruku za jakost ve smyslu § 2113 Občanského zákoníku.

6.2 Smluvní strany se dohodly, že Kupující je oprávněn vytknout vady Systému proti bezpečnostním hrozbám kdykoli v průběhu doby platnosti maintenance a oproti § 2099 až 2117 Občanského zákoníku pozdější uplatnění práva z vadného plnění nemůže zakládat žádné negativní účinky, omezení či zánik jeho práva, které tato ustanovení předvídají.

6.3 Vadou se rozumí stav, kdy funkce, jakost nebo množství Systému proti bezpečnostním hrozbám není v souladu s § 2095 a § 2096 Občanského zákoníku a/nebo s podmínkami specifikovanými v této Smlouvě.

6.4 Prodávající je povinen na své náklady odstranit veškeré vady dodaný Systém proti bezpečnostním hrozbám, které Kupující vytkne kdykoliv během doby platnosti, a to tak, že nedohodnou-li se Smluvní strany v jednotlivém případě jinak, Prodávající odstraní vytknuté vady do dvou pracovních dnů ode dne jejich vytknutí.

7 SANKCE

7.1 V případě prodlení Kupujícího s platbou ceny je Kupující povinen uhradit Prodávajícímu zákonný úrok z prodlení.

7.2 V případě, že Prodávající poruší svou povinnost dodat Systém proti bezpečnostním hrozbám dle podmínek stanovených touto Smlouvou a v termínu dle čl. 3.4 této Smlouvy zaplatí Kupujícímu smluvní pokutu ve výši 1.000 Kč za každý započatý den prodlení.

7.3 V případě, že Prodávající poruší svou povinnost uvedenou v čl. 5.4 této Smlouvy (neoprávněné plnění prostřednictvím třetích osob), zaplatí Kupujícímu smluvní pokutu ve výši 10.000 Kč za každé takové porušení.

7.4 V případě, že Prodávající poruší svou povinnost dodat či zajistit Kupujícímu veškerá oprávnění nezbytná k řádnému užívání Systému proti bezpečnostním hrozbám dle čl. 2 této Smlouvy, zaplatí Kupujícímu smluvní pokutu ve výši 20.000 Kč za každý jednotlivý případ porušení této povinnosti.

7.5 V případě, že Prodávající neodstraní jakoukoli vadu uvedenou v Předávacím protokolu ve lhůtě dle čl. 3.3 této Smlouvy a/nebo neodstraní jakoukoli vytknutou vadu ve lhůtě podle článku 6.4. této Smlouvy, zaplatí Kupujícímu smluvní pokutu ve výši 1.000 Kč za každou vadu a za každý i započatý den prodlení.

7.6 Smluvní pokuty stanovené dle tohoto článku jsou splatné do 30 dnů ode dne doručení výzvy k zaplacení smluvní pokuty povinné Smluvní straně.

7.7 Smluvní strany odchylně od ustanovení § 2050 Občanský zákoník sjednaly, že zaplacením jakékoli smluvní pokuty podle této Smlouvy není dotčena povinnost Prodávajícího nahradit Kupujícímu v plné výši též škodu vzniklou porušením povinnosti, na kterou se smluvní pokuta vztahuje.

8 MOŽNOST UKONČENÍ SMLOUVY

8.1 Kupující je oprávněn odstoupit od této Smlouvy v případě, že se Prodávající dostane do prodlení s plněním této Smlouvy po dobu delší než 10 dní oproti termínům dle čl. 3.4 této Smlouvy a nezjedná nápravu ani do 5 kalendářních dní od doručení písemné výzvy Kupujícího.

8.2 Prodávající je oprávněn odstoupit od této Smlouvy pouze v případě, že se Kupující dostane do prodlení s platbou ceny po dobu delší než 45 kalendářních dnů a nezjedná nápravu ani do 5 kalendářních dnů od doručení písemné výzvy Prodávajícího k nápravě.

8.3 Odstoupení od této Smlouvy je účinné okamžikem doručení písemného oznámení o odstoupení druhé Smluvní straně.

8.4 Ukončením této Smlouvy nejsou dotčena ujednání týkající se (i) smluvních pokut, (ii) práva na náhradu škody vzniklé z porušení smluvní povinnosti a (iii) ujednání týkající se takových práv a povinností, z jejichž povahy vyplývá, že mají trvat i po ukončení této Smlouvy.

9 OPRÁVNĚNÉ OSOBY

9.1 Komunikace mezi Smluvními stranami bude probíhat zejména prostřednictvím následujících oprávněných osob, pověřených pracovníků nebo statutárních zástupců Smluvních stran:

9.1.1 Oprávněnými osobami Kupujícího jsou:

jméno:	Ing. Luděk Chaloupka
adresa:	Nám. 14. října 1381/4, 150 00 Praha 5
telefon:	+420 257 000 583
e-mail:	ludek.chaloupka@praha5.cz

9.1.2 Oprávněnými osobami Prodávajícího jsou:

jméno:	Mgr. Ondřej Dedek
adresa:	Na hřebenech II 1718/10, Nusle, 140 00 Praha 4
telefon:	[redacted]
e-mail:	

9.2 Oprávněné osoby, nejsou-li statutárním orgánem, nejsou oprávněny ke změnám této Smlouvy, jejich doplňkům ani zrušení, ledaže se prokáží plnou mocí udělenou jim k tomu osobami oprávněnými jednat navenek za příslušnou Smluvní stranu v záležitostech této Smlouvy. Smluvní strany jsou oprávněny jednostranně změnit oprávněné osoby, jsou však povinny takovou změnu příslušné Smluvní straně bezodkladně písemně oznámit.

9.3 Všechna oznámení mezi Smluvními stranami, která se vztahují k této Smlouvě nebo která mají být učiněna na základě této Smlouvy, musí být učiněna písemně a druhé straně doručena buď osobně nebo doporučeným dopisem či jinou formou registrovaného poštovního styku nebo e-mailem s použitím elektronického podpisu na adresu uvedenou v záhlaví této Smlouvy nebo čl. 9.1 této Smlouvy, není-li stanoveno nebo mezi Smluvními stranami dohodnuto jinak.

10 ZÁVĚREČNÁ UJEDNÁNÍ

10.1 Vyjma změn oprávněných osob podle čl. 9.1 této Smlouvy mohou veškeré změny a doplňky této Smlouvy být provedeny pouze po dosažení úplného konsenzu na obsahu změny či doplňku, a to písemným dodatkem k této Smlouvě podepsaným oběma Smluvními stranami. Smluvní strany vylučují možnost uzavření dodatku bez ujednání o veškerých náležitostí dle § 1726 Občanského zákoníku. Smluvní strany rovněž vylučují použití § 1740 odst. 3 a § 1757 odst. 2 Občanského zákoníku.

10.2 Prodávající tímto výslovně prohlašuje, že v souladu s § 1765 odst. 2 Občanského zákoníku na sebe bere nebezpečí změny okolností.

10.3 Tato Smlouva a všechny vztahy z ní vyplývající se řídí právním řádem České republiky. Obchodních podmínek kterékoli Smluvní strany se použije, pouze pokud to tato Smlouva, resp. její dodatky stanovují. V případě jakéhokoli rozporu bude mít přednost vždy ustanovení této Smlouvy ve znění případných dodatků.

10.4 Spor, který vznikne na základě této Smlouvy nebo který s ní souvisí, se Smluvní strany zavazují řešit přednostně smírnou cestou, pokud možno do 30 dní ode dne, kdy o sporu jedna Smluvní strana uvědomí druhou Smluvní stranu. Jinak jsou pro řešení sporů z této Smlouvy příslušné obecné soudy České republiky.

10.5 V případě, že některé ujednání této Smlouvy je nebo se stane v budoucnu neplatným, neúčinným či nevymahatelným nebo bude-li takovým příslušným orgánem shledáno, zůstávají ostatní ujednání této Smlouvy v platnosti a účinnosti, pokud z povahy takového ujednání nebo z jeho obsahu anebo z okolností, za nichž bylo uzavřeno, nevyplývá, že je nelze oddělit od ostatního obsahu této Smlouvy. Smluvní strany se zavazují nahradit neplatné, neúčinné nebo nevymahatelné ujednání této Smlouvy ujednáním jiným, které svým obsahem a smyslem odpovídá nejlépe ujednání původnímu a této Smlouvě jako celku.

10.6 Tato Smlouva je vyhotovena ve čtyřech stejnopisech, kdy každé ze stran náleží dva.

10.7 Smluvní strany berou na vědomí, že k nabytí účinnosti této Smlouvy je nezbytné její uveřejnění v Registru smluv podle § 5 odst. 2) zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv, ve znění pozdějších předpisů, a to bezodkladně nejpozději však ve lhůtě do 30 dnů ode dne podpisu smlouvy poslední smluvní stranou, které provede Městská část Praha 5. Smluvní strany berou na vědomí, že uveřejnění osobních údajů ve Smlouvě uveřejněné v Registru smluv podle věty první se děje v souladu s tímto zákonem a s čl. 6 odst. 1) písm. c) nařízení Evropského parlamentu a Rady (EU) 2016/679. Smluvní strany prohlašují, že skutečnosti obsažené ve smlouvě nepovažují za obchodní tajemství ve smyslu § 504 občanského zákoníku a udělují svolení k jejich užití a uveřejnění bez stanovení jakýchkoliv dalších podmínek.

10.8 Smlouva včetně příloh bude uveřejněna dle platných právních předpisů.

10.9 Nedílnou součástí této Smlouvy jsou následující přílohy:

Příloha č. 1: Technická specifikace systému pro identifikaci a zastavení pokročilých bezpečnostních hrozeb

V případě rozporu mezi textem této Smlouvy a textem přílohy má přednost ujednání této Smlouvy.

10.10 Tímto se ve smyslu ustanovení § 43 odst. 1 zákona č. 131/2000 Sb., o hlavním městě Praze, ve znění pozdějších předpisů, potvrzuje, že byly splněny podmínky pro platnost právního jednání městské části Praha 5, a to usnesením RMČ č. 33/918/2022 ze dne 25. 07. 2022.

10.11 Smluvní strany prohlašují, že si tuto Smlouvu přečetly, že s jejím obsahem souhlasí a na důkaz toho k ní připojují své podpisy.

V Praze dne 03 -08- 2022
za Městskou část Praha 5

[redacted]

Podpis: [redacted]
J[redacted] Renáta Zajíčková
P[redacted]ostka

[redacted]

V Praze dne 28.7.2022
za ICZ a.s.

[redacted]

Podpis: [redacted]
Jméno: Ing. Marian Arbet
Funkce: ředitel sekce Infrastruktura

[redacted]

PŘÍLOHA Č. 1
Technická specifikace systému pro identifikaci a zastavení pokročilých bezpečnostních hrozeb

Systém pro identifikaci a zastavení pokročilých bezpečnostních hrozeb – Fidelis Elevate.

Technická specifikace je uvedena na následujících stranách.

Oblast Analýza síťového provozu (network)

NDR	Požadavky na systém/funkčnost síťového prostředí			
A	**Základní požadavky na funkčnost části systému pro analýzu síťového provozu:**		**Splňuje požadavky ANO/NE**	**popis jak**
1	Vyšetřování	Vestavěná funkcionalita pro vyšetřování, shromáždění indicií a vygenerování reportu o incidentu	ANO	Nabízený systém Fidelis Elevate je navržen jako integrovaná vyšetřovací, detekční a reakční platforma s podporou také pro hunting. Pokročilý reporting, včetně vestavěného editoru reportů, je součástí systému.
2	Vyšetřování	Kontinuální záznam informací o síťové komunikaci v podobě, která umožní její pozdější analýzu	ANO	Síťový provoz je neselektivně a kontinuálně popisován v podobě metadat a tato metadata jsou uchovávána po určenou dobu retence.
3	Rozhraní	Systém poskytuje webové uživatelské rozhraní pro analýzu zaznamenaného provozu bezpečnostními specialisty, které bude součástí jednotného uživatelského rozhraní	ANO	Systém poskytuje jednotné webové uživatelské rozhraní.
4	Detekce	Analýza síťového provozu v rámci systému probíhá pro veškerý síťový provoz a bez ohledu na použité komunikační protokoly a monitorována a analyzována jsou tedy všechna probíhající spojení na všech síťových portech	ANO	Systém využívá vlastní senzory a analyzuje veškerý IP provoz bez ohledu na použitý protokol a číslo portu.
5	Vyšetřování	K dispozici jsou historické informace o provozu s určenou dobou retence pro následnou analýzu	ANO	Metadata a alerty jsou historickou informací, kterou lze využít pro analýzu a vyšetřování.
6	Vyšetřování	Schopnost průběžně zaznamenávat a retrospektivně analyzovat informace o veškerém dění na síti se záznamem: - IP adresy a jejich geolokace - identity uživatele (například emailové adresy pro SMTP/POP3/IMAP a web-mailová rozhraní nebo uživatelského jména pro další protokoly) - čísla portů - skutečný rozpoznaný typu protokolu	ANO	Všechny uvedené údaje jsou zaznamenávány jako atributy v metadatech. Celkové množství atributů je několik set různých typů.

		- parametry rozpoznatelných komunikačních protokolů (například hlavičky SMTP, HTTP, ...) - typ přenášených souborů (alespoň excel, word, powerpoint, pdf, exe, msi, obrázkové formáty, archivní a komprimační formáty, a to včetně vzájemně vnořených) - HASH přenášených souborů - velikost přenášených souborů - jméno a přípona přenášených souborů - informace o tom, že je soubor šifrován a obecně informace o entropii obsahu souborů - čas a délka spojení - objem přenesených dat		
7	Vyšetřování	Záznam popisu síťového provozu bude obsahovat údaje o: - protokolu spojení a jeho parametrech, minimálně pak: -- pro http atributy - URL, příkaz, referer, status code, user agent, x-forwarded-for, host -- pro SMTP atributy - from, to, response code, user a pro MIME obálky pak – from, to, message-id, reply-to, return-path, subject -- pro POP3 – user -- pro IMAP – user, from, to, subject -- pro FTP – command, mode, filename -- pro TLS – SNI, JA3, JA3S a atributy certifikátu použitého pro vystavení spojení -- uchazeč uvede další protokoly, které jsou při analýze síťového provozu rozpoznány a sadu atributů, které jsou pro ně generovány. - přenášených souborech jakýmkoliv protokolem - alespoň jejich jména, velikost, hash a informaci o skutečném typu souboru bez ohledu na příponu jeho jména, -- v případě archivů nebo vložených (embedovaných) souborů bude popis obsahovat také jejich	ANO	Všechny uvedené údaje jsou zaznamenávány jako atributy v metadatech. Analýza je prováděna nad celým obsahem spojení a v případě kompozitních dokumentů je prováděna opakovaně pro vložený obsah bez omezení počtu úrovní.

		parametry, a to do libovolné hloubky vnoření.		
8	Vyšetřování	Zaznamenané informace o provozu umožní vyhledávání spojení dle libovolného atributu popisujícího spojení nebo pomocí logického výrazu s relačními operátory odkazujícího se na atributy spojení	ANO	Vyhledávání je možné s využitím logických výrazů a relačních operátorů odkazujících se na atributy a jejich hodnoty.
9	Detekce	Detekce malware přenášeného jakýmkoliv nešifrovaným protokolem	ANO	Systém podporuje množství detekčních metod cílených na známý i neznámý malware (signatury, heuristika, korelace událostí, ML/AI, pravidla)
10	Detekce	Podpora spolupráce s TLS/SSL Visibility řešeními pro možnost inspekce provozu přenášeného šifrovaným spojením	ANO	Podporována je spolupráce s vlastním Fidelis TLS dešifrátorem i s dešifrátory třetích stran.
11	Detekce	Detekce zpětných volání malware typu Command&Control	ANO	Pomocí pravidel, analýzou provozu a reputací IP adres.
12	Detekce	Detekce projevů RAT (Remote Access Tool)	ANO	Pomocí pravidel, analýzou provozu.
13	Detekce	Detekce pokusů vzdáleně po síti zneužít zranitelnosti	ANO	Pomocí pravidel, analýzou provozu.
14	Detekce	Detekce malware zabaleného i hluboko v obsahu (v archivech a jiných složených dokumentech)	ANO	Technologie DSI (Deep Session Ispection) aplikuje detekční metody malware i na kompozitní/vložený obsah.
15	Detekce	Identifikace spojení využívajících neočekávané nebo neznámé protokoly (například nesoulad portu a protokolu)	ANO	Systém rozpoznává protokoly bez ohledu na použité porty a je schopen rozpoznat neshodu.
16	Detekce	DLP pro detekci exfiltrace a zamezení úniku informací schopné nasazení do prostředí s klasifikačními značkami i bez nich	ANO	Síťová DLP funkcionalita je součástí funkcionalit systému. Pravidla umožňují rozpoznat určený obsah (číslo platební karty, rodné číslo, adresa, ...) v dokumentech nebo obecné komunikaci.
17	Detekce	DLP funkcionalita informace přenášené i hluboko v obsahu, bez ohledu na hloubku vložení a bez ohledu na souborový formát	ANO	Technologie DSI (Deep Session Ispection) aplikuje DLP funkcionalitu i na kompozitní/vložený obsah.
18	Detekce	Možnost definovat vlastní pravidla detekce nad veškerým typem přenášeného obsahu, charakteristikami chování, nebo posloupnosti dějů v síti	ANO	Systém není blackbox. Veškerý threat-intel je editovatelný a viditelný ve srozumitelné podobě, včetně možnosti tvorby vlastních pravidel.

19	Detekce	Systém bude schopný aplikovat právě aktualizované signatury na historický provoz sítě a nalézt tak nyní již známý malware, který nebyl detekován v minulosti	ANO	Pomocí pravidel pracujícími nad metadaty (tzv. kolektorová analytika)
20	Detekce	Detekce malware je prováděna pomocí: signatur a pravidel heuristickou analýzou vyhledáváním typického chování (behavioral analýza) detekcí na sandboxu virtuálním provedením detekcí anolámií	ANO	Všechny uvedené detekční metody jsou podporovány a implementovány.
21	Detekce	Detekce anomálií pomocí Machine Learning modelů a případně generování alarmů pro významné anomálie	ANO	Systém vyhodnocuje cca 25 Machine Learning modelů, které jsou schopné rozpoznat anomálie v určité oblasti. Tato detekční metoda je schopna generovat alerty pro vybrané ML modely.
22	Detekce	Pravidla pro analýzu provozu umožní definovat podmínky odkazující se na přenášený obsah a parametry aplikační vrstvy – například odhalit přenášené soubory, kde koncovky soborů nesouhlasí s obsahem, nebo čísla typických portů nesouhlasících s typem rozpoznaného komunikačního protokolu	ANO	Systém rozpoznává síťové protokoly i typy přenášených souborů. Toto umožňuje tvorbu pravidel, která rozpoznají uvedené situace.
23	Detekce	Schopnost definovat pravidla hledající souběh událostí nebo posloupnost událostí v síťovém provozu a generovat upozornění (alerty) a to kontinuální analýzou okamžitého dění i analýzou již uložených historických záznamů o provozu zpětně	ANO	Pravidla mohou pracovat nad okamžitým provozem a reagovat na něj, včetně možné prevence, nebo nad historickými metadaty a hledat v nich posloupnosti určitých jevů.
24	Ostatní	Součástí dodávky je kontinuální služba aktualizace signatur/definic chování malware a aktualizace pravidel sandboxu z komerčního zdroje	ANO	Aktualizace threat-intel je součástí služby produktové podpory.
25	Vyšetřování	Systém musí v oblasti detekce a vyšetřování útoků typu APT splňovat požadavek viditelnosti stop daného útoku a dostupnosti forenzních dat ze všech zachytitelných fází APT útoku (dle	ANO	Splněno neselektivním záznamem metadat a detekčními metodami cílícími na všechny fáze kill-chain.

		fází kill-chain – od iniciální kompromitace do ex-filtrace dat)		
26	Detekce	Retrospektivní analýza zaznamenaných dat o chování sítě za účelem odhalení posloupnosti událostí vedoucích k projevu kybernetického incidentu	ANO	Analýza je možná manuálně (např. hunting) nad metadaty nebo automatizovaně pomocí kolektorové analytiky.
27	Detekce	Schopnost definovat pravidla (komunikační matice) pro vyhodnocení, zda se jedná o legitimní odchozí komunikace vůči definovaným kritickým informačním systémům pomocí kombinací parametrů: - IP adresa/Seznam IP adres/Adresní rozsah - Skutečně rozpoznaný typ protokolu (nezávisle na definovaném čísle portu TCP/UDP) - Čísla portů (TCP/UDP)	ANO	Komunikační matici lze odrazit ve vlastní politice (zde vlastně sada pravidel), která bude vyhodnocovat soulad provozu s definovanými pravidly.
28	Vyšetřování	Systém asociuje informace o uživatelských účtech se spojeními	ANO	Systém zaznamenává informaci o uživateli jako atribut spojení.
29	Detekce	Schopnost systému identifikovat specifické komunikační protokoly nacházející se v provozu organizace Zadavatele. - Možnost takto identifikovaný protokol zahrnout do definice detekčních pravidel.	ANO	Je možné zavést vlastní „rozpozávač" protokolu a ten využít pro vlastní pavidla.
B	**Požadované funkcionality v oblasti otevřenosti systému analýzy sítového provozu:**		**Splňuje požadavky ANO/NE**	**popis jak**
1	Rozhraní	Dokumentované aplikační rozhraní pro zákaznické integrace s dalšími bezpečnostními komponentami. Preferujeme http & XML nebo JSON API rozhraní	ANO	RESTful API s JSON
2	Rozhraní	Předpřipravené integrační vazby na aplikace typu SIEM	ANO	Předpřipravené konektory pro ArcSight, Qradar, Splunk a některé další, včetně generických. konfigurovatelných.
3	Detekce	Možnost importu detekčních pravidel s podporou formátů YARA a zdrojů dle specifikace TAXII/STYX	ANO	Tyto formáty jsou podporovány.

4	Vyšetřování	Export plného záznamu pravidly předem popsané síťové komunikace ve formátu PCAP pro další vyšetřování	ANO	Volitelnou součástí alertů může být i PCAP komunikace v čase „okolo" alertu.
5	Detekce	Možnost importu plného záznamu síťového provozu k provedení jeho inspekce, popsání a hluboké analytice	ANO	Je možné naimportovat zaznamenaný PCAP a nechat systém jej analyzovat.
6	Vyšetřování	Extrakce obsahu souborů zachycených při jejich pohybu na síti pro forensní účely pomocí konsole systému	ANO	Forenzní data jsou součástí alertů a lze je uložit do souboru.
7	Rozhraní	Systém musí být schopen integrací s EDR/EPP řešením spouštět vyšetřovací nebo remediační úlohy na koncových bodech	ANO	Podporováno s Fidelis Endpoint.
8	Rozhraní	Systém je připraven na integraci funkcionalit spojených s návnadami (honeypots/Deception)	ANO	Podporováno s Fidelis Deception.
9	Ostatní	Systém musí podporovat práci v hierarchickém režimu (včetně selektivního řízení práv k informacím) pro případné budoucí zahrnutí podřízených organizací do bezpečnostního dohledu	ANO	Systém lze postavit jako hierarchický s podřízenými a nadřízenými konzolemi.
C	**Ostatní požadavky na vlastnosti části systému pro bezpečnostní monitorování síťového provozu**		**Splňuje požadavky ANO/NE**	**popis jak**
1	Ostatní	Systém je platforma pro forenzní analytiku, detekci, vyšetřování a řízení reakcí na zaznamenané kybernetické události	ANO	Zaměření systému pokrývá požadované oblasti.
2	Ostatní	Celková požadovaná retence všech historických dat o chování sítě v délce 30 dnů	ANO	Bude promítnuto do návrhu sizingu zdrojů na straně Zadavatele a licencování systému.
3	Reakce	Schopnost automatizace pracovních postupů při nápravě kybernetických incidentů: - plně automatická reakce definovaná bezpečnostní politikou pro síťový provoz (DROP při in-line zapojení, nebo TCP Reset pro out-of-band připojení)	ANO	Systém je schopen takové automatické prevence/reakce.
4	Vyšetřování	Systém podporuje efektivitu vyšetřování tím, že dokáže automatizovaně spojovat jednotlivé bezpečnostní události, které mají společnou příčinu, do jedné události (incidentu)	ANO	Systém sdružuje alerty odpovídající jednomu incidentu do tzv. Conclusions.

5	Detekce	Import popisu hrozeb (Threat Intel) od třetích stran a vlastních, které mohou být dodány ve formátech STIX, TAXII, CSV (podpora ThreatConnect)	ANO	Uvedené formáty jsou podporovány.
6	Vyšetřování	Vestavěná podpora pro řízení životního cyklu tiketů pro distribuci úkolů mezi uživatele systému/vyšetřovatele	ANO	Alerty mají vlastnosti tiketů – lze je přiřadit uživateli a řídit jejich životní cyklus.
7	Rozhraní	Dashboard a možnosti jeho úprav pro grafické zobrazení informací a podpory rozhodovacího procesu (alert triage)	ANO	Dashboard je upravitelný výběrem a parametrizací widgetů a graficky prezentuje vybrané údaje.
8	Ostatní	Generování reportů dle předpřipravených šablon	ANO	Podporováno reporting funkcionalitou.
9	Ostatní	Tvorba a generování zákaznicky definovaných reportů	ANO	Dostupný vestavěný editor reportů.
10	Ostatní	Možnost nastavení automatického generování a odesílání reportů na emailové adresy	ANO	Pomocí definice časového rozpisu generování reportů a jejich odesílání na určené adresy.
11	Detekce	Whitelisting pravidla pro vyloučení určité komunikace z inspekce daným pravidlem	ANO	Whiotelisting je podporován tvorbou vlastních indikátorů a jejich přiřazením pravidlu jako whitelistu.
12	Vyšetřování	Geolokace komunikujících stran	ANO	Vestavěná mapovací tabulka.
13	Vyšetřování	Možnost vlastní definice geolokačních tabulek IP adres (pro geolokaci privátní IP segmentů)	ANO	Importem vlastní mapovací tabulky IP rozsahů na lokality.
14	Rozhraní	Možnost detailního řízení přístupových práv pro více úrovní pracovníků SOC (analytici, operátoři, IT podpora, forenzní analytici, vyšetřovatelé)	ANO	Granulárním RBAC a definicí vlastních rolí.
15	Rozhraní	Možnost napojení na ActiveDirectory/LDAP pro autentizaci uživatelů systému.	ANO	Podporováno, včetně obecného LDAP serveru.
16	Rozhraní	Jednotné uživatelské rozhraní pro veškerou analytiku, vyšetřování a reakci	ANO	Systém poskytuje jednotné rozhraní.
17	Ostatní	Systém monitoruje svůj vnitřní chod a drží historické informace o událostech týkající se vlastního chodu a problémů	ANO	Vlastní provozní události jsou drženy systémem a je možné je zobrazit ve webovém rozhraní.
18	Ostatní	Podpora instalace jednotlivých komponent řešení do virtuálního prostředí (VMware)	ANO	VMware je podporován jako provozní platforma až do 5 Gbps monitorovaného provozu.
19	Ostatní	Funkcionalita analýzy a záznamu síťového provozu pracuje nad zrcadleným provozem sítě	ANO	Toto je možný režim nasazení senzorů. In-line režim je také podporován.

20	Reakce	Schopnost ukončit spojení na základě detekce	ANO	Systém má prevenční vlastnosti a umožňuje ukončit spojení pomocí TCP reset paketů s podvrženými IP adresami.
21	Reakce	Schopnost umísit škodlivý email do karantény	ANO	Pokryto vlastnostmi Mail senzoru.
22	Detekce	Systém musí klasifikovat události podle MITRE ATT&AC frameworku uvedením odpovídající techniky a/nebo taktiky útočníka - Vlastní pravidla lze definovat tak, aby také používali kategorie MITRE ATT&CK frameworku	ANO	Alerty jsou kategorizovány dle technik a taktik MITRE ATT&CK frameworku. Vlastní pravidla také podporují tuto kategorizaci.

Oblast Bezpečnost koncových bodů (EDR)

EDR	**Požadavky na systém/funkčnost pro část ochrany koncových bodů (EDR)**			
A	**Základní požadavky na funkčnost části systému pro bezpečnostní monitorování koncových bodů:**		**Splňuje požadavky ANO/NE**	**popis jak**
1	Detekce	Pokročilá detekce hrozeb: - detekce škodlivého kódu jeho rozpoznáním podle vzorů pro obsah - detekce škodlivého kódu pomocí pravidel popisující chování, - detekce projevů činnosti útočníka na koncovém bodě, - analýza běžících procesů na stanici a jejich ohodnocení z hlediska činností, které provádějí nebo by mohly provádět.	ANO	Uvedené detekční metody jsou podporovány.
2	Vyšetřování	Systém bude kontinuálně a centrálně zaznamenávat činnosti na koncových bodech v podobě meta-dat v těchto oblastech: - spuštění a ukončení procesů, - souborové manipulace, - manipulace s registry,	ANO	Uvedené děje jsou kontinuálně popisovány v metadatech a uchovávány s požadovanou retencí. Metadata obsahují uvedené údaje jako atributy.

		- síťových spojení včetně URL pro http spojení, - DNS překladů, - Manipulace s USB médii a přenosy souborů na ně, - Windows události (Windows Events).		
3	Reakce	Systém umožní provedení akce na koncovém bodě nebo bodech odesláním úlohy k provedení a také interakcí s koncovým bodem v reálném čase	ANO	Systém podporuje asynchronní úlohy i konzolový přístup v reálném čase.
4	Reakce	Automatizace reakce na incidenty: - automatickým spouštěním akcí (nachystaných i uživatelem definovaných) na koncových bodech v případě výskytu určitého alarmu, který se ke koncovému bodu vztahuje.	ANO	Pomocí tvz. Playbooků.
5	Reakce	Ochrana koncového bodu: - Zabránění spuštění procesu dle hashe	ANO	Pokryto funkcionalitou Process Blocking
6	Reakce	- Ukončení procesu na základě vyhodnocení pravidla nad metadaty z koncového bodu	ANO	Pokryto funkcionalitou Behavior (Detection) pravidel.
7	Ostatní	Základní systémová správa koncových bodů: - správa uživatelů, - instalace a odinstalace aplikací, - změna nastavení operačního systému (například zapnutí firewallu a AV).	ANO	Pomocí úloh.
B	**Požadavky v oblasti otevřenosti platformy:**		**Splňuje požadavky ANO/NE**	**popis jak**
1	Rozhraní	Dokumentované standardizované aplikační rozhraní pro zákaznické integrace s dalšími bezpečnostními komponentami. Preferujeme http & XML nebo JSON API rozhraní	ANO	RESTful API s JSON dokumenty
2	Rozhraní	Předpřipravené integrační vazby na aplikace typu SIEM	ANO	Podporovány jsou ArcSight, Qradar a formáty CEF a LEEF.
3	Rozhraní	Systém musí pro budoucí potřeby podporovat integraci s: - Komponenty pro detekci APT útoků na síťovém provozu (NDR/NTA) - Komponenty síťových návnad (honeypots)	ANO	Tyto integrační vazby jsou podporovány.

4	Ostatní	Systém bude napojen na zdroj aktualizovaných informací o hrozbách (threat-intelligence) a bude z toho zdroje provádět pravidelně aktualizace	ANO	Aktualizace threat-intel je součástí služby produktové podpory.
5	Ostatní	Systém bude možné napojit na vlastní nebo otevřené zdroje informací o hrozbách ve formátech JSON, CSV a STIX	ANO	Je možné zavést vlastní feedy s podporou uvedených formátů.
6	Ostatní	Systém bude umožňovat import popisu IOC ve formátu OpenIOC a YARA	ANO	Tyto formáty jsou podporovány.
C	**Ostatní požadavky na vlastnosti části systému pro bezpečnostní monitorování koncových bodů:**		**Splňuje požadavky ANO/NE**	**popis jak**
1	Ostatní	Systém musí podporovat koncové body s operačními systémy: - Windows 7 a výše - Windows Server 2008 R2 a výše - Linux CentOS 7 a výše - RedHat Enterprise Linux 7 a výše - macOS 10.12 a výše a to na Intel a M1 procesoru	ANO	Uvedené OS jsou podporovány Fidelis Endpoint agenty.
2	Ostatní	Na koncových stanicích musí agentská část využívat zanedbatelnou část zdrojů - agent by neměl překročit po většinu času jednotky (max. 4%) využití CPU	ANO	Agent průměrně využívá do cca 2% CPU.
3	Ostatní	Agent systému musí být odolný proti odinstalování a pokusům jej zastavit nebo poškodit.	ANO	Odinstalace je chráněna dalším heslem. Agent je schopen rozpoznat pokusy mu uškodit a je schopen znovu-zprovoznění své činnosti.
4	Ostatní	Agent bude komunikovat se systémem jedním šifrovaným a autentizovaným spojením vystavovaným ze strany agenta	ANO	Je použito jedno certifikátem autentizované TLS spojení.
5	Ostatní	Agent je schopen delegovat činnosti spojené s detekcemi na GPU (například Intel TDT technologie)	ANO	Podporováno od verze FE 9.5.
6	Ostatní	Odinstalace agentů musí vyžadovat zvláštní autentizaci (heslo pro odinstalaci).	ANO	Odinstalace je chráněna dalším heslem.
7	Ostatní	Události budou zaznamenávány do centrálního úložiště v reálném čase a budou zpětně dostupné s časovou retencí min. 30 dnů.	ANO	Toto není omezeno u EDR licencí. Sizing zdrojů Zadavatele bude navržen s vědomím této retence.

8	Ostatní	Systém musí být schopný zaznamenávat metadata o chování koncových bodů, alerty a výsledky úloh i pro koncové body, které jsou dočasně mimo síť, jejich uchováním na koncovém bodě až do jejich odeslání so systému alespoň po dobu 5 dní.	ANO	U případě off-line agenta jsou metadata jsou uložena do cache a odeslána po obnovení spojení.
9	Rozhraní	Alerty generované systémem musí být zobrazovány v centrální konzoli.	ANO	Pomocí integrace s Fidelis Network.
D	**Požadované funkcionality v oblasti viditelnosti, vyšetřování a analýzy na koncových bodech:**		**Splňuje požadavky ANO/NE**	**popis jak**
1	Vyšetřování	Systém musí být schopen nalézt soubor na disku koncovéhpo bodu dle: - obsahu - hashe - názvu - velikosti - koncovky - času vytvoření/modifikace - kombinace výše uvedeného	ANO	Pomocí parametrizace úlohy „Najdi soubor“.
2	Vyšetřování	Systém bude umožňovat vyhledávání souboru i pro smazané soubory	ANO	Pomocí parametrizace úlohy „Najdi soubor“.
3	Vyšetřování	Systém bude umožňovat vyhledávání souboru na souborovém systému, logickém i fyzickém disku v jejich využité (obsazené/alokované) i nevyužité části	ANO	Pomocí parametrizace úlohy „Najdi soubor“.
4	Vyšetřování	Systém bude pro běžící procesy schopen extrahovat: - otevřené sokety - souborové handle - informace o DDL, které byly dynamicky přilinkovány včetně informace, zda byly injektovány - obsazený virtuální adresní prostor	ANO	Pomocí úlohy pro analýzu běžících procesů.
5	Vyšetřování	Systém musí být schopen na vyžádání – nebo jako součást automatické reakce – získat informace o okamžitém stavu koncového bodu minimálně v oblastech: - Přihlášení uživatelé - Vystavená síťová spojení	ANO	Pomocí úloh, které jsou k dispozici pro všechny uvedené oblasti, včetně mnoha dalších. K dispozici je cca 200 předpřipravených typů úloh.

		- Běžící procesy - Seznam zavedených lokálních správců - Seznam nainstalovaného software - Seznam nainstalovaných důvěryhodných certifikátů - Čas od spuštění počítače - Stav antiviru - Stav firewallu - Seznam do paměti nahraných ovladačů - Seznam klíčů a hodnot autorun v registrech - Výpis obsahu DNS a APR vyrovnávacích pamětí - HW inventář - Obsah směrovací tabulky - Seznam aktivních síťových rozhraní		
6	Rozhraní	Systém bude umožňovat vyhledávání v metadatech dle libovolného parametru události (například jméno procesu, jméno rodiče, PID, hash, jméno souboru, jméno klíče v registrech, IP adresa serveru, URL spojení).	ANO	Pomocí prohledávání/filtrování metadat. Toto prohledávání lze provádět s využitím logických a relačních operátorů na atributy metadat.
7	Vyšetřování	Systém musí být schopný zobrazit činnosti určitého procesu ve vztahu k: - souborovým manipulacím - manipulacím s registry - síťovým spojením - spuštěným podprocesům - to vše ideálně na časové ose	ANO	K procesu jsou zaznamenávány také jeho souborové, registrové, síťové a další činnosti (vzdálená vlákna).
8	Vyšetřování	Forenzní analýza: - vzdáleně – získáním obrazu paměti nebo určitého procesu, - vzdáleně – získáním obrazu disku, - záznamem činnosti operačního systému a aplikací	ANO	Pokryto úlohami a sběrem metadat.
E	**Požadované funkcionality v oblasti odpovědi na hrozbu na koncových bodech:**		**Splňuje požadavky ANO/NE**	**popis jak**
1	Reakce	Systém musí umožnit na stanici: - Smazat soubor - Ukončit proces	ANO	Pomocí úloh.

		- Síťová izolace koncového bodu (při zachování komunikace systému s agentem na koncovém bodě) - Modifikace/mazání obsahu registrů - Instalace a odinstalace aplikací a záplat - Odhlášení uživatele - Zapnutí a vypnutí firewallu - Restartování, vypnutí a hibernace koncového bodu		
2	Reakce	Systém musí být schopen automatického spuštění vybrané akce jako automatické odpovědi na určitý alert.	ANO	Pomocí tzv. Playbooků.
3	Reakce	Schopnost agenta systému provádět více akcí současně.	ANO	Agent provádí více činností současně.
4	Reakce	Systém musí umožnit přístup ke koncovému bodu pomocí sezení v reálném čase (konzolový přístup) pro účely vyšetřování a remediace.	ANO	Pokryto tzv. LiveConsole.
5	Reakce	Systém musí umožnit zobrazení běžících procesů na koncovém bodě v reálném čase a základní manipulaci s nimi – například jejich ukončení a získání obrazu paměti procesu.	ANO	Pokryto LiveProcesses.
6	Reakce	Systém musí umožnit zobrazení vzdáleného souborového systému koncového bodu a základní manipulace se soubory – například získání souboru, smazání souboru.	ANO	Pokryto LiveFiles.
7	Reakce	Automatizace reakce na incidenty: - automatickým spouštěním akcí (nachystaných i uživatelem definovaných) na koncových bodech v případě výskytu určitého alarmu, který se ke koncovému bodu vztahuje.	ANO	Pomocí tzv. Playbooků.
F	**Požadované funkcionality v oblasti klasifikace události podle MITRE ATT&AC framework:**		**Splňuje požadavky ANO/NE**	**popis jak**
1	Ostatní	Systém musí klasifikovat události podle MITRE ATT&AC frameworku uvedením odpovídající techniky a/nebo taktiky útočníka:	ANO	Alerty jsou kategorizovány dle taktik a technik definovaných MITRE ATT&CK.
2	Ostatní	Vlastní pravidla lze definovat tak, aby také používali kategorie MITRE ATT&CK frameworku	ANO	Vlastní pravidla umožňují kategorizaci jimi generovaných alertů dle MITRE ATT&CK.

3	Detekce	Systém musí rozpoznat zranitelnosti nainstalovaného software na koncových bodech.	ANO	Systém porovnává nainstalovaný software s CVE databází a generuje tabulku se zranitelnostmi.

Oblast Návnady a pasti (Honeypots)

HP	**Požadavky na systém/funkčnost pro část návnad a pastí (Honeypots)**			
A	**Základní požadavky na funkčnost části systému pro analýzu prostředí a vytváření pastí**		**Splňuje požadavky ANO/NE**	**popis jak**
1	Detekce	Brzká detekce infikovaných zařízení uvnitř organizace pokrytím následujících případů užití: 1) Detekce laterálního pohybu 2) Vnitřní útočník 3) Ukradené přihlašovací údaje 4) Man-in-the-Middle 5) Ransomware 6) Útoky na IP tiskárny, úložiště a síťové prvky 7) Hunting a reakce na útok	ANO	Fidelis Deception modul je cílen na uvedené případy užití, včetně některých dalších (budování asset profilů, analytika nad odchozím a příchozím provozem, ...)
2	Vizibilita	Klasifikace a profilování zařízení v síti vytvářením profilů zařízení na základě analýzy síťového provozu, tedy bez instalace agentů na koncové body.	ANO	Systém vytváří tzv. Terrain a to poslechem síťového provozu.
3	Vizibilita	Rozpoznání spojení na aktualizační služby (například Windows Update, Linux APT feeds, ...)	ANO	Analýzou odchozího provozu.
4	Nasazení	Realizace v podobě hardwarové nebo virtuální appliance schopné realizovat stovky pastí v desítkách VLANů	ANO	Jedno zařízení je schopno realizovat až 1000 emulovaných pastí.
5	Nasazení	Podpora připojení appliance trunkem i porty bez VLAN tagování	ANO	VLAN tagging je podporován.
6	Nasazení	Emulované pasti bez nutnosti spouštění virtuálních strojů pro jejich realizaci	ANO	Podporovány jsou emulované pasti i pasti založené na skutečných operačních systémech.
7	Nasazení	Pasti založené na skutečných operačních systémech spouštěných v rámci virtuálních strojů	ANO	Podporovány jsou emulované pasti i pasti založené na skutečných operačních systémech.
8	Nasazení	Vlastní instalační obraz na pasti - Systém umožní nasazení vlastního pre-loadu operačního systému organizace na pasti	ANO	Past je možné založit na vlastní image operačního systému.

9	Nasazení	Pasti jako docker kontejnery	ANO	Past je možné nasadit i jako docker kontejner.
10	Nasazení	Automatická tvorba pastí relevantních pro dalý VLAN/IP rozsah na základě vytvořených profilů skutečných zařízení	ANO	Automatizace nasazení/tvorby pastí na základě informací o terénu je podporována.
11	Nasazení	Ruční vytváření pastí s možností detailní parametrizace	ANO	Pasti je možné tvořit ručně a detailně je parametrizovat.
12	Lákání útočníka	Pasti vystupují aktivně na síti tak, aby byly útočníkem, který monitoruje síťový provoz slyšeny (NetBIOS, LLMNR, WAPD, ...)	ANO	Pasti jsou na síti viditelné a generují provoz několika protokoly. Nad rámec uvedených provádějí APR poissoning, UPnP, AD komunikaci.
13	Nasazení	Emulované pasti poskytují interaktivitu pro protokoly SSH, FTP, SMB, HTTP/HTTPS	ANO	Tyto typy emulovaných služeb jsou implementovány.
14	Nasazení	Emulované pasti podporují další protokoly, například databázové, Remote Desktop, VNC.	ANO	Tyto typy emulovaných služeb jsou implementovány.
15	Lákání útočníka	Systém umožňuje tvorbu falešných profilů odkazujících na pasti do klientských aplikací na skutečných koncových bodech s cílem lákat útočníka směrem k pastím	ANO	Distribucí tzv. Breadcrumbs.
16	Lákání útočníka	Systém umožní nasadit pasti se zranitelnostmi a bude určité zranitelnosti i emulovat	ANO	Emulované pasti emulují také některé zranitelnosti.
17	Lákání útočníka	Systém podporuje tvorbu falešných profilů také pro AWS a Azure cloudové služby	ANO	Podporováno funkcionalitou Breadcrumbs.
18	Vizibilita	Systém bude implementovat mechanismy pro zpomalení aktivit útočníka	ANO	Lze nastavit rychlost reakce pastí na interakci.
19	Vizibilita	Retrospektivní analýza - Systém poskytne informace o komunikaci mezi koncovými body, a tedy jdoucími i mimo vlastní pasti	ANO	Systém vytváří mapu komunikací ve vnitřní síti.
B	**Požadované funkcionality v oblasti otevřenosti systému**		**Splňuje požadavky ANO/NE**	**popis jak**
1	Integrace	Systém podporuje integraci se systémy typu NTA/NDR pro dohledání detailů o spojeních	ANO	Systém podporuje tuto integraci.
2	Integrace	Systém poskytuje otevřené a dokumentované API pro napojení na systémy jiných stran	ANO	RESTful API s JSON
3	Integrace	Systém umožňuje jednoduché/předpřipravené napojení na aplikace typu SIEM.	ANO	Podporovány jsou ArcSight, Qradar, Splunk a další, včetně parametrizovatelného napojení na obecný syslog.

C	Ostatní požadavky na vlastnosti části systému pro vytváření a využití systému návnad a pastí		Splňuje požadavky ANO/NE	popis jak
1	Vizibilita	Rozpoznání dalších zařízení připojených po IP protokolu - například síťových tiskáren - a vytvoření odpovídajícího profilu	ANO	Součástí funkcionality Asset Profillingu.
2	Nasazení	Vytvoření pastí typu: 1) IP tiskárna 2) směrovač, přepínač 3) WiFi AP 4) NAS 5) IP telefon	ANO	Pasti podporují emulaci uvedených typů zařízení.
3	Lákání útočníka	Pasti jsou schopné provádět autentizaci proti AD infrastruktuře, aby předstíraly aktivitu uživatelů	ANO	Pokryto Active Directory Deception, kdy jsou pasti zavedeny do AD.
4	Nasazení	Systém změní typ nasazených pastí v případě změny profilů skutečných koncových bodů v dané části sítě tak, aby pasti odpovídaly typově okolním zařízením	ANO	Pokryto adaptací na změny terénu.
5	Lákání útočníka	Systém umožní vytvořit past se souborovou strukturou (nikoliv obsahem) odpovídající skutečným koncovým bodům	ANO	Pomocí dodávané utility je možné sejmout strukturu složek a souborů a přenést ji na emulovanou past.
6	Lákání útočníka	Systém umožní nahrát obsah pro pasti přístupné přes http(s).	ANO	Podporováno včetně možnosti nasadit pro emulované pasti vlastní certifikáty.
7	Vizibilita	Systém umožní simulace z pohledů Red týmu and Blue týmu - analýza možných zdrojů a cílů útoků pro daný koncový bod	ANO	Simulace probíhá nad terénem a komunikační mapou.
8	Vizibilita	Systém bude detekovat příchozí spojení z Internetu včetně rozpoznání protokolu	ANO	Včetně tvorby seznamu služeb ve vnitřní síti dostupnými z internetu.
9	Reporting	Systém obsahuje předpřipravené typické reporty.	ANO	Pokryto vestavěným reportingem.
10	Reporting	Systém umožňuje nastavit periodicitu a adresy příjemců pro generování reportů.	ANO	Pokryto nastavením časového rozpisu generování reportů a jejich odesílání na zadané adresy.
11	Reporting	Systém umožňuje export informací minimálně ve formátech PDF a CSV.	ANO	PDF a CSV jsou podporovány.
12	Reporting	Systém umožní export pohledů na alerty s aplikovanými filtry do souboru PDF nebo CSV.	ANO	PDF a CSV jsou podporovány.
13	Vizibilita	Systém klasifikuje alerty z hlediska technik a taktik dle MITRE ATT&CK frameworku.	ANO	Kategorizace alertů dle MITRE ATT&CK je implementována.

14	Ostatní	Systém umožňuje whitelistovat situace. kdy by nemělo dojít ke vzniku alertu (například při přístupu bezpečnostního skeneru na past).	ANO	Whitelisting pro Deception je podporován.

Oblast Kvantitativní požadavky

A	Základní požadavky na funkčnost části systému pro bezpečnostní monitorování koncových bodů:		Splňuje požadavky ANO/NE	popis jak
1	Analýza síťového provozu (network)	Systém bude licencován na sběr provozu pro průměrný objem provozu 100 Mbps Systém bude zálohovat popis provozu po dobu 30 dní.	ANO	Požadavek je promítnut do nabízené licence.
2	Bezpečnost koncových bodů (EDR)	Systém bude nasazen na 100 koncových bodů (servery)	ANO	Požadavek je promítnut do nabízené licence.
3	Návnady a pasti (Honeypots)	Systém bude licencován pro nasazení v prostředí s 500 IP adresovatelnými zařízeními.	ANO	Požadavek je promítnut do nabízené licence.

PLNÁ MOC

ICZ a.s., IČO: 251 45 444, se sídlem Praha 4 - Nusle, Na hřebenech II 1718/10, PSČ 147 00, Česká republika, zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, oddíl B, vložka 4840 (dále „**Zmocnitel**"),

tímto zmocňuje

Ing. Mariana Arbeta, dat. nar. 10. srpna 1971, trvale bytem U Pražské dráhy 1188/11, 312 00 Plzeň (dále jen „**Zmocněnec**"),

aby za Zmocnitele činil veškerá právní jednání a jiné úkony v **obchodních vztazích** (včetně vztahů týkajících se veřejných zakázek ve smyslu ustanovení zákona č. 134/2016 Sb., zákon o zadávání veřejných zakázek, ve znění pozdějších předpisů), v nichž cena předmětu plnění vyjádřená peněžní částkou nepřesáhne částku **13.000.000,-Kč** (slovy třináct miliónů korun českých) s tím, že půjde-li o opakující se plnění, je základem pro výpočet tohoto limitu součet ceny všech opakujících se plnění bez DPH.

Tato plná moc nezahrnuje oprávnění Zmocněnce nakupovat a zcizovat cenné papíry, obchodní podíly, uzavírat smlouvy o prodeji části nebo celého podniku, zprostředkovatelské smlouvy, smlouvy o sdružení, smlouvy příkazní či mandátní, smlouvy nájemní, podnájemní či leasingové, přijímat a poskytovat úvěry, sjednávat odstupné, podepisovat směnky, zcizovat nemovitosti a zatěžovat je právními závazky. Zmocněnec dále není na základě této plné moci oprávněn uzavírat jakákoli narovnání a zavazovat Zmocnitele jakýmikoli ručitelskými závazky.

Tato plná moc se uděluje na dobu neurčitou s účinností od 1.1.2019.

V Praze dne 18. prosince 2018

ICZ a.s.

[redacted]

Ing. Bohuslav Cempírek
předseda představenstva

Zmocnění přijímám v plném rozsahu.

[redacted]

Ing. Marian Arbet

PROHLÁŠENÍ O PRAVOSTI PODPISU – C

Běžné číslo knihy o prohlášeních o pravosti podpisu 009790/270/2018/C
Já, níže podepsaná Mgr. Petra Koutná, advokátka se sídlem v Praze 7, Kostelní 875/6, zapsa v seznamu advokátů vedeném Českou advokátní komorou pod ev. č. 11082, prohlašuji, že tuto listi přede mnou vlastnoručně v 2 vyhotoveních) podepsal(a):

1) Ing. Bohuslav Cempírek, 18.3.1961, nar.
bytem v. Vězn. Brat. Sinku 400/12, Praha 4
jejíž/ jehož totožnost jsem zjistil z : OP. 209413966

Podepsaný advokát tímto prohlášením o pravosti podpisu nepotvrzuje správnost ani pravdivost úda uvedených v této listině, ani její soulad s právními předpisy.

V Praze, dne 18.12. 2018

[redacted]

OVĚŘOVACÍ DOLOŽKA PRO VIDIMACI
Podle ověřovací knihy Úřad městské části Pra
poř.č. vidimace III/2037/2022
tato úplná kopie obsahující 1 stranu
souhlasí doslovně s předloženou listinou, z níž byla pořízena.
a tato listina je prvopisem obsahujícím 1 stranu.
stina, z níž je vidimovaná listina pořízena, neobsahuje viditelný
jišťovací prvek.

[redacted]

Praze 4 dne 20.6.2022

Vidimaci
Jindra Vo

[redacted]