Ev. č. objednatele: S2020/121
Číslo smlouvy OHS 1109/2020

Smlouva o poskytování služeb
(Provozování systému SIEM formou HaaS)

Smluvní strany:

ISECO.CZ s.r.o.
se sídlem Bartůňkova 2349/3a, 149 00 Praha 4
zastoupena: Ing. Tomášem Dedkem, jednatelem
IČO: 03641074
DIČ: CZ03641074
Bank. spojení: [redacted]
kontaktní osoba: Ing. Tomáš Dedek
tel.: [redacted]
dále jen „**poskytovatel**"

a

Česká republika – Kancelář Poslanecké sněmovny
se sídlem: Sněmovní 176/4, 128 26 Praha 1 – Malá Strana
zastoupena: Mgr. Janem Morávkem, vedoucím Kanceláře Poslanecké sněmovny
osoba oprávněna jednat ve věcech smluvních: Ing. Mgr. Naďa Formanová, ředitelka odboru hospodářské správy, na základě pověření vedoucího zaměstnance k jednání jménem státu ze dne 1. 7. 2017
IČO: 00006572
DIČ: CZ00006572
bankovní spojení: ČNB Praha, číslo účtu: 5622001/0710
datová schránka ID: bykaigw
kontaktní osoba: Ing. Marek Fiala, manažer kybernetické bezpečnosti
[redacted]
dále jen „**objednatel**"

(poskytovatel a objednatel dále též společně jako „smluvní strany" a každý jednotlivě jako „smluvní strana")

Smluvní strany ujednávají následující:

Článek I.
Předmět smlouvy

1.1 Předmětem této smlouvy je závazek poskytovatele poskytnout objednateli služby spojené s poskytováním systému SIEM formou HaaS a závazek objednatele zaplatit poskytovateli za řádně poskytnuté služby sjednanou cenu. Bližší specifikace předmětu plnění je uvedena v příloze č. 1 smlouvy – Technická specifikace nabízeného řešení.

1.2 Závazek poskytovatele spočívá zejména v poskytnutí, zprovoznění a udržování systému SIEM formou HaaS a s tím souvisejících služeb.

1.3 Poskytovatel se dále zavazuje zajistit po celou dobu realizace předmětu plnění vzdálenou podporu v režimu 24x7 e-mailovou a telefonní hot-line v českém jazyce. Pro tyto účely uvádí poskytovatel následující kontakty pro hot-line:

1.3.1 Telefonický kontakt: +420 230 234 168

1.3.2 Elektronický kontakt: support@iseco.cz

1.4 Poskytovatel se zavazuje poskytovat služby správy a provozu systému SIEM. Poskytovatel má právo odmítnout poskytnutí služeb, které by znamenalo překročení sjednaného rozsahu. Poskytnutí služby nad rámec sjednaného rozsahu nezakládá právo na vyšší úplatu.

1.5 Poskytovatel se zavazuje poskytovat služby způsobem, v rozsahu, kvalitě a termínech uvedených v této smlouvě včetně všech příloh a v jeho nabídce podané v rámci zadávacího řízení nadlimitní veřejné zakázky s názvem „Nákup systému SIEM formou HaaS".

Článek II.
Místo plnění

2.1 Místem plnění předmětu smlouvy je sídlo objednatele, služby podpory budou poskytovány vzdáleně, pokud nebude objednatelem požadováno jinak.

Článek III.
Termín plnění

3.1 Poskytovatel se zavazuje zahájit plnění předmětu této smlouvy, tedy dokončit implementaci systému SIEM do 2 měsíců od účinnosti smlouvy.

3.2 Poskytovatel se zavazuje systém SIEM formou HaaS poskytovat objednateli po dobu 5 let od implementace systému SIEM.

Článek IV.
Smluvní cena a platební podmínky

4.1 Smluvní strany se dohodly na jednorázové ceně za řádnou implementaci systému SIEM ve výši 700 000 Kč bez DPH, DPH činí 147 000 Kč, tj. 847 000 Kč včetně DPH.

4.2 Cena dle odst. 4.1 Smlouvy je konečná a nepřekročitelná a zahrnuje veškeré náklady vynaložené v souvislosti s implementací předmětu plnění.

4.3 Poskytovateli vzniká nárok na úplatu za řádnou implementaci předmětu plnění po řádném předání předmětu plnění bez vad a nedodělků, tj. po ukončení akceptačního řízení s výsledkem bez výhrad.

4.4 Smluvní strany se dohodly na ceně za řádně poskytnuté služby ve výši: 110 000 Kč bez DPH/měsíc, DPH 23 100 Kč, tj. 133 100 Kč včetně DPH.

4.5 Měsíční sazba uvedená v odst. 4.4 smlouvy je konečná a nepřekročitelná a zahrnuje veškeré náklady vynaložené v souvislosti s plněním předmětu této veřejné zakázky.

4.6 K uvedené ceně bez DPH bude připočtena DPH v příslušné zákonné sazbě platné ke dni zdanitelného plnění.

4.7 Maximální výše plnění za celou dobu realizace této smlouvy (tj. 60 měsíců) včetně implementace systému SIEM nesmí přesáhnout částku 7 300 000 Kč bez DPH, DPH 1 533 000 Kč, tj. částku 8 833 000 Kč včetně DPH.

4.8 Platba za řádně poskytnuté služby bude prováděna měsíčně zpětně na základě faktury vystavené poskytovatelem. Poskytovatel je povinen vystavit a doručit fakturu nejpozději do 15. dne měsíce následujícího po měsíci, v němž byly služby poskytnuty.

4.9 Faktura vystavená poskytovatelem musí splňovat náležitosti daňového dokladu stanovené právními předpisy.

4.10 Fakturované částky budou hrazeny bezhotovostně, a to bankovním převodem na účet poskytovatele uvedený v této smlouvě, nebo na účet poskytovatele dodatečně písemně oznámený objednateli, a to nejpozději ke dni doručení faktury.

4.11 Splatnost faktury je 30 kalendářních dnů ode dne doručení řádně vystavené faktury objednateli. V případě, že faktura nebude obsahovat náležitosti daňového dokladu nebo nebude vystavena v souladu s podmínkami sjednanými v této smlouvě, je objednatel oprávněn vrátit ji poskytovateli k doplnění. V takovém případě se přeruší plynutí lhůty splatnosti a nová lhůta splatnosti začne plynout doručením opravené faktury objednateli.

4.12 Objednatel umožňuje doručení faktury v písemné i elektronické podobě. Elektronická faktura musí být zaslána na e-mail: faktury@psp.cz

4.13 Faktura se považuje za zaplacenou dnem, kdy bude fakturovaná částka odeslána

z účtu objednatele ve prospěch účtu poskytovatele.

4.14 Poskytovatel prohlašuje a svým podpisem v závěru smlouvy potvrzuje, že ke dni uzavření smlouvy není veden v rejstříku nespolehlivých plátců DPH, a pro případ, že se stane nespolehlivým plátcem DPH až po uzavření této smlouvy, zavazuje se bezodkladně a prokazatelně po vydání rozhodnutí správce daně podle §106a zákona o DPH, informovat objednatele o této skutečnosti.

4.15 Pokud objednatel jako příjemce zdanitelného plnění zjistí po doručení daňového dokladu (faktury), že poskytovatel je v evidenci plátců DPH označen jako nespolehlivý plátce DPH, anebo bankovní účet, který poskytovatel uvede na daňovém dokladu (faktuře), není zveřejněn v registru plátců DPH, je objednatel oprávněn uhradit poskytovateli pouze tu část peněžitého závazku vyplývajícího z daňového dokladu, jež odpovídá výši základu daně, a zbylou část pak ve smyslu §109a zákona o DPH uhradit přímo správci daně. V případě uplatnění výše uvedeného postupu zaniká nárok poskytovatele, který je na seznamu nespolehlivých plátců DPH, na zaplacení částky odpovídající výši DPH.

Článek V.
Další podmínky plnění předmětu smlouvy

5.1 Poskytovatel je povinen poskytovat služby sjednané v této smlouvě řádně, včas, s odbornou péčí, podle svých nejlepších znalostí a schopností a v souladu s obecně závaznými právními předpisy, přičemž je povinen sledovat a chránit oprávněné zájmy objednatele.

5.2 Poskytovatel postupuje při poskytování služeb samostatně, je však povinen dbát pokynů objednatele, pokud objednatel pokyny uděluje.

5.3 Poskytovatel je povinen upozornit objednatele na zřejmě nesprávný pokyn, a to bez zbytečného odkladu, a s jeho plněním vyčkat až do doby, než objednatel potvrdí poskytovateli, že na splnění pokynu přesto trvá.

5.4 V případě prodlení objednatele se zaplacením jakéhokoliv finančního plnění poskytovateli podle této smlouvy nemá poskytovatel právo přerušit poskytování služeb.

5.5 Poskytovatel nemá právo přenechat poskytování služeb poddodavatelům, s výjimkou poddodavatelů uvedených v nabídce poskytovatele.

5.6 V případě, že poskytovatel bude pro řádné poskytování služeb potřebovat informace od objednatele, má objednatel povinnost poskytnout poskytovateli součinnost, zejména mu sdělit veškeré požadované informace, a to bez zbytečného odkladu.

5.7 Objednatel se zavazuje zajistit poskytovateli veškeré podmínky nezbytné pro řádné poskytování služeb, zejména zajistit či poskytnout všechny potřebné přístupy.

5.8 Poskytovatel se zavazuje předat objednateli veškeré informace o změnách v realizačním týmu. Dále se zavazuje evidovat všechny jím provedené změny v konfiguraci formou provozního deníku nebo komentářů k jednotlivým konfiguračním dokumentům.

Článek VI.
Autorská práva

6.1 Součástí poskytovaných služeb jsou SW licence včetně produktové podpory na dobu poskytování služeb.

6.2 Součástí plnění podle této smlouvy není vývoj aplikací ani SW. Podpůrné aplikace a skripty budou řešeny ad hoc.

6.3 Objednatel nemá právo udělit třetím osobám podlicence.

6.4 Poskytovatel nemá právo na jakoukoli dodatečnou odměnu v souvislosti s autorskými právy souvisejícími s poskytováním služeb.

Článek VII.
Komunikace

7.1 Poskytovatel a objednatel budou komunikovat zejména prostřednictvím kontaktních osob uvedených v této smlouvě, preferovaným způsobem komunikace je komunikace elektronická.

7.2 Změna kontaktních osob je možná jen na základě předchozího písemného upozornění.

Článek VIII.
Odpovědnost za škodu

8.1 Poskytovatel plně odpovídá za škodu způsobenou objednateli poskytovatelem jakýmkoli porušením povinností poskytovatele uvedených v této smlouvě a jejích přílohách.

8.2 Poskytovatel je povinen mít po celou dobu trvání smlouvy uzavřené platné pojištění odpovědnosti za škodu způsobenou třetí osobě s pojistným limitem minimálně 5 000 000,- Kč. V případě, že pojistný vztah mezi poskytovatelem a pojistitelem skončí, je poskytovatel povinen sjednat nový pojistný vztah ve stejném rozsahu tak, aby byla zachována podmínka existence pojištění v předmětném rozsahu po celou dobu trvání tohoto smluvního vztahu. Existenci pojištění je poskytovatel povinen na žádost objednatele kdykoliv prokázat.

Článek IX.
Důvěrnost

9.1 Poskytovatel je vázán Dohodou o mlčenlivosti, která tvoří přílohu č. 2 této smlouvy.

9.2 Poskytovatel není oprávněn užívat data uživatelů ani aplikací, s výjimkou auditních záznamů, konfigurací a nastavení potřebných pro řešené PMR. Data mohou být vydána jen se souhlasem manažera kybernetické bezpečnosti.

9.3 Mezi důvěrné informace nepatří žádné informace, které jsou v době jejich zpřístupnění nebo použití běžně dostupné veřejnosti.

9.4 Objednatel dává souhlas poskytovateli, aby jej poskytovatel uváděl jako svého zákazníka.

Článek X.
Smluvní pokuta

10.1 Poskytovatel se zavazuje zaplatit smluvní pokutu ve výši 0,05 % za každý započatý den prodlení v případě porušení povinnosti specifikované v odst. 3.1 smlouvy.

10.2 V případě porušení povinností ohledně mlčenlivosti a důvěrnosti informací (dle čl. IX. A přílohy č. 2 této smlouvy), zavazuje se uhradit Objednateli smluvní pokutu ve výši 50.000, - Kč za každé jednotlivé porušení povinnosti.

10.3 Poskytovatel se zavazuje zaplatit smluvní pokutu ve výši 100 000,- Kč v případě implementace neověřeného updatu, a to za každý jednotlivý případ.

10.4 Poskytovatel se zavazuje zaplatit smluvní pokutu ve výši 100 000,- Kč za každý případ havárie systému, která byla způsobena chybou konfigurace poskytovatelem.

10.5 Poskytovatel se zavazuje zaplatit smluvní pokutu ve výši 100 000,- Kč za každý případ kybernetického bezpečnostního incidentu, který byl zaviněn poskytovatelem.

10.6 V případě prodlení Objednatele s úhradou řádně vystavené faktury, je Poskytovatel oprávněn účtovat objednateli úrok z prodlení v zákonné výši z fakturované částky za každý započatý den prodlení.

10.7 Smluvní pokuta a úrok z prodlení jsou splatné do 15 kalendářních dnů ode dne doručení jejich vyúčtování.

10.8 Zaplacením smluvní pokuty není dotčeno právo oprávněné strany na náhradu škody vzniklé v příčinné souvislosti s porušením smluvní povinnosti, za jejíž nedodržení je smluvní pokuta vymáhána a účtována.

10.9 Objednatel je oprávněn jednostranně započíst splatné smluvní pokuty vzniklé Poskytovateli vůči splatné úhradě za poskytování služeb dle této smlouvy.

Článek XI.
Platnost smlouvy

11.1 Tato smlouva nabývá platnosti dnem podpisu oprávněnými zástupci obou smluvních stran.

11.2 Tato smlouva se uzavírá na dobu 60 měsíců od zahájení poskytování služeb dle této smlouvy.

11.3 Obě smluvní strany jsou oprávněny ukončit tuto smlouvu písemnou výpovědí i bez udání důvodů. Výpovědní doba činí jeden (1) měsíc a počíná běžet prvním dnem měsíce následujícího po měsíci, v němž došlo k doručení výpovědi druhé smluvní straně.

Článek XII.
Ostatní ujednání

12.1 Objednatel si vyhrazuje právo na provedení auditu kybernetické bezpečnosti u poskytovatele. Tento audit lze nahradit poskytnutím výroční auditní zprávy v souladu s ČSN EN ISO/IEC 2700X.

12.2 Všichni jednotliví poddodavatelé se zavazují dodržovat v plném rozsahu ujednání mezi povinnou osobou a poskytovatelem a nebudou v rozporu s požadavky povinné osoby (dle Dohody o mlčenlivosti). Součástí této povinnosti je podpis Dohody o mlčenlivosti poddodavatelem.

12.3 Poskytovatel se zavazuje dodržovat veškerá pravidla vyplývající z obecné bezpečnostní politiky a systémové bezpečnostní politiky, případně její odsouhlasení po jejím zpracování.

12.4 Poskytovatel se zavazuje informovat Národní úřad kybernetické a informační bezpečnosti a objednatele o kybernetických bezpečnostních incidentech souvisejících s poskytováním služeb podle této smlouvy.

12.5 Poskytovatel se dále zavazuje informovat objednatele o způsobu řízení rizik na straně poskytovatele a o zbytkových rizicích souvisejících s plněním smlouvy.

12.6 Poskytovatel se zavazuje informovat objednatele a Národní úřad kybernetické a informační bezpečnosti o významné změně ovládání poskytovatele podle zákona o obchodních korporacích nebo o změně vlastnictví základních aktiv, změně oprávnění nakládat s těmito aktivy, využívanými poskytovatelem k plnění této smlouvy.

12.7 Objednatel si vyhrazuje právo v případě havárie nebo kybernetického bezpečnostního incidentu požádat poskytovatele o zajištění účasti jeho zaměstnanců do ISIRT týmu objednatele. Poskytovatel se zavazuje poskytnout objednateli matici kontaktních údajů

zaměstnanců poskytovatele, kteří mohou být zařazeni do ISIRT týmu, včetně jejich odborného zaměření.

12.8 Poskytovatel bere na vědomí, že podle ustanovení § 3 odst. 2 písm. f) zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), nebude tato smlouva uveřejněna v registru smluv.

Článek XIII.

Vyšší moc

13.1 Smluvní strany se zprošťují veškeré odpovědnosti za nesplnění svých povinností z této smlouvy po dobu trvání vyšší moci do té míry, pokud po nich nebylo možné požadovat, aby neplnění svých povinností z této smlouvy v důsledku vyšší moci předešly.

13.2 Za vyšší moc je pro účely této smlouvy považována každá událost nezávislá na vůli smluvních stran, která znemožňuje plnění smluvních závazků a kterou nebylo možno předvídat v době vzniku této smlouvy. Za vyšší moc se z hlediska této Smlouvy považuje zejména přírodní katastrofa, požár, výbuch, silná vichřice, zemětřesení, záplavy, válka, stávka nebo jiné události, které jsou mimo jakoukoliv kontrolu smluvních stran.

13.3 Po dobu trvání vyšší moci se plnění závazků podle této smlouvy pozastavuje do doby odstranění následků vyšší moci.

Článek XIV.

Závěrečná ustanovení

14.1 Tato smlouva, jakož i práva a povinnosti vzniklé na základě této smlouvy nebo v souvislosti s ní se řídí právním řádem České republiky, zejména zák. č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.

14.2 Nevymahatelnost či neplatnost kteréhokoliv ustanovení této smlouvy nemá vliv na vymahatelnost či platnost zbývajících ustanovení této smlouvy, pokud z povahy nebo obsahu takového ustanovení nevyplývá, že nemůže být odděleno od ostatního obsahu této smlouvy.

14.3 Tato smlouva představuje úplné ujednání smluvních stran ve vztahu k předmětu této smlouvy.

14.4 Tato smlouva může být měněna jen vzestupně číslovanými Dodatky.

14.5 Nedílnou součást smlouvy tvoří tyto přílohy:

Příloha č. 1 – Technická specifikace

Příloha č. 2 – Dohoda o mlčenlivosti

14.6 Tato smlouva je uzavřena v pěti (5) vyhotoveních, z nichž Objednatel obdrží tři (3) vyhotovení a Poskytovatel dvě (2) vyhotovení, případně v jednom elektronickém vyhotovení s platností originálu.

14.7 Smluvní strany si smlouvu přečetly, souhlasí s jejím obsahem a prohlašují, že je ujednána svobodně.

V Praze dne …….

……
objednatel

Ing. Mgr. Naďa Formanová,
ředitelka odboru hospodářské správy,
na základě pověření vedoucího
zaměstnance k jednání jménem
státu ze dne 1. 7. 2017

V Praze dne …….

……
poskytovatel

Ing. Tomáš Dedek,
jednatel

Příloha č. 1 - Technická specifikace zařízení

Tato příloha slouží k uvedení názvu / typu konkrétního nabízeného zařízení a dále k vymezení minimálních technických požadavků zadavatele na zboží a osvědčení jejich splnění účastníkem.

Název / typ zařízení: [redacted]

Požadavky zadavatele jsou uvedeny ve **sloupci 2**, účastník vyplní všechny položky **sloupce 3** (např. popisem nabízeného parametru nebo jen slovem „ano", pokud by byl popis stejný jako text uvedený ve sloupci 2).
Následná smlouva s vybraným dodavatelem může být v této části upravena tak, aby obsahovala již pouze účastníkem nabídnuté zařízení a jeho technické parametry.

Administrace řešení

	Minimálními technickými požadavky na zařízení	Technická specifikace nabízeného zařízení
1	Řešení poskytuje centrální webovou konzoli, ze které lze spravovat celé řešení (centrální správa z jednoho místa).	[redacted]
2	Řešení poskytuje webové uživatelské rozhraní pro: správu, analýzy, reportovaní a podobně. Rozhraní by nemělo obsahovat pluginy. Rozhraní nesmí vyžadovat instalaci dalšího SW na straně uživatelů (technologie Java, Flash, apod.) a nesmí vyžadovat používání nebo instalaci tlustého klienta.	
3	Řešení musí podporovat práci s interními překrývajícími se rozsahy adres spolu se síťovými toky, událostmi a zařízeními v síti, a umožnit tak v jednom řešení například správu a funkčnost například partnerské nebo podřízené organizace.	
4	Řešení musí umožňovat definici uživatelských oprávnění pro možnost oddělení přístupu jednotlivých administrátorů k jednotlivým zdrojům logů a toků, jejich skupinám či síťovým segmentům.	

Nasazení a rozšiřitelnost

	Minimálními technickými požadavky na zařízení	Technická specifikace nabízeného zařízení
1	Řešení musí výkonově podporovat zpracování množství událostí (EPS=Events Per Second) a toků (FPM=Flows Per Minute), a to nejen požadovaných aktuálních, ale i po případném navýšení EPS a FPM na zadavatelem předpokládané hodnoty, a to bez nutnosti dokupování HW. Tedy čistě dokoupením potřebných licencí.	[redacted]
2	Řešení musí být dodáno formou All-In-One appliance, tedy jako jedno zařízení pokrývající veškeré požadované funkce.	

3	Řešení musí být dodáno v HW formě jako fyzická appliance montovaná do racku.	[redacted]
4	Řešení musí umožňovat vzdálený sběr logů (například na pobočce, nebo v DMZ apod.) samostatným kolektorem s následným přeposíláním událostí v komprimované podobě do zbytku řešení. V případě výpadku spojení se SIEMem (centrálním AIO hostem), musí kolektor pokračovat ve sběru/příjmu událostí/logů, a tyto dočasně lokálně ukládat. Po obnovení spojení musí tyto data dodatečně přeposlat do SIEMu.	
5	Řešení musí umožňovat provádět automatické aktualizace řešení bez pomoci profesionálních služeb výrobce.	
6	Řešení musí obsahovat mechanismus na interní kontrolu stavu komponent řešení a upozornění administrátora v případě problému.	
7	Řešení musí nativně umožňovat nasazení v režimu vysoké dostupnosti bez nutnosti využití dalších softwarů a řešení třetích stran. Tedy dokoupením licencí a dokoupením potřebného HW/SW.	
8	Nabízené řešení musí umožňovat budoucí rozšíření o HA funkcionalitu, a to dokoupením potřebných licencí, HW, SW.	
9	Režim vysoké dostupnosti musí být možné připojit v jakékoliv fázi, a to bez nutnosti reinstalace celého řešení a bez ztráty již nasbíraných dat.	
10	V případě, že řešení není dodáno na HW vendora SIEMu, ale jako SW běžící na HW třetí strany, je nutné tento HW dodat včetně odpovídajícího rozsahu náležitostí a podpory, musí splňovat požadavky vendora SIEMu, a dále musí splnit tyto minimální požadavky: RAM: 128GB a více CPU: 2x CPU, celkový počet všech fyzických jader: 24 a více. OS: HW plně podporovaný Linux RHEL v7.5, 64bit Řadič disků: s funkcí odpovídající RAID 5 nebo 6 nebo 10, a s funkcionalitou odpovídající řešením s dedikovanou pamětí pro urychlení zápisů a podporou bezpečných „Write back caching“ operací.	

Příjem událostí/logů a zdroje logů

	Minimálními technickými požadavky na zařízení	Technická specifikace nabízeného zařízení
1	Licence a výkon pro zpracování událostí minimálně 2500 EPS, s možností rozšíření na 5000 EPS, bez nutnosti rozšíření HW	[redacted]

2	Licence a výkon minimálně pro 300 vstupních zdrojů logů.	[redacted]
3	Řešení musí umožňovat sběr logů bez agentů, tedy umožňovat sběr bez nutnosti instalovat agenta a SW na cílový systém (zdroj logů).	
4	Řešení musí umožnit instalovat agenta na cílový systém pro sběr událostí z Microsoft Windows prostředí.	
5	Řešení musí obsahovat kolektor událostí/logů (pro všechny podporované typy a zdroje logů/událostí), do virtuálního prostředí VMWARE. V případě budoucí potřeby zadavatele, musí umožnovat reinstalaci tohoto kolektoru na vendorem podporovaný HW zadavatele.	
6	Řešení musí obsahovat vestavěný mechanismus kategorizace zdrojů logů dle typu.	
7	Řešení musí podporovat agregaci události dle vybraných atributů, včetně vlastních uživatelem přidaných=definovaných.	
8	Řešení umožnuje sběr událostí z následujících typů zdrojů (a pomocí následujících protokolů): Syslog, Windows Events Collection (WinRM/ RPC), FTP, SCP, SNMP, ODBC/JDBC, CP-LEA, SDEE, log file.	
9	Řešení umožňuje příjem dat ze zdrojů logů/toků pomocí šifrované komunikace.	
10	Řešení musí umožňovat vytvářet uživatelem definované atributy a plnit jich i ze surového (RAW) obsahu přijatých logů (událostí), pomocí uživatelsky definovatelných regulárních výrazů (REGEX).	
11	Podpora a vyhodnocování logů z následujících bezpečnostních a síťových systémů: FlowMon ADS, FW PaloAlto, AV Symantec.	

Příjem toků a zdroje toků

	Minimálními technickými požadavky na zařízení	Technická specifikace nabízeného zařízení
1	Licence a výkon pro zpracování toků minimálně 15 000 FPM s možností rozšíření na 200 000 FPM, bez nutnosti rozšíření HW.	[redacted]
2	Licence a výkon minimálně pro 50 vstupních zdrojů toků.	
3	Řešení musí podporovat sběr síťových toků z infrastrukturních prvků ve formátech IPFIX, NetFlow v9, J-Flow, sFlow.	

4	Řešení musí podporovat agregaci záznamů o síťovém provozu z obou stran datového toku do jedno záznamu popisující obousměrnou komunikaci.	[redacted]

Ukládání dat

	Minimálními technickými požadavky na zařízení	Technická specifikace nabízeného zařízení
1	Pro 50% zdrojů logů je požadována retence 18 měsíců, a pro zbytek zdrojů logů 6 měsíců. Průměrná velikost události (včetně následných indexů a strukturovaných údajů z ní) cca 1000B na událost.	[redacted]
2	Pro toky je požadována retence minimálně 2 měsíců. Toky jsou ve formátu IPFIX od technologie Flowmonu, s plnou sadou rozšířených atributů L2-L7.	
3	Úložní kapacita pro uložení logů a toků musí být minimálně 10TB.	
4	Řešení musí ukládat příchozí události v normalizovaném formátu a zároveň i v originálním „RAW“ formátu.	
5	Řešení musí obsahovat mechanismus pro zajištění integrity ukládaných dat.	
6	Řešení musí obsahovat mechanismus pro odhalení dodatečných změn uložených událostí.	
7	Řešení musí obsahovat mechanismus pro plánované archivování uložených dat na externí uložiště.	
8	Řešení musí mít schopnost uchovat interně (tzv. online) potřebné množství dat, aniž by řešení vyžadovalo použití externích paměťových zařízení.	
9	Řešení musí obsahovat funkcionalitu automatické tvorby záloh konfigurace s následnou možností obnovy.	

Analýza, Korelace, Detekce

Účelem je co nejvíce odlehčit práci analytika, a předložit mu seznam prioritizovaných potenciálních incidentů, kterými by se měl dále zabývat.
Systém musí být schopen události předzpracovat, najít mezi událostmi spojitosti a souvislosti, a seskupit je v rámci jednoho prioritizovaného incidentu (co nejvíce očištěného od false-positive událostí) k řešení.

	Minimálními technickými požadavky na zařízení	Technická specifikace nabízeného zařízení

1	Řešení musí mít možnost přidávat další korelační pravidla a to i bez potřeby rozšíření/navýšení licence/licencí.	[redacted]
2	Řešení musí již out-of-box obsahovat analytické a korelační pravidla, která lze začít používat ihned po instalaci v rozsahu alespoň 250 pravidel. Alternativně, dodavatel se zaváže navrhnout a naimportovat tyto pravidla dle „best practices“ tak, aby je zákazník akceptoval.	
3	Řešení musí provádět analýzu událostí téměř v reálném čase (near-real-time, nebo on-the-fly), tedy v momentě příchodu události do řešení bude událost testována korelačními pravidly, a nečeká se na pravidelná dávkové zpracování pravidel v časových intervalech ani za časové okno.	
4	Řešení musí obsahovat takzvanou „Network Behavior Anomaly Detection“ funkcionalitu, která provádí analýzu dlouhodobých trendů, které vychází z příchozích událostí a toků.	
5	Řešení musí podporovat schopnost monitorovat historii útoků (typů událostí) na kritické komponenty.	
6	Řešení musí být schopno korelovat události z DHCP, VPN a Active Directory a sledovat průběh uživatelské relace v rámci celé organizace.	
7	Řešení musí umožňovat korelovat události (data z události) se statickými i dynamickými seznamy.	
8	Řešení musí být schopno plnit nebo odebírat hodnoty atributů ze statických nebo dynamických seznamů, a to na základě vybraných atributů (dat) z událostí. Například plnění seznamů přihlášených uživatelů z událostí o přihlášení uživatele apod.	
9	Některá zařízení v síti často mění svou IP adresu. Řešení musí být schopno udržet databázi zařízení konzistentní i pro zařízení, která často mění svou IP adresu v síti.	
10	Řešení musí obsahovat funkcionalitu behaviorální analýzy uživatelů, pro možnosti zkoumání chování uživatelů. Tato funkcionalita má být úzce provázána se zbytkem systému a pomáhat analytikům s vyšetřováním. Řešení musí obsahovat i základní out-of-the-box pravidla pro funkcionalitu behaviorální analýzy uživatelů.	
11	Řešení musí umožňovat automatické i manuální načítání (např. z Active Directory/LDAP) a korelaci uživatelských identit pro následné vyhodnocování anomálního chování sledovaných uživatelských identit.	

12	Sledování a vyhodnocování uživatelského chování musí: • být integrováno do jednotného uživatelského rozhraní a • podporovat jednoduchou správu, ladění a vytváření uživatelských „use cases“ Uživatel SIEM systému musí mít možnost ovlivňovat risk skóre jednotlivých „use cases“ a rovněž možnost konfigurace globálních mezních hodnot pro vygenerování potenciálních bezpečnostních incidentů.	[redacted]
13	Řešení musí podporovat analýzu chování sledovaných uživatelů za podpory automatizovaného profilování chování uživatelů pomocí algoritmů strojového učení.	
14	Řešení musí obsahovat funkcionalitu pro výměnu standardizovaných informací informačně bezpečnostního charakteru jako jsou STIX nebo TAXII.	
15	Řešení musí být schopno zřetězit všechny detekované události z různých zdrojů logů, které mohou mít souvislost s detekovanou aktivitou (například útokem), a vytvořit tak jeden incident, ke kterému dané události přiřadí.	

Vyhledávání

Funkcionality, které umožňují uživatelům manuální vyhledávání a prohledávání přijatých i uložených událostí (jak v původním (tzv. RAW) stavu, tak v normalizovaném strukturovaném stavu), včetně tzv. dril-down procházení dat vytvořených incidentů.

	Minimálními technickými požadavky na zařízení	**Technická specifikace nabízeného zařízení**
1	Řešení musí v centrální webové konzoli umožňovat provádět kombinované hledání v indexovaných i neindexovaných auditních datech s použitím regulárních výrazů a fulltextového vyhledávání v nestrukturovaném textu současně.	[redacted]
2	Řešení musí poskytovat pokročilé detailní vyhledávání tzv. drill-down s možností filtrace až na úroveň IP adresy, typu události, protokolu, portu atd.	
3	Řešení musí umožňovat filtrování dohledaných výsledků (formou rozšíření existujícího dotazu pro vyhledání) přes kliknutí na některou hodnotu výsledku a výběru Booleovy logiky vůči dané hodnotě. Také musí umožnit kdykoli v tomto procesu provést editaci a úpravu nebo změnu kterékoli části vyhledávacího dotazu, včetně uložení takovéhoto dotazu pro pozdější použití.	

4	Řešení musí umožňovat zadat i pokročilý složený podmiňovací vyhledávací dotaz čistě pomocí grafického rozhraní, tedy výběrem a kombinací podmínek, atributů a jejich hodnot v nich, tedy bez potřeby znalosti syntaxu případného dotazovacího jazyka řešení.	Ano, vlastnost IBM QRadar.
5	Řešení musí umožňovat zadat i pokročilý složený podmiňovací vyhledávací dotaz čistě pomocí zadání dotazovacího jazyka řešení (ala SQL dotaz).	Ano, vlastnost IBM QRadar.
6	Řešení musí podporovat vyhledávání s použitím Booleovy logiky i regulárního výrazu.	Ano, vlastnost IBM QRadar.

Alarmy, Upozornění, Incidenty

	Minimálními technickými požadavky na zařízení	Technická specifikace nabízeného zařízení
1	Řešení musí být schopno zobrazit ve webovém rozhraní (a také i zaslat emailem i Syslogem) upozornění správcům, v případě výskytů provozních problémů s řešením (například dochází volná úložní kapacita, výpadek některé části řešení, dostupné aktualizace, překročení/dosažení licenčních a jiných prahových provozních hodnot a podobně).	[redacted]
2	Řešení musí být schopno vytvářet události i incidenty na základě takových korelací, které umožní detekovat: Detekované hrozby, anomálie, porušení bezpečnostní politiky a překročení nastavených hraničních hodnot.	
3	Řešení musí mít možnost zaslat upozornění při výpadku sběru událostí ze zařízení (zdroje logů).	
4	Řešení musí umožňovat při vytvoření i příjmu **události** (i všechny možnosti níže současně): odeslání emailu, odeslání Syslog správy, odeslání SMTP trapu, spuštění skriptu, vytvoření nové vlastní události, vytvoření nového incidentu, vložení nebo odmazání záznamu ze seznamů použitých pro korelace (seznam IP adres, seznam sledovaných uživatelů apod.).	

5	Řešení musí umožňovat při vytvoření **incidentu** (i všechny možnosti níže současně): odeslání emailu, odeslání Syslog správy, odeslání SMTP trapu, spuštění skriptu, vytvoření nové vlastní události, vložení nebo odmazání záznamu ze seznamů použitých pro korelace (seznam IP adres, seznam sledovaných uživatelů apod.).	[redacted]

Reportování

	Minimálními technickými požadavky na zařízení	Technická specifikace nabízeného zařízení
1	Počet reportů nesmí být limitován licenčně.	[redacted]
2	Řešení musí obsahovat předpřipravené reporty (takzvaně out-of-box), které lze začít používat ihned po instalaci, v rozsahu minimálně 100 reportů. Alternativně, dodavatel se zaváže navrhnout a naimportovat tyto reporty dle „best practices“ tak, aby je zákazník akceptoval.	
3	V rámci dodaných/implementovaných reportů, kromě standardních bezpečnostních SIEM reportů, musí reporty pokrývat komplexně i oblasti ISO 27001, GDPR, provozní a auditní oblast SIEMu, reporty pro integrované technologie (zdroje logů) apod.	
4	Řešení musí umožňovat vytvářet vlastní reporty pomocí grafického rozhraní, kde obsah dat reportu je možné definovat stejným vyhledávacím dotazem i způsoby, jakým se vytváří dotaz pro hledání.	
5	Řešení musí umožňovat vytvářet vlastní reporty pomocí grafického rozhraní, kde obsah dat reportu je možné definovat pomocí již existujícího uloženého vyhledávacího dotazu z předchozího vyhledávání/hledání.	
6	Řešení musí podporovat nezměněnou funkcionalitu reportingu i pokud dojde ke změně některé technologie, jako např. firewallu nebo IDS, a podobně.	

Integrace

	Minimálními technickými požadavky na zařízení	Technická specifikace nabízeného zařízení

1	Řešení musí podporovat integraci pomocí otevřeného API rozhraní. API může sloužit pro strojovou interakci s řešením nebo pro integraci s řešeními třetích stran.	[redacted]
2	Řešení musí umožňovat ověřování uživatelů pomocí integrace s adresářovým systémem Active Directory.	
3	Řešení musí umožňovat pracovat s reputačními službami výrobce nebo s reputačními službami třetích stran. Reputační služby poskytují například IP geolokaci, botnet kanály atp.	
4	Řešení musí umožňovat rozšíření funkcionality pomocí aplikačního frameworku s veřejně dostupným obsahem.	

Oblast zranitelností a řízení rizik

	Minimálními technickými požadavky na zařízení	Technická specifikace nabízeného zařízení
1	Řešení musí umožňovat přidání integrovaného managementu rizik na základě síťových toků a konfigurace aktivních prvků do GUI formou rozšíření licence.	[redacted]
2	Řešení musí být schopno konsolidovat výsledky z několika řešení, jako jsou vulnerability scannery, risk management nástroje a externí vstupy bezpečnostních informací z různých zdrojů.	
3	Řešení musí umět aktivně skenovat zařízení v sítí na zranitelnosti. Musí být schopno v jednom skenu prověřit rozsah definovaný síťovým subnetem (například 10.0.0.0/8), a z něj pak provést analýzu, zpracovat, vyhodnotit a uložit výsledky pro alespoň 500 “živých=aktivních“ hostů v této síti.	
4	Skeny a skeny zranitelností, musí umět následující typy skenů: 1. „Discovery“ sken (síťový horizontální i vertikální). 2. Autentizovaný sken (například WMI sken a další). 3. Aplikační skeny, minimálně webový sken a databázový sken.	
5	Řešení musí být schopno provádět požadované skeny přímo z AIO HW SIEMu.	

6	Řešení musí obsahovat další skener (pro všechny požadované typy skenů), do virtuálního prostředí VMWARE, ideálně na stejný host, na kterém je/bude provozován kolektor událostí/logů. V případě budoucí potřeby zadavatele, musí umožnovat reinstalaci tohoto skeneru na vendorem podporovaný HW zadavatele. Zároveň řešení musí být možno rozšířit (po dokoupení odpovídajících licencí) o další instance požadovaných skenerů.	[redacted]
6	Kontrola zranitelností musí reagovat na pravidly definované události a případě naplnění podmínek (například nové neznámé zařízení) musí spustit automatizovaný sken zranitelností.	
7	Řešení musí umožňovat definici výjimek pro jednotlivé zranitelnosti dle různých kritérií tak, aby se nalezené zranitelnosti nepropagovaly v korelacích nebo v reportech.	
8	Řešení musí být schopno na základě historického výsledku skenů a informacích o nových zranitelnostech identifikovat zařízení, která mohou být ohrožena.	
9	Řešení musí umožňovat simulovat možné vektory útoku na topologii v síti a upozornit tak na mezery v konfiguraci nebo na kritické assety.	
10	Řešení musí obsahovat funkcionalitu pro výměnu standardizovaných informací informačně bezpečnostního charakteru jako jsou STIX nebo TAXII.	

Umělá inteligence

	Minimálními technickými požadavky na zařízení	Technická specifikace nabízeného zařízení
1	Řešení musí být schopno zapojit umělou inteligenci do vyšetřování incidentů, tak aby ulehčila práci analytikům. Pokud jsou pro tuto funkci požadovány licence, musí odpovídat požadavkům EPS a FPM.	[redacted]
2	Umělá inteligence musí minimálně doplňovat informace o hrozbách nalezených v incidentech a informace o jejich možném šíření včetně vizualizace.	
3	Umělá inteligence musí doporučovat další kroky při řešení incidentů, a to na základě sledování historie řešení útoků/incidentů.	

Support a servis

	Minimálními technickými požadavky na zařízení	Technická specifikace nabízeného zařízení
1	Softwarová podpora – v průběhu služby počínaje podpisem smlouvy dodávka supportních služeb výrobce SIEM a jeho součástí	[redacted]
2	Servisní služby – v průběhu poskytované služby požaduje objednatel zabezpečení následujících činností spojených s podporou a rozvojem SIEM řešení v rozsahu minimálně 24 MD/rok následně: 1. Úprava konfigurace SIEM: • Vytváření / změny profilů; • Vytváření reportů; 2. Ladění SIEM systému: • Úprava korelačních pravidel a detekčních metod k odstranění false-positive událostí; 3. Upgrade SIEM systému (služba dle katalogu dodavatele); • Zajištění služby upgrade, odladění upgrade a jeho nasazení • Analýza vhodných modulu, informace o těchto modulech, instalace a ladění 4. Profylaxe SIEM, správa ROOT oprávnění, Helath monitoring 5. Školení pro nové uživatele, popř. oživení pro stávající uživatele (služba dle katalogu dodavatele); 6. Konzultace návazných aktivit v rámci bezpečnosti a řízení IT (služba dle katalogu dodavatele) • Výběr a instalace vhodných doplňkových modulů pro SIEM; • Prověřování vybraných událostí detekovaných SIEM; • Procesní zajištění řešení detekovaných událostí a/nebo bezpečnostních incidentů; • Integrace na 3rd party systémy	

Zadavatel spadá pod působnost zákona č. 181/2014 Sb., zákon o kybernetické bezpečnosti, ve znění pozdějších předpisů a 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). V případě kancelářského vybavení (scannery, tiskárny, faxy) se na zadavatele vztahuje § 4 a příloha č. 4 vyhlášky o kybernetické bezpečnosti, pro stupeň 3 vysoká.

Paměťové médium dodávané jako součást SIEM musí být plně ve správě zadavatele a při ukončení nájmu a obměně pronajatého zařízení nebo servisním zásahu nemůže být dodavateli vráceno. Dodavatel vždy zajistí demontáž vadného pevného disku a předá jej zadavateli, který zajistí jeho likvidaci v souladu s ustanovením vyhlášky č. 82/2018 Sb.

Příloha č. 2

Dohoda o mlčenlivosti

Smluvní strany:
ISECO.CZ s.r.o.
se sídlem Bartůňkova 2349/3a, 149 00 Praha 4
zastoupena: Ing. Tomášem Dedkem, jednatelem
IČO: 03641074
DIČ: CZ03641074
Bank. spojení: [redacted]
dále jen „**poskytovatel**"

a

Česká republika – Kancelář Poslanecké sněmovny
se sídlem: Sněmovní 176/4, 128 26 Praha 1 – Malá Strana
zastoupena: Mgr. Janem Morávkem, vedoucím Kanceláře Poslanecké sněmovny
osoba oprávněna jednat ve věcech smluvních: Ing. Mgr. Naďa Formanová, ředitelka odboru hospodářské správy, na základě pověření vedoucího zaměstnance k jednání jménem státu ze dne 1. 7. 2017
IČO: 00006572
DIČ: CZ00006572
bankovní spojení: ČNB Praha, číslo účtu: 5622001/0710
datová schránka ID: bykaigw
dále je **„objednatel"**

Smluvní strany ujednávají následující:

1. Smluvní strany prohlašují, že veškeré důvěrné podklady a důvěrné informace, které od sebe navzájem získají, budou použity výhradně pro potřebu přípravy a realizace projektu. Tyto důvěrné informace nebudou poskytnuty v žádné formě třetím osobám ani nebudou použity smluvními stranami k žádnému dalšímu účelu, pokud nedojde k písemné dohodě, která by nakládání s informacemi tohoto charakteru upravila způsobem odlišným.

2. Smluvní strany se zavazují po zde sjednanou dobu ochraňovat důvěrné informace obvyklým způsobem, přinejmenším však, jako by se jednalo o důvěrné informace jejich vlastní.
3. Za důvěrné podklady a důvěrné informace podle předchozího odstavce se bez ohledu na formu jejich zachycení považují veškeré podklady a informace, které byly některou ze smluvních stran označeny jako důvěrné, a které se týkají zmíněného projektu jeho plnění anebo podklady a informace, které se týkají přímo některé ze smluvních stran (zejména osobní údaje, obchodní tajemství, informace o činnosti, struktuře, hospodářských výsledcích, know-how, připravovaných projektech apod.).
4. Smluvní strany se dále zavazují považovat za důvěrné podle tohoto ustanovení taktéž veškeré neveřejné informace, mající povahu obchodního tajemství, vzájemně získané ústním podáním některé ze smluvních stran.
5. Po skončení projektu se strany této dohody zavazují vrátit si vzájemně do tří pracovních dnů veškeré si v písemné či elektronické podobě poskytnuté důvěrné podklady a důvěrné informace, případně zničit jejich elektronický tvar na nosičích ve vlastním systému.
6. O postupu dle bodu 5. bude pořízen dvojmo zápis, v němž bude toto prohlášení obsaženo, a každá smluvní strana obdrží jeden výtisk podepsaný přítomnými zástupci obou smluvních stran.
7. Tato dohoda se netýká informací, obsažených ve veřejně dostupných materiálech, které smluvní strany poskytují svým anonymním zákazníkům nebo klientům v jakékoli formě. Týká se však takových informací, které jsou vypracovány přímo pro druhou smluvní stranu, jsou takto označeny a mají současně povahu informací, uvedených v bodu 1. této dohody.
8. Závazkem ochrany veškerých informací, uvedených v bodu 1. této dohody, jsou smluvní strany vázány od okamžiku podpisu této dohody s tím, že závazek ochrany důvěrných informací zůstává v platnosti i po ukončení projektu.
9. Bez ohledu na výše uvedená ustanovení se za důvěrné nepovažují informace, které:
   - se staly veřejně známými, aniž by to zavinila záměrně či opomenutím strana přijímající dle této dohody důvěrnou informaci,
   - měla přijímající strana legálně k dispozici před uzavřením této dohody, pokud takové informace nebyly předmětem jiné, dříve mezi smluvními stranami uzavřené smlouvy o ochraně informací,
   - jsou výsledkem postupu, při kterém k nim přijímající strana dospěje nezávisle a je to schopna doložit svými záznamy nebo informacemi třetí strany, bez ohledu na to, zda obsahuje důvěrné informace či nikoli,
   - po podpisu této dohody poskytne přijímající straně třetí osoba, jež takové informace přitom nezíská přímo ani nepřímo od strany, jež je jejich vlastníkem.

V Praze dne 30. září 2020

……

objednatel

Ing. Mgr. Naďa Formanová,
ředitelka odboru hospodářské správy

Ing. Mgr. Naďa Formanová
Digitální podpis: 30.09.2020 11:56

V Praze dne …….

……

poskytovatel

Ing. Tomáš Dedek,
jednatel

Tomáš Dedek
Digitálně podepsal Tomáš Dedek
Datum: 2020.10.01 10:19:01 +02'00'