Spolufinancováno Evropskou unií

MINISTERSTVO PRO MÍSTNÍ ROZVOJ ČR

SMLOUVA

„Modernizace a rozšíření bezpečnostní infrastruktury Kanceláře veřejného ochránce práv“
podle zákona č. 89/2012 Sb., občanského zákoníku
(dále jen „smlouva“)

uzavřená níže uvedeného dne, měsíce, roku mezi následujícími smluvní stranami:

1. **O2 Czech Republic a.s.**
   se sídlem/místem podnikání: Za Brumlovkou 266/2, 140 22 Praha 4
   zapsaný v obchodním rejstříku vedeném Městským soudem v Praze
   vložka B, oddíl 2322
   Identifikační číslo: 60193336
   DIČ: CZ60193336
   bankovní spojení: Komerční banka, a.s., pobočka Praha, č.ú.: [redacted]
   jednající: Josef Kukačka, Account Manager, na základě pověření ze dne 1.12.2023
   (dále jen „poskytovatel“)

a

2. **Kancelář veřejného ochránce práv, organizační složka státu**
   se sídlem: Údolní 658/39; 60200 Brno, Brno-město
   Identifikační číslo: 70836981
   bankovní spojení:
   ID datové schránky: jz5adky
   zastoupený: JUDr. Pavlem Pořízkem, Ph.D., vedoucím Kanceláře veřejného ochránce práv
   (dále jen „objednatel“);

obě dále také samostatně jako „smluvní strana“ a společně jako „smluvní strany“.

Preambule, účel

Tato smlouva se uzavírá na základě výsledku zadávacího řízení na 1. část veřejné zakázky s názvem „Modernizace a rozšíření bezpečnostní infrastruktury Kanceláře veřejného ochránce práv“ veřejného zadavatele Kancelář veřejného ochránce práv, organizační složka státu, se sídlem Údolní 658/39; 60200 Brno, Brno-město, identifikační číslo 70836981.

Uzavřením této smlouvy se naplní účely 1. části veřejné zakázky „Modernizace a rozšíření bezpečnostní infrastruktury Kanceláře veřejného ochránce práv“.

Článek 1
Předmět smlouvy, předmět plnění

Předmětem plnění je realizace technických opatření k modernizaci a rozšíření bezpečnostní infrastruktury zadavatele sestávající z těchto dílčích plnění:

1. Podrobný návrh cílového konceptu řešení
2. Firewall
3. NDR systém
4. EDR systém
5. LOG management systém
6. PAM systém
7. SIEM systém
8. Svolávací systém SAIW
9. Požadované služby a dodávky integrace
10. SOC

vše včetně projektového řízení a zajištění podpory provozu po dobu 5 let od úplného předání a převzetí. Obsah činností podpory provozu je určen v příloze č. 1 této smlouvy. Před úplným předáním a převzetím díla provádí poskytovatel rovněž podporu provozu příslušných již provedených částí plnění.

Podrobně je předmět plnění popsán v příloze č. 1 této smlouvy.

Článek 2
Způsob, čas dodání, místo dodání, odevzdání a převzetí, podmínky plnění

2.1 Poskytovatel se zavazuje předat předmět plnění do 8 měsíců od nabytí účinnosti smlouvy.

2.2 Toto plnění bude dodáno kompletní, včetně projektového řízení a včetně všech náležitostí nezbytných pro řádný provoz a zajištění podpory provozu po dobu 5 let.

2.3 Veškeré plnění se poskytovatel zavazuje dodat bez jakýchkoliv právních vad; dále se zavazuje převést na objednatele veškerá práva užívání tohoto plnění (licence) bez časového omezení.

2.4 Místem odevzdání (dodání a poskytnutí) a převzetí plnění je sídlo objednatele na adrese Údolní 658/39, 60200 Brno. Náklady odevzdávání a rizika spojená s odevzdáváním (dodáním) včetně dokladů a dokumentů vztahujících se k dodávce a dopravou do místa dodání, včetně vykládky a manipulace na místě dodání nese poskytovatel.

2.5 Plnění poskytovatele podle odst. 2.1 této smlouvy bude protokolárně odevzdáno poskytovatelem objednateli v místě dodání, objednatelem pak převzato v případě řádného splnění se všemi sjednanými vlastnostmi, a to formou Protokolu o odevzdání a převzetí, který bude podepsán oběma smluvními stranami osobami oprávněnými jednat jménem příslušné smluvní strany (dále jen „Protokol o odevzdání a převzetí“).

2.6 K převzetí v místě dodání je povinen poskytovatel vyzvat objednatele nejméně dva pracovní dny přede dnem dodání. Výzva poskytovatele bude písemná, doručení výzvy provedeno pomocí prostředků elektronické pošty nebo prostřednictvím provozovatele poštovních (kurýrních) služeb a v příloze výzvy dodán písemný návrh Protokolu o odevzdání a převzetí, podepsaný poskytovatelem ve dvojím vyhotovení.

Protokol o odevzdání a převzetí obsahuje nejméně tyto obsahové náležitosti:

- výkaz dodaných a zprovozněných předmětů, poskytnutého příslušenství a ostatních poskytnutých věcí, poskytnutých služeb a předaných dokladů a dokumentů vztahujících se k plnění;

- datum vystavení Protokolu o odevzdání a převzetí a podpis osoby oprávněné jednat za poskytovatele;
- uvedení data, v němž má dojít k podpisu Protokolu o odevzdání a převzetí objednatelem a označení místa, kde má být proveden podpis objednatele.

2.7 Objednatel je oprávněn odmítnout převzít vadné plnění poskytovatele v případě vad nebo jiných nedostatků, a to bez ohledu na jejich množství a povahu nebo neobsahuje-li Protokol o odevzdání a převzetí obsahové náležitosti dle této smlouvy bez ohledu na počet nebo povahu chybějících náležitostí. Důvody odmítnutí budou objednatelem specifikovány v Protokolu o odevzdání a převzetí. V případě, že objednatel odmítne převzetí plnění poskytovatele, nepřechází na objednatele nebezpečí škody na žádné části plnění.

2.8 Poskytovatel je povinen umožnit objednateli provést kontrolu průběhu plnění dle této smlouvy, a to po celou dobu trvání této smlouvy.

2.9 Poskytovatel se zavazuje, že bude provádět činnosti za pomoci realizačního týmu, jehož členové jsou popsáni v příloze č. 2 smlouvy. Poskytovatel je oprávněn provést nahrazení členů realizačního týmu pouze s písemným souhlasem Objednatele. V takovém případě musí náhradníci původních členů realizačního týmu splňovat kvalifikační požadavky, které byly uvedeny v zadávací dokumentaci veřejné zakázky.

Článek 3
Cena

3.1 Poskytovateli náleží za řádné a úplné splnění předmětu smlouvy cena ve výši [redacted] + DPH ve výši [redacted]; cena včetně příslušné výše DPH činí [redacted].

3.2 Cena jednotlivých dílčích plnění dle této smlouvy je sjednána v příloze č. 3 této smlouvy.

3.3 Cena dle čl. 3.1 této smlouvy byla stanovena na základě zadávacího řízení na veřejnou zakázku „Modernizace a rozšíření bezpečnostní infrastruktury Kanceláře veřejného ochránce práv“ a obsahuje veškeré náklady poskytovatele nutné k plnění poskytovatele při realizaci předmětu této smlouvy po celou dobu stanovenou touto smlouvou a veškeré výdaje poskytovatele, spojené s plněním závazků poskytovatele v souvislosti s plněním smlouvy.

3.4 Vedle případů upravených dále v čl. 8 této smlouvy je změna ceny dle čl. 3.1 této smlouvy možná, pokud při realizaci předmětu plnění dojde ke změnám zákonných sazeb DPH. V tomto případě se cena upraví podle výše sazby DPH platné v době vzniku zdanitelného plnění, v takovém případě bude vyhotoven dodatek k této smlouvě a účinnost této změny nastává v návaznosti na účinnost změny příslušného obecně závazného daňového právního předpisu.

Článek 4
Platební podmínky

4.1 Fakturace proběhne po dodání a převzetí celého díla (mimo podpory provozu po dobu 5 let).

4.2 Objednatel uhradí cenu na základě faktury - daňového dokladu, kterou poskytovatel vystavil a doručil objednateli.

4.3 Cenu dle vyúčtování fakturou - daňovým dokladem uhradí objednatel formou bezhotovostního převodu na účet poskytovatele uvedený v záhlaví této smlouvy. Faktura - daňový doklad musí obsahovat odkaz na tuto smlouvu a v příloze faktury - daňového dokladu kopie oboustranně podepsaného Protokolu o odevzdání a převzetí. Dále musí faktura - daňový doklad obsahovat veškeré náležitosti daňového dokladu stanovené příslušnými právními předpisy, zejména zákonem č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů. Faktura musí být

označena názvem projektu „Modernizace a rozšíření bezpečnostní infrastruktury Kanceláře veřejného ochránce práv“ a reg. číslem projektu: CZ.06.01.01/00/22_004/0000237.

4.4 Nebude-li faktura – daňový doklad splňovat veškeré výše uvedené náležitosti daňového dokladu, nebo bude-li mít jiné závady v obsahu, je objednatel oprávněn ji ve lhůtě její splatnosti poskytovali vrátit a poskytovatel je povinen vystavit a doručit objednateli fakturu – daňový doklad opravený či doplněný. V případě vrácení faktury – daňového dokladu dle předcházející věty se lhůta splatnosti přerušuje a nová lhůta splatnosti počíná běžet od počátku až dnem následujícím po dni, kdy byla opravená nebo doplněná faktura – daňový doklad splňující všechny náležitosti dle příslušných právních předpisů a požadavky dle této smlouvy, doručena objednateli.

4.5 Splatnost faktury – daňového dokladu činí dvacet jedna kalendářních dní a počítá se ode dne doručení objednateli.

4.6 Smluvní strany se dohodly, že dnem úhrady se rozumí den odepsání fakturované částky z účtu objednatele. Objednatel není v prodlení, uhradí-li fakturu - daňový doklad do dvaceti jedna kalendářních dní po jeho obdržení, byť úhrada proběhne po termínu, který je na faktuře - daňovém dokladu uveden jako den splatnosti.

4.7 Poskytovatel se zavazuje do 15 kalendářních dnů po uzavření této smlouvy poskytnout objednateli písemné potvrzení správce daně o své registraci k dani z přidané hodnoty.

4.8 Podpora provozu bude fakturována vždy za proběhlé kalendářní čtvrtletí.

Článek 5
Práva objednatele z vadného plnění poskytovatele

5.1 Práva objednatele z vadného plnění poskytovatele se podřizují dikci § 2615 až § 2619, § 2099 až § 2117 a přiměřeně rovněž § 2165 až § 2174 zákona číslo 89/2012 Sb., občanského zákoníku (dále jen „občanský zákoník“). Objednatel je oprávněn oznámit poskytovali vady předmětu plnění, popř. jeho částí bez zbytečného odkladu poté, kdy byly nebo mohly být zjištěny při vynaložení odborné péče, nejpozději však do dvou let od převzetí předmětu plnění Protokolem o odevzdání a převzetí, a zvolit si a písemně uplatit právo z vadného plnění. V případě, že objednatel oznámí vadu a/nebo uvede způsob, jakým se vada projevuje, a současně uplatní nárok na odstranění vady, Poskytovatel se zavazuje, že nastoupí v místě dodání k odstranění vady zboží nebo vadného plnění servisní podpory ve lhůtách uvedených v příloze č. 1 smlouvy – bod 3.4.7 a vadu odstraní nejpozději ve lhůtách dle v této větě citované pasáži přílohy č. 1 smlouvy. Odchylně od ostatních ujednání se poskytovatel se zavazuje opravit bezpečnostní chyby v kódu firewallu do 15 kalendářních dnů od oznámení vady nebo od zjištění, které učinil sám. Nenastoupí-li poskytovatel k odstranění oznámené vady ani do desíti pracovních dnů po obdržení oznámení, je objednatel oprávněn pověřit odstraněním vady jiný subjekt a veškeré takto vzniklé náklady je oprávněn objednatel požadovat a vymáhat na poskytovateli. Pokud to oprava vady umožňuje, dodavatel může odstranění vady provést i za použití vzdáleného připojení.

5.2 Poskytovatel poskytuje objednateli záruku za jakost celého plnění v délce dvou let ode dne převzetí předmětu Protokolem o odevzdání a převzetí.

Článek 6
Mlčenlivost

6.1 Není-li dále stanoveno jinak, poskytovatel je povinen zachovávat mlčenlivost o všech skutečnostech, které se dozví v souvislosti s plněním této smlouvy. Tento závazek se rovněž vztahuje na veškeré informace, které objednatel předá poskytovateli, a na veškeré skutečnosti, se kterými se poskytovatel seznámí při plnění této smlouvy, zejména, nikoliv výlučně, na skutečnosti tvořící předmět obchodního tajemství nebo důvěrnou informaci (dále jen „chráněné informace“).

6.2 Závazek mlčenlivosti je poskytovatel povinen zajistit mimo jiné tím, že bez předchozího písemného souhlasu objednatele nedojde k jakémukoli šíření chráněných informací, anebo jejich zpřístupnění třetím osobám. Splnění tohoto závazku nevylučuje rozmnožení chráněných informací pro potřeby

objednatele, které je nutné pro řádné plnění závazků objednatele vyplývajících z této smlouvy a zákona.

6.3 Závazek mlčenlivosti je poskytovatel povinen zachovávat jak po dobu plnění předmětu této smlouvy, tak po jejím dokončení; tohoto závazku jej může zprostit pouze objednatel svým písemným prohlášením.

6.4 Poskytovatel je povinen zajistit, že chráněné informace budou přístupné pouze zaměstnancům a/nebo jiným osobám, které se budou podílet na plnění předmětu této smlouvy (dále jen „oprávněné osoby"). Na vyžádání objednatele je poskytovatel povinen neprodleně objednateli poskytnout úplný seznam oprávněných osob (jméno a příjmení u fyzických osob a obchodní firmu a identifikační číslo u právnických osob).

6.5 Poskytovatel je povinen zajistit splnění závazku mlčenlivosti ve stejném rozsahu u oprávněných osob, a to tak, aby oprávněné osoby byly tímto závazkem vázány i po skončení pracovněprávního nebo jiného smluvního vztahu k poskytovateli.

6.6 Závazek mlčenlivosti se nevztahuje na následující kontroly, které mohou být prováděny a ve vztahu k nimž je poskytovatel povinen umožnit kontrolu dokumentů souvisejících s poskytováním plnění dle této smlouvy ze strany objednatele a jiných orgánů oprávněných k provádění kontroly, a to zejména Ministerstva financí České republiky, Nejvyššího kontrolního úřadu případně dalších orgánů oprávněných k výkonu kontroly ve veřejné správě nebo dalších institucí nebo osob, které tyto orgány pověří nebo zmocní ke kontrole.

Článek 7
Utvrzení smluvních závazků

7.1 Pokud bude poskytovatel v prodlení s odevzdáním (dodáním) předmětu plnění jeho části ve lhůtě dle odst. 2.1 čl. 2 této smlouvy nebo prodlení s poskytnutím služby servisní podpory v reakční době do dalšího pracovního dne, je objednatel oprávněn požadovat, aby poskytovatel zaplatil za každý den prodlení smluvní pokutu ve výši [redacted] (slovy: [redacted]. Nárokováním, resp. úhradou této smluvní pokuty poskytovatelem není dotčeno právo objednatele na náhradu škody, která na základě porušení závazku vznikla objednateli či třetím osobám, ani právo objednatele požadovat po poskytovateli úrok z prodlení z neuhrazené smluvní pokuty a objednatel je oprávněn domáhat se na poskytovateli případné náhrady škody v plné výši.

7.2 Pro případ porušení závazku mlčenlivosti poskytovatele dle této smlouvy, je poskytovatel povinen zaplatit objednateli smluvní pokutu ve výši [redacted] (slovy: [redacted] za každý jednotlivý případ porušení závazku. Nárokováním, resp. úhradou, této smluvní pokuty není dotčeno právo objednatele na náhradu škody, která mu na základě porušení závazku mlčenlivosti vznikla a objednatel je oprávněn domáhat se náhrady škody v plné výši.

7.3 Pro případ porušení závazku realizovat veřejnou zakázku pomocí realizačního týmu podle odst. 2.9 této smlouvy této smlouvy, je poskytovatel povinen zaplatit objednateli smluvní pokutu ve výši [redacted] (slovy: [redacted] za každý jednotlivý případ porušení závazku. Nárokováním, resp. úhradou, této smluvní pokuty není dotčeno právo objednatele na náhradu škody, která mu na základě porušení závazku mlčenlivosti vznikla a objednatel je oprávněn domáhat se náhrady škody v plné výši.

7.4 Smluvní strany se dohodly, že smluvní pokuta je splatná patnáctý kalendářní den od doručení písemné výzvy objednatele k její úhradě poskytovali.

Článek 8
Změna závazku ze smlouvy, zánik smlouvy

8.1 Změna závazku ze smlouvy je možná, nastanou-li zákonné předpoklady dle zákona č. 134/2016 Sb., o zadávání veřejných zakázek (dále jen „zákon o zadávání veřejných zakázek"), pro dovolenou změnu závazku ze smlouvy jako smlouvy na veřejnou zakázku a dohodnou-li se smluvní strany na takové dovolené změně dle objednatelem vystaveného smluvního dodatku, doručeného

poskytovali, akceptovaného poskytovatelem a poté doručeného objednateli, či uzavřeného mezi přítomnými zástupci či pověřenými osobami jednajícími jménem smluvních stran.

8.2 Objednatel je oprávněn odstoupit od smlouvy v těchto případech:

a) Smluvní strany shodnou vůlí dospěly k závěru, že pokračování plnění smlouvy by bylo porušením pravidel a zákonných požadavků dovolujících uzavření dovolené změny závazku ze smlouvy dle příslušného ustanovení zákona o zadávání veřejných zakázek.

b) V případech dle zákona o zadávání veřejných zakázek, které opravňují objednatele odstoupit od této smlouvy.

8.3 Smlouva nebo část smlouvy v rozsahu nesplněného závazku poskytovatele zaniká vedle případů stanovených výše v odst. 8.1 nebo 8.2, nebo případů dle občanského zákoníku, také:

a) dohodou smluvních stran, v jejímž obsahu je dohodnuto též vzájemné vyrovnání účelně vynaložených nákladů,

b) odstoupením od celé smlouvy objednatelem nebo odstoupením od části smlouvy v rozsahu nesplněného předmětu plnění nebo nesplněné části předmětu plnění poskytovatele vymezené objednatelem v odstupovacím úkonu pro její podstatné porušení poskytovatelem, kterým se rozumí:

- prodlení poskytovatele s plněním kteréhokoli závazku této smlouvy vymezeného dobou, buď lhůtou, nebo dnem splnění, delším než patnáct kalendářních dní nebo
- marné uplynutí objednatelem stanovené náhradní lhůty k dodáním předmětu plnění včetně dokladů a dokumentů vztahujících se k plnění v případě, že se poskytovatel ocitl v prodlení s řádným dodáním předmětu plnění včetně dokladů a dokumentů vztahujících se k němu, pokud byl objednatelem výslovně písemně upozorněn na jeho prodlení;

c) odstoupením objednatele od smlouvy v případě, že na majetek poskytovatele je vedeno insolvenční řízení nebo byl insolvenční návrh zamítnut pro nedostatek majetku poskytovatele, či poskytovatel vstoupí do likvidace.

8.4 Odstoupení od smlouvy objednatel oznámí poskytovali písemně a je považováno za účinné okamžikem doručení písemného oznámení o odstoupení poskytovali. Účinky odstoupení od smlouvy se netýkají smluvních závazků souvisejících se závazkem mlčenlivosti a závazkem hradit jednotlivé smluvní pokuty, úroku z prodlení, pokud již dospěl do dne odstoupení, nároku na náhradu škody včetně nároku na náhradu škody, vzniklé porušením utvrzeného smluvního závazku, vypořádání smluvních stran po odstoupení ani ujednání, které má vzhledem ke své povaze zavazovat smluvní strany po odstoupení.

8.5 Objednatel je oprávněn vypovědět smlouvu během poskytování podpory provozu. Výpovědní doba započne běžet doručením výpovědi poskytovateli a činí 3 měsíce. Poskytovatel není oprávněn objednatele za tento právní úkon jakkoliv postihovat.

Článek 9
Komunikace

9.1 Veškerá sdělení v souvislosti se vznikem, změnou nebo zánikem závazků plynoucích z této smlouvy musí být formulována písemně a podepsána osobou oprávněnou jednat jménem příslušné smluvní strany a adresována na sídla (adresy) smluvních stran specifikovaná v hlavičce této smlouvy. Tato sdělení mohou být doručována osobně, doporučenou poštou, faxem nebo provozovatelem poštovních (kurýrních) služeb a budou považována za doručená okamžikem písemného potvrzení jejich přijetí. Sdělení doručená v den, který není dnem pracovním, budou považována za doručená v nejbližší následující pracovní den. Obě smluvní strany jsou povinny zajistit příjem poštovních (kurýrních) zásilek doručovaných na uvedené adresy. Za doručení zásilky podle této smlouvy se bude považovat i případ, kdy provozovatel poštovních (kurýrních) služeb zásilku vrátí odesílateli, neboť se adresát nezdržoval na uvedené adrese nebo odmítl zásilku z jakéhokoliv důvodu převzít. Dnem doručení bude v takovém případě den oznámení o neúspěšném doručení zásilky.

9.2 Ostatní sdělení, příkazy, požadavky, výzvy a úkony týkající se plnění závazků z této smlouvy se zavazují smluvní strany činit písemně prostřednictvím provozovatele poštovních (kurýrních) služeb

nebo písemně prostředky elektronické komunikace a to následujícími kontaktními osobami smluvních stran:

Za objednatele:

- 
- 

Za poskytovatele:

- 
- 

Článek 10
Uveřejnění uzavřené smlouvy, smluvních dodatků, skutečně uhrazené ceny

10.1 Smluvní strany stanoví dohodou, že (i) žádné ustanovení této smlouvy nepodléhá obchodnímu tajemství dle ustanovení § 504 občanského zákoníku, ani neobsahuje důvěrnou informaci o poměrech smluvní strany nebo skutečnostech, které má smluvní strana potřebu ochraňovat jako důvěrnou informaci nebo předmět obchodního tajemství, a (ii) poskytovatel souhlasí se zveřejněním této smlouvy na profilu zadavatele objednatele podle zákona o zadávání veřejných zakázek nebo v registru smluv dle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv, ve znění pozdějších předpisů (dále jen „zákon o registru smluv“).

10.2 Poskytovatel bere na vědomí povinnost zveřejnění obsahu této smlouvy, změny smlouvy (v podobě uzavřeného smluvního dodatku) a skutečně uhrazené ceny podle povinností, které se stanoví ve smyslu zákona o zadávání veřejných zakázek a povinnost zveřejnění obsahu této smlouvy a změny smlouvy (uzavřeného smluvního dodatku) dle zákona o registru smluv. Pokud jsou naplněny požadavky zákona o zadávání veřejných zakázek, objednatel uveřejní znění uzavřené smlouvy včetně jejích změn a doplnění (tj. smluvních dodatků) a skutečně uhrazené ceny, pokud cena - dle uzavřené smlouvy včetně případného smluvního dodatku - dosáhne limitu, stanoveného zákonem o zadávání veřejných zakázek, nedojde-li k uveřejnění uzavřené smlouvy, nebo případně uzavřeného smluvního dodatku podle zákona o registru smluv.

10.3 Smluvní strany se dohodly, že poskytovatel sdělí objednateli bezprostředně po uzavření této smlouvy, nejpozději však do 5 pracovních dní po uzavření smlouvy, která data obsažená ve smlouvě, případně ve smluvním dodatku, jsou informací (informacemi), jejíž uveřejnění zapovídá § 3 odst. 1 zákona o registru smluv.

10.4 Splnění zákonné povinnosti podle zákona o registru smluv uveřejnit uzavřenou smlouvu, případně smluvní dodatek, v rozsahu dle § 5 odst. 1 zákona o registru smluv, nejde-li o výjimku z povinnosti uveřejnění podle § 2 zákona o registru smluv, provede objednatel.

10.5 Poskytovatel bere na vědomí, že objednatel je povinen zveřejnit či zpřístupnit obsah této smlouvy na základě právních předpisů, zejména dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů.

Článek 11
Závěrečná ustanovení

11.1 Smluvní strany se dohodly, že (i) poskytovatel není oprávněn postoupit smlouvu, práva a závazky nebo pohledávky z této smlouvy na třetí osobu, (ii) započtení pohledávky poskytovatele proti pohledávce objednatele lze pouze po dohodě smluvních stran a za podmínek stanovených příslušným právním předpisem.

11.2 Smluvní strany podpisem této smlouvy činí rovněž prohlášení, že neexistuje žádné ujednání, smlouva či řízení, ani ústní ujednání, které by nepříznivě ovlivnilo výkon jakýchkoliv práv a závazků dle této smlouvy. Současně smluvní strany potvrzují svým podpisem, že veškerá ujištění

a dokumenty, které byly poskytnuty poskytovatelem objednateli před uzavřením a po uzavření této smlouvy, jsou pravdivé, platné a právně vymahatelné.

11.3 Poskytovatel je povinen ve smyslu zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů, ve znění pozdějších předpisů, spolupůsobit při výkonu finanční kontroly.

11.4 Jestliže se ukáže jakékoliv ustanovení nebo ujednání této smlouvy jako neplatné nebo nevymahatelné nebo právně neúčinné, nedotýká se to ostatních ujednání nebo ustanovení této smlouvy. Smluvní strany se zavazují, že nahradí jakékoliv neplatné, neúčinné nebo nevymahatelné ustanovení nebo ujednání platným, účinným a vymahatelným ustanovením nebo ujednáním, které má stejný nebo obdobný smysl nebo účinek; učiní tak do patnácti pracovních dnů od doručení výzvy jedné smluvní strany druhé smluvní straně.

11.5 Tato smlouva a veškeré mimosmluvní závazky vyplývající z této smlouvy se řídí a vykládají v souladu s právem České republiky, zejména občanským zákoníkem. Použití dispozitivních ustanovení právních předpisů je však vyloučeno v rozsahu, ve kterém by mohlo měnit význam, účel nebo interpretaci kteréhokoliv ustanovení této smlouvy.

11.6 Smluvní strany se zavazují, že budou postupovat v souladu s oprávněnými zájmy druhé smluvní strany, a že uskuteční veškerá právní jednání, která se ukáží být nezbytná pro realizaci závazků upravených touto smlouvou. Závazek součinnosti se vztahuje pouze na takové úkony, které přispějí či mají přispět k dosažení účelu této smlouvy.

11.7 Veškeré změny a doplnění jednotlivých ujednání nebo ustanovení této smlouvy mohou být provedeny při splnění předpokladů dle odst. 8.1 této smlouvy pouze formou vzestupně číslovaného písemného dodatku podepsaného oběma smluvními stranami a výslovně nazvaným dodatek ke smlouvě; písemná forma se vyžaduje i pro jiná právní jednání smluvních stran včetně změny písemné formy. Odpověď smluvní strany přijímající návrh na uzavření dodatku smlouvy s doplněním nebo odchylkou není přijetím návrhu dodatku na jeho uzavření. Smluvní strany mohou namítnout neplatnost změny smlouvy nebo doplnění smlouvy nebo jiného právního jednání, která nebudou učiněna v souladu s tímto odstavcem i v případě, že již bylo plněno.

11.8 Tato smlouva nabývá platnosti a účinnosti dnem podpisu oběma smluvními stranami.

11.9 Tato smlouva se vyhotovuje ve třech stejnopisech a každý stejnopis má platnost originálu, z toho jedno vyhotovení obdrží poskytovatel a dvě vyhotovení objednatel.

11.10 Smluvní strany prohlašují, že smlouva byla uzavřena podle jejich vážné a svobodné vůle, že nejednají v omylu či tísni, smlouvu si přečetly, považují obsah této smlouvy za určitý a srozumitelný, jsou jim známy veškeré skutečnosti, jež jsou pro uzavření této smlouvy rozhodující, a na důkaz toho připojují ke smlouvě své podpisy.

11.11 Poskytovatel je povinen archivovat a uchovávat veškerou originální dokumentaci týkající se veřejné zakázky uvedené v Preambuli, účelu této smlouvy a s plněním této smlouvy minimálně do konce roku 2035. Zároveň poskytovatel musí zajistit dostupnost všech originálů dokumentů a dokladů týkající se veřejné zakázky uvedené v Preambuli, účelu této smlouvy a plnění této smlouvy pro kontroly prováděné oprávněnými osobami (např. Nejvyšší kontrolní úřad, Ministerstvo financí ČR – Auditní orgán, Evropská komise, Evropský účetní dvůr, Evropský úřad pro boj proti podvodům, Úřad pro ochranu hospodářské soutěže, Orgán finanční správy) minimálně do konce roku 2035.

Přílohy:

Příloha č. 1 – Specifikace předmětu plnění

Příloha č. 2 – Seznam realizačního týmu

Příloha č. 3 – Rozpis ceny plnění

V Brně dne *shodném s datem el. podpisu*

Josef Kukačka

Digitálně podepsal Josef Kukačka
Datum: 2025.06.27 08:04:54 +02'00'

za poskytovatele:

Josef Kukačka, Account Manager, na základě pověření ze dne 1.12.2023

V Brně dne *shodném s datem el. podpisu*

Pavel Pořízek

Digitálně podepsal Pavel Pořízek
Datum: 2025.06.30 11:41:16 +02'00'

za objednatele:

JUDr. Pavel Pořízek, Ph.D.

vedoucí Kanceláře veřejného ochránce práv

Příloha č.1 - Specifikace předmětu plnění

1. Předmět nabídky

Předmětem nabídky dodavatele je dodávka níže uvedených technologií a všech souvisejících služeb poptávaných zadavatelem v příloze 1 zadávací dokumentace, tedy v dokumentu „Technická specifikace k veřejné zakázce „Modernizace a rozšíření bezpečnostní infrastruktury Kanceláře veřejného ochránce práv“.

Konkrétně:

- Řešení bude implementováno do stávajícího stavu popsaném v kapitole 3.1 přílohy č.1 zadávací dokumentace;
- Řešení zahrnuje všechny požadované dodávky a základní služby popsané v kapitole 3.2 přílohy č.1 zadávací dokumentace;
- Rozsah zajištění funkčních a nefunkčních požadavků je specifikován níže v rámci popisu plnění jednotlivých funkcí a funkčních celků nabízeného řešení;
- Řešení zahrnuje všechny další požadované služby uvedené v kapitole 3.4 přílohy č.1 zadávací dokumentace;

V rámci nabízeného plnění dodavatel zajistí modifikaci architektury bezpečnostních řešení, dle požadavků zadavatele a v souladu s požadovaným cílovým konceptem, který bude zpracován v úvodu projektu.

V rámci implementace plnění (viz jednotlivé technologie níže) dojde k převodu stávající HW appliance na virtuální appliance, tam kde to bude technicky možné a bude to v souladu s požadavky zadavatele. Technologie budou provozovány na dodaném HW, který je specifikován v Příloha č. 1.2 – Technické podmínky – část 2.docx.

Virtualizovány budou technologie LM, SIEM a PAM. NDR bude dodáno dle požadavku zadavatele jako HW a nahradí stávající řešení.

AV+EDR+MFA bude dodáno jako klientské řešení pro koncové stanice a servery a způsob nasazení bude realizován dle odsouhlaseného cílového konceptu tak, aby co nejvíce vyhovoval potřebám zadavatele.

2. Nabízené technologie

2.1 FW systém pro ochranu perimetru

Na základě požadavku zadavatele a v souladu s požadavky stanovenými Přílohou č.1.1.1 Technické specifikace: „Funkční a nefunkční požadavky částí plnění veřejné zakázky“ pro část FW dodavatel nabízí:

Popis řešení:

Kernun Security Appliance (KSA), což je síťové bezpečnostní řešení vyvinuté českou společností Trusted Network Solutions (TNS). Jde o komplexní firewall a proxy systém, který slouží k ochraně sítí a uživatelů před kybernetickými hrozbami. Jeho hlavní výhodou je vysoká míra konfigurovatelnosti a přehledné řízení síťového provozu.

Hlavní vlastnosti Kernun Security Appliance:

- Firewall – chrání síť před neoprávněným přístupem.
- Web proxy a URL filtr – umožňuje detailní řízení a filtrování webového provozu.
- Antivirová ochrana – integrace s různými antiviry (např. ClamAV, Kaspersky).
- Podrobný log a reportování – přehledná vizualizace provozu, výstrah a chyb.
- Autentizace uživatelů – možnost integrace s Active Directory nebo LDAP.
- Detekce anomálií a hrozeb – systém varuje před neobvyklým chováním.
- Reverzní proxy – ochrana serverů před útoky z internetu.

Součástí řešení jsou i licence potřebné k provozu FW v HA režimu po dobu 5 let a dodání řešení vč. supportu/servisní podpory na dobu 5 let. Podpora bude zahrnovat všechny updaty i upgrady, telefonická nebo emailová podpora výrobce v rozsahu nejméně 8x5 (8-16 hod., po-pá).

2.1.1 Funkční a nefunkční požadavky na FW

Nabízené plnění zajistí naplnění požadovaných funkčních a nefunkčních požadavků v následujícím rozsahu:

ID	Název požadavku	Popis splnění požadavku
FW01	Základní funkce	Budou dodány 2 centrální firewally, ve formě HW Appliance, které umožní: • poskytování HA (High Availability = vysoká dostupnost) • terminování zabezpečených spojení, • správu bezpečnostních politik, • správu MFA (multifaktorová autentizace)
FW02	Základní požadavek na implementaci	Implementace vč. uvedení do pilotního provozu bude obsahovat tyto aktivity: • Přenesení komplexních FW pravidel (bezpečnostních politik) a nastavení ze starých FW na nové FW; • Aktualizace dokumentace, školení uživatelů; • Vyhodnocení pilotního provozu a realizace nápravných opatření.
FW03	Analýza síťového provozu	Firewall bude provádět analýzu síťového provozu v reálném čase k identifikaci potenciálních hrozeb a anomálií.
FW04	Systém detekce útoků	Firewall bude obsahovat systém detekce útoků (IDS), který dokáže detekovat a zabránit neoprávněným pokusům o přístup.
FW05	Filtrace na úrovni aplikace	Firewall bude být schopen filtrovat a řídit provoz na základě protokolů a atributů aplikací.
FW06	Podpora virtuálních soukromých sítí (VPN)	Firewall bude podporovat připojení pomocí virtuálních soukromých sítí (VPN) pro bezpečný vzdálený přístup.
FW07	Autentizace uživatelů	Firewall bude poskytovat mechanismy autentizace uživatelů, aby bylo zajištěno, že pouze autorizovaní uživatelé mají přístup do sítě.
FW08	Filtrace obsahu	Firewall bude mít schopnost filtrovat obsah a blokovat přístup k nevhodným nebo škodlivým webovým stránkám.
FW09	Řízení provozu	Firewall bude umožňovat řízení přístupu k webovým stránkám na základě příslušnosti přihlášeného uživatele koncové stanice do doménových skupin.

ID	Název požadavku	Popis splnění požadavku
FW10	Ochrana provozu	Firewall bude disponovat systémem detekce nebezpečných spojení s napojením na databázi známých a lokálně významných nebezpečných IP adres.
FW11	Systém odchytávání útoků	Firewall bude disponovat systémem pro detekci podezřelých spojení (Honeypot) pomocí TCP handshaku na zvoleném seznamu portů a adres.
FW12	Rozšiřitelnost	Firewall bude umožňovat propojení vícero rozhraní do jednoho (agregace) pro případ nutnosti navýšení propustnosti nebo zvýšení robustnosti.
FW13	Vzdálený servisní zásah	Firewall bude poskytovat zabezpečený způsob připojení ze sítě dodavatele, nedostupný z veřejného internetu, pro případ nutnosti zásahu servisního týmu.
FW14	Řízení adresace	Firewall bude poskytovat systém řízení adresace interní sítě pomocí DHCP serveru.
FW15	Kontrola DNS	Firewall bude poskytovat systém překladu doménových jmen (DNS) pro poskytování klientům interní sítě.
FW16	Doménová jména	Firewall bude podporovat zadávání pravidel provozu na webové servery pomocí doménových jmen. Firewall musí pro taková pravidla podporovat tzn. hvězdičkovou notaci (např. *.google.com).
FW17	Paralelní verze	Firewall bude umožňovat instalaci více verzí firmwaru zároveň s možností bezztrátového návratu k předchozí verzi firmware.
FW18	Bezpečnostní komunita	Firewall bude moct být zapojen do komunitního systému ochrany dodavatele, který umožní sdílení informací o bezpečnostních hrozbách.
FW19	Škálovatelnost	Firewall bude snadno škálovatelný, aby se mohl přizpůsobit růstu sítě a zvýšenému provozu.
FW20	Vyvažování zátěže	Firewall bude podporovat techniky vyvažování zátěže pro rovnoměrné rozložení síťového provozu a prevenci úzkých míst.
FW21	Vysoká dostupnost	Firewall bude mít vysokou dostupnost, minimalizovat výpadky a zajišťovat nepřetržitou ochranu sítě.
FW22	Tolerance vůči chybám	Firewall bude navržen s mechanismy pro toleranci vůči chybám a minimalizaci dopadu hardwarových nebo softwarových poruch.
FW23	Zálohování a obnova	Firewall bude poskytovat mechanismy pro pravidelné zálohování a obnovu pro ochranu konfigurace a dat.
FW24	Šifrování dat	Firewall bude podporovat silné protokoly pro šifrování dat, aby ochránil citlivé informace při přenosu.
FW25	Detekce proniknutí	Firewall bude mít schopnost detekovat a monitorovat potenciální pokusy o neoprávněný přístup.
FW26	Auditování a záznamování	Firewall bude generovat audity a poskytovat komplexní funkcionalitu pro záznamování pro účely dodržování předpisů a forenzní analýzy.
FW27	Ochrana proti přehřátí	Firewall bude zajišťovat ochranu proti přehřátí. Informovat o tomto stavu a zajistit ochranu proti vnitřnímu přehřátí.

ID	Název požadavku	Popis splnění požadavku
FW28	Snadná konfigurace	Firewall bude mít uživatelsky přívětivé rozhraní a intuitivní možnosti konfigurace pro snadné spravování a nastavení.
FW29	Vzdálené monitorování a správa	Firewall bude podporovat možnosti vzdáleného monitorování a správy pro efektivní správu distribuovaných prostředí.
FW30	Uživatelské rozhraní	Firewall bude mít dobře navržené a intuitivní uživatelské rozhraní pro efektivní monitorování a administraci.
FW31	Integrace s existujícími systémy	Firewall bude bezproblémově integrován s existující infrastrukturou sítě a bezpečnostními systémy.
FW32	Podpora standardních protokolů	Firewall bude podporovat standardní síťové protokoly pro bezproblémovou komunikaci s dalšími zařízeními a systémy.
FW33	Výkon	• Výkon IPS – min. 5 Gbps vč. Logování – konkrétně 6 Gbps • Výkon Threat Protection – min. 3 Gbps vč. Logování – konkrétně 5 Gbps • IPsec VPN výkon (512 bytů) - min. 5 Gbps vč. Logování – konkrétně 5,2 Bbps • SSL-VPN výkon - min. 2 Gbps vč. Logování – konkrétně OpenVPN 2.2 Bbps • Současná TCP spojení – min. 2 500 000 – konkrétně 2 500 000 • Nová spojení za sekundu (TCP) – min. 200 000 – konkrétně 250 000
FW34	HW požadavky	• Rozhraní – min. 10x1 GE RJ45, možnost rozšíření o min. 4x10 SFP+ další sítová rozhraní – konkrétně 10x1 Gbps s možností uvedeného rozšíření + 4x1 Gbps síťová rozhraní • Management rozhraní – min 1 Gbe RJ45 – konkrétně 1 Gbps RJ45 • Uložiště – integrovaný pevný disk, minimálně 480GB – konkrétně 960 Gbps
FW35	Jazyk	Uživatelské rozhraní firewallu bude dostupné kompletně v Českém jazyce, a to včetně všech dokumentačních materiálů.

2.2 NDR systém (Network Detection & Response)

Na základě požadavku zadavatele a dle Přílohy 1.1.1 Technické specifikace: „Funkční a nefunkční požadavky částí plnění veřejné zakázky“ pro část NDR řešení dodavatel nabízí:

- **sondu Progress Flowmon Probe 10 000 SFP+**
- **centrální kolektor Flowmon Collector R1-1000**
- vše s podporou výrobce Standard Support na 60 měsíců

Popis řešení:

Sondu bude osazena nejčastěji využívaným modulem – ve specifikaci SFP+ SR. Do tohoto portu bude z centrálního přepínače přivedena kopie monitorovaného provozu. Flow záznamy budou ze sondy posílané (přes 1G Cu port) do centrální ho kolektoru, kde budou uložené a zároveň zpracovávané moduly Monitoring Centrum.

Tato konfigurace bude jinak dále fungovat shodně se stávajícím řešení.

Dodavatel předpokládá využití stávající licence Flow Mon ADS s tím, že licence bude přesunuta ze stávající sondy do nově dodávaného konektoru.

Součástí řešení je rovněž support/servisní podpora na dobu 5 let. Podpora bude zahrnovat všechny updaty i upgrady a telefonickou nebo emailovou podporu v rozsahu nejméně 8x5 (8-16 hod., po-pá).

2.2.1 Funkční a nefunkční požadavky na NDR

Nabízené plnění zajistí naplnění požadovaných funkčních a nefunkčních požadavků v následujícím rozsahu:

ID	Název požadavku	Popis splnění požadavku
NDR01	Shoda se standardy	Nabízené řešení zajistí tyto podpory: • Podpora standardů NetFlow v5, NetFlow v9, IPFIX pro export i příjem statistik o síťovém provozu v souladu s příslušnými RFC pro dané standardy • Podpora pro spolehlivý a bezpečný přenos dat ve formátu IPFIX mezi sondami a kolektorem v souladu s RFC 7011 • Podpora pro nastavení času aktivní a neaktivní expirace toků (RFC 3954). Řešení dále zajistí to, že události bude možné automaticky exportovat do systémů typu log management nebo SIEM prostřednictvím protokolu syslog ve standardizovaném formátu CEF Systém bude obsahovat REST API, které pokrývá přístup k datům i konfiguraci. REST API je plnohodnotně dokumentované a oficiálně podporované výrobcem
NDR02	Obecné požadavky na monitorování	Vlastnosti nabízeného monitorování: • Monitorování v pasivním režimu (SPAN/TAP) a aktivním režimu (GRE/ERSPAN). • Monitorování MAC adres • Monitorování VLAN tagů.
NDR03	Monitorování výkonnostních parametrů sítě:	Z pohledu výkonnostních parametrů se budou monitorovat: • round trip time, • server response time, • TCP retransmise.
NDR04	Monitorování odezvy aplikací	Budou se monitorovat odezvy aplikací: • Pro protokoly http, HTTPS • Pro MS SQL, Pstgre SQL a My SQL
NDR05	Monitorování odezvy aplikací	V rámci monitorování odezvy aplikací budou k dispozici následující metriky: • network transport time (doba přenosu požadavku a odpovědi), • application response time (odezva aplikační transakce).
NDR06	Monitorování výkonu a odezvy aplikací proti definovanému SLA	Systém umožní monitorovat skutečnou odezvu aplikací z pohledu uživatele, tj. monitorovat transakce jednotlivých uživatelů v reálném čase bez nutnosti instalovat softwarové agenty na servery nebo koncové stanice. Systém umožní pro každou aplikaci, resp. i její část definovat SLA pro dobu odezvy. Systém kontinuálně bude hodnotit všechny uživatelské transakce a stanoví celkový index výkonu aplikace na základě plnění SLA

ID	Název požadavku	Popis splnění požadavku
NDR07	Identifikace a extrakce metadat	Indexace a extrakce metadat bude možná: • z aplikačního protokolu http • z aplikačního protokolu SSL/TLS vč. TLS 1.3. • z aplikačního protokolu DNS • z aplikačního protokolu DHCP • z aplikačního protokolu SMTP
NDR08	Exporty statistik	Řešení bude obsahovat uživatelsky definované šablony pro export statistik o síťovém provozu ve formátu IPFIX
NDR09	Vizualizace statistik	Řešení obsahuje vizualizaci s těmito parametry: • Vizualizace statistik o provozu datové sítě v 5 minutových, 1 minutových nebo 30 sekundových intervalech, • Zobrazování výkonnostních metrik v grafech • Systém umožňuje zpracovávat dotazy na dlouhé časové intervaly s délkou minimálně 1 měsíc • Systém umožňuje agregovat síťové statistiky podle libovolných atributů a sumarizovat podle různých kritérií • Susystém poskytuje mu souhrnné informace o nejvýznamnějších událostech, nových incidentech (nebyly zaznamenány v předchozím období), rizikových stanicích a trendech. • Systém podporuje pokročilé dashboardy s libovolným počtem pohledů na data. Uživatel může sdílet dashboard s dalšími uživateli
NDR10	Detekce útoků	Systém bude obsahovat funkcionalitu detekce útoků, bezpečnostních incidentů a anomálií kombinací tradičního IDS pro identifikaci známých útoků a hrozeb základě signatur s moderní behaviorální analýzou pro detekci neznámých/nových útoků na základě analýzy chování.
NDR11	Threat intelligence	Výrobce bude poskytovat automatické, pravidelné aktualizace databáze známých indikátorů kompromitace (tzv. threat intelligence) a databáze signatur.
NDR12	Záchyt provozu	Na základě události bude možné automaticky spustit záchyt provozu v plném rozsahu. Záchyt provozu bude cílený
NDR13	Reporting	Systém bude obsahovat předdefinovanou sadu reportů s možností plné konfigurace uživatelem. Reporty budou obsahově ekvivalentní s dashboardy a umožní zobrazit veškeré informace, které je možné zobrazit na dashboardu. Reporty budou dostupné prostřednictvím webového uživatelského rozhraní, ve formátu PDF nebo CSV
NDR14	Autentizace uživatelů	Systém bude využívat integraci LDAP/AD pro autentizaci a autorizaci uživatelů. V rámci konfigurace bude možné prostřednictvím uživatelského rozhraní manuálně mapovat skupiny v rámci LDAP/AD na role v systému

ID	Název požadavku	Popis splnění požadavku
NDR15	Zálohování a obnova logů o aktivitě na síti	• K řešení bude možné připojit standardizované datové úložiště (např. Samba, NFS, S3). • Objem zálohovaných dat nebude licenčně omezen a bude limitován pouze kapacitou úložiště. • Data, která budou předmětem zálohování bude možné definovat pomocí libovolné kombinace atributů záznamů o síťovém provozu. Takových definic půjde možné vytvořit větší počet, bez explicitního omezení. • Zálohování dat probíhá pravidelně, minimálně jednou za 24 hodin. • Zálohovaná data bude možné v případě potřeby obnovit tak, aby tato data bylo možné analyzovat standardními prostředky řešení identicky jako data, která jsou standardně v systému dostupná.
NDR16	Podpora pro FlowLogs	Systém bude připravený na monitoring datového provozu v prostředí AWS nebo Azure s využitím technologie tzv. FlowLogs. Obsahuje nativní podporu pro VPC FlowLogs v případě AWS a NSG FlowLogs v případě Azure.
NDR17	Pokročilé zpracování flow dat	Systém umožní přijímat data ve formátu NetFlow/IPFIX z vlastních senzorů. Tato data bude následně možné předávat do systémů třetích stran včetně duplikace, filtrování a konverze formátu.
NDR18	Modelování topologie	Systém umožní vytvářet libovolné logické nebo fyzické topologie a na tyto topologie mapovat síťový provoz, resp. libovolně filtrovaný síťový provoz. Půjde modelovat a vizualizovat prostředí datové sítě, význačné systémy a zobrazovat jejich síťový provoz a vytížení
NDR19	Záchyt provozu s krátkodobým bufferem	Nabízené řešení umožní selektivní záznam datového provozu v plném rozsahu ve formátu PCAP pro následnou analýzu. Zároveň bude k dispozici krátkodobá paměť pro datový provoz, který bezprostředně předcházel spuštění záchytu provozu. Záchyt bude integrován se systémem detekce anomálií a umožní v případě signifikantní detekce provoz automaticky zaznamenat
NDR20	Automatická analýza záchytů provozu ve formátu PCAP	Nabízené řešení umožní automaticky analyzovat obsah záchytu provozu ve formátu PCAP s cílem identifikovat příčiny provozních a výkonnostních problémů bez nutnosti manuální analýzy v nástroji třetí strany a bez specifických znalostí v oblasti paketové analýzy

2.3 EDR systém (Endpoint Detection & Response)

Na základě požadavku zadavatele a dle Přílohy 1.1.1 Technické specifikace: „Funkční a nefunkční požadavky částí plnění veřejné zakázky“ pro část EDR řešení nabízí dodavatel produkt od společnosti ESET, a to konkrétně **ESET PROTECT Elite** v celkovém objemu **250 ks licencí** určených pro koncová zařízení.

Popis řešení:

ESET PROTECT Elite kombinuje prevenci, detekci, reakci a XDR funkci s vícevrstvou ochranou. Nabízené řešení obsahuje všechny požadované moduly, konkrétně se jedná o Antivirové řešení, EDR řešení, MFA a SandBox. Řešení je možné nasadit s centrální správou v cloudu i lokálně. Konkrétní způsob nasazení bude upřesněn v rámci cílového konceptu.

ESET PROTECT Elite je ucelené řešení pro organizace, které potřebují mít o svých sítích podrobný přehled.

Funkce pokročilé detekce a reakce na podnikové úrovni zajistí, že nově vznikající hrozby, lehkomyslné chování zaměstnanců a nežádoucí aplikace neohrozí vaši firemní reputaci nebo zisk.

ESET PROTECT Elite proaktivně reaguje na neustále se vyvíjející hrozby. Vaši kybernetickou obranu posílí o několik průběžně inovovaných ochranných vrstev, které pokrývají koncová zařízení, e-mail, aplikace pro spolupráci v cloudu a úložiště.

Toto řešení zahrnuje technologii ochrany proti pokročilým hrozbám, která pomáhá předcházet zcela novým, dosud neznámým hrozbám, průběžně vyhodnocuje zranitelnosti. Využívá při tom určování priority řešení podle rizik, což snižuje míru vystavení útokům, a nabízí šifrování celého disku nebo vícefaktorové ověření posilující ochranu dat a identit.

Podrobnou specifikaci je možné zobrazit na webu výrobce řešení společnosti ESET

Součástí nabízeného plnění je rovněž support/servisní podpora na dobu 5 let. Podpora zahrnuje všechny updaty i upgrady, telefonickou nebo emailovou podporu výrobce v rozsahu nejméně 8x5 (8-16 hod. po-pá).

2.3.1 Funkční a nefunkční požadavky na EDR

Nabízené plnění zajistí naplnění požadovaných funkčních a nefunkčních požadavků v následujícím rozsahu:

Požadavky na ANTIVIR

ID	Popis splnění požadavku	
AV01	Podporované klientské platformy	Podporované platformy jsou min.: Windows, Linux, MacOS, Android, vše v českém jazyce
AV02	Nativní podpora architektur pro platformy Windows a MacOS:	Podporované architektury jsou x86, x84, ARM64

ID	Popis splnění požadavku	
AV03	Rozsah funkcionalit	Antimalware, antiransomware, antispyware a anti-phishing pro aktivní ochranu před všemi typy hrozeb. Dále IPS, Application control, Device control, Security Memory (zabraňuje útokům na běžící aplikace), kontrola integrity systémových komponent. Dále ochrana proti pokročilým hrozbám (APT) a zero-day zranitelnostem
AV04	Personální firewall	Součástí řešení je i personální firewall pro zabránění neautorizovanému přístupu k zařízení se schopností automatického přebrání pravidel z brány Windows Firewall.
AV05	Ochrana operačního systému	Součástí řešení je i Modul pro ochranu operačního systému a eliminaci aktivit ohrožující bezpečnost zařízení s možností definovat pravidla pro systémové registry, procesy, aplikace a soubory.
AV06	Implementované ochrany	Součástí řešení je i ochrana před neautorizovanou změnou nastavení / vyřazení z provozu / odinstalací antimalware řešení a kritických nastavení a souborů operačního systému.
AV07	Heuristická analýza	Součástí řešení je i aktivní i pasivní heuristická analýza pro detekci dosud neznámých hrozeb.
AV08	Ochrana proti zero-day zranitelnostem	Součástí řešení je i systém pro blokaci exploitů zneužívajících zero-day zranitelností, jenž pokrývá nejpoužívanější vektory útoku: • síťové protokoly, • Flash Player, • Javu, • Microsoft Office, • webové prohlížeče, • e-mailové klienty, • PDF čtečky… • Systém pro detekci malwaru již na síťové úrovni poskytující ochranu i před zneužitím zranitelností na síťové vrstvě. • Kontrola šifrovaných spojení (SSL, TLS, HTTPS, IMAPS…).
AV09	Anti-phishing	Součástí řešení je i anti-phishing se schopností detekce homoglyph útoků.
AV10	Kontrola RAM paměti	Součástí řešení je i kontrola RAM paměti pro lepší detekci malwaru využívající silnou obfuskaci a šifrování.
AV11	Kontrola souborů	Součástí řešení je i: • Cloud kontrola souborů pro urychlení skenování fungující na základě reputace souborů. • Kontrola souborů v průběhu stahování pro snížení celkového času kontroly • Kontrola souborů při zapisování na disku a extrahování archivačních souborů
AV12	Heuristická analýza	Součástí řešení je i detekce hrozeb a zranitelností s využitím strojového učení.
AV13	Ochrana proti botnetu	Součástí řešení je i funkce ochrany proti zapojení do botnetu pracující s detekcí síťových signatur.
AV14	Ochrana před síťovými útoky	Součástí řešení je i ochrana před síťovými útoky skenující síťovou komunikaci a blokující pokusy o zneužití zranitelností na síťové úrovni.

ID	Popis splnění požadavku	
AV15	Kontrola aplikací	Součástí řešení je i kontrola s podporou cloudu pro odesílání a online vyhodnocování neznámých a potenciálně škodlivých aplikací.
AV16	Lokální sandbox	Součástí řešení je i lokální sandbox
AV17	Behaviorální analýza	Součástí řešení je i modul behaviorální analýzy pro detekce chování nových typů ransomwaru.
AV18	Systém reputace	Součástí řešení je i systém reputace pro získání informací o závadnosti souborů a URL adres.
AV19	Detekce nového mallwaru	Součástí řešení je i cloudový systém pro detekci nového malwaru ještě nezaneseného v aktualizacích signatur
AV20	Úvodní skenování	Součástí řešení je i skener firmwaru, BIOSu a UEFI
AV22	Skenování souborů v cloudu OneDrive.	Součástí řešení je i skenování souborů v cloudu OneDrive.
AV23	Funkcionalita pro klienty	• MS Windows – Antimalware, Antispyware, Personal Firewall • MacOS – Personal Firewall, Device control, autoupgrade.
AV24	Bezpečnostní politiky	Součástí řešení je i možnost aplikování bezpečnostních politik i v offline režimu na základě definovaných podmínek.
AV25	Automatické vytváření dump souborů	Součástí řešení je i podpora automatického vytváření dump souborů na stanici na základě nálezů.
AV26	Okamžité blokování/mazání napadených souborů	Součástí řešení je i okamžité blokování/mazání napadených souborů na stanici (s možností stažení administrátorem k další analýze).
AV27	Duální aktualizační profil	Součástí řešení je i Duální aktualizační profil pro možnost stahování aktualizací z mirroru v lokální síti a zároveň vzdálených serverů při nedostupnosti lokálního mirroru (pro cestující uživatele s notebooky).
AV28	Spouštění web stránek v chráněném režimu	Součástí řešení je i možnost definovat webové stránky, které se spustí v chráněném režimu prohlížeče, pro bezpečnou práci s kritickými systémy nebo internetovým bankovnictví.
AV29	Aktivní ochrany před útoky hrubou silou	Součástí řešení je i systém aktivní ochrany před útoky hrubou silou na protokol SMB a RDP.
AV30	Blokování IP adres	Součástí řešení je i možnost zablokování konkrétní IP adresy po sérii neúspěšných pokusů o přihlášení pro protokoly SMB a RDP s možností výjimek ve vnitřních sítích.
AV31	Automatické aktualizace	Součástí řešení jsou i automatické aktualizace bezpečnostního softwaru s možností odložení restartu stanice.
AV32	„Zmražení“ na požadované verzi	Součástí řešení je i tzv. „Zmražení“ na požadované verzi – produkt je možné nakonfigurovat tak, aby nedocházelo k automatickému povyšování majoritních a minoritních verzí zejména na stanicích, kde se vyžaduje vysoká stabilita.

Požadavky na SANDBOX

ID	Popis splnění požadavku
SB01	Funkce cloudového sandboxu je integrována do produktu pro koncové a serverové zařízení, tzn. Cloudový sandbox, který nemá vlastního agenta, nevyžaduje instalaci další komponenty ať už v rámci produktu nebo implementace HW prvku do sítě.
SB02	Sandbox umožňuje spuštění vzorků malwaru pro Windows a Linux.
SB03	Řešení je možné využívat na koncových bodech a serverech pro aktivní detekci škodlivých souborů.
SB04	Součástí řešení je analýza neznámých vzorků v řádu jednotek minut.
SB05	Sandbox lze optimalizovat pro znemožnění obejití anti-sandbox mechanismy.
SB06	Řešení má schopnost analýzy rootkitů a ransomwaru.
SB07	Součástí řešení je schopnost detekce a zastavení zneužití nebo pokusu o zneužití zero day zranitelnosti.
SB08	Dodávané řešení pracuje s behaviorální analýzou.
SB09	Sandbox zobrazí kompletní výsledek o zanalyzovaném souboru včetně informace o nalezeném i nenalezeném škodlivém chování daného souboru.
SB10	Nabízené řešení umožnuje manuální odeslání vzorku do sandboxu.
SB11	Řešení nabízí možnost proaktivní ochrany, kdy je potenciální hrozba blokována, dokud není znám výsledek analýzy ze sandboxu.
SB12	Součástí řešení je neomezené množství odesílaných souborů.
SB13	Řešení Sandboxu zajišťuje veškerou komunikaci šifrovaným kanálem.
SB14	Dodávané řešení umožnuje okamžitě odstranění souboru po dokončení analýzy v cloudovém sandboxu.
SB15	Součástí rešení jemožnost volby, jaké kategorie souborů do cloudového sandboxu budou odcházet (spustitelné soubory, archivy, skripty, pravděpodobný spam, dokumenty atp.)
SB16	Do cloudovéhé sandboxu je možné odeslat soubory o velikosti 64MB.
SB17	Součástí nabízeného řešení Sandbox jsou automatizovaně distribuované výsledky analyzovaných souboru všem serverům a stanicím napříč organizací, tak aby nedocházelo k duplicitnímu testování.

Požadavky na vlastní EDR

ID	Popis splnění požadavku
EDR01	Součástí nabízeného řešení EDR je provoz centrálního serveru on-premise na platformě Windows Server.
EDR02	Nabízené řešení EDR obsahuje funkcionalitu webová konzole pro správu a vyhodnocení.
EDR03	Řešení EDR umožňuje provozu s databázemi MS SQL a My SQL.
EDR04	Nabízení řešení EDR má možnost provozu v offline prostředí.
EDR05	Součástí řešení EDR je autonomní chování se schopností vyhodnotit podezřelou/ škodlivou aktivitu a zareagovat na ni i bez aktuálně dostupného řídícího serveru nebo internetového připojení.
EDR06	Součástí nabízeného řešení je i funkcionalita logování činností administrátora (Audit Log).

ID	Popis splnění požadavku
EDR07	Součástí řešení je podpora EDR pro systémy Windows, Windows server, MacOS a Linux.
EDR08	Nabízené řešení splňuje požadavek na autentizaci do managementu EDR pomocí 2FA.
EDR09	Součástí řešení je možnost řízení managementu EDR prostřednictvím API, a to jak pro přijímání informací z EDR serverů, tak i pro zasílání příkazů na EDR servery.
EDR10	Součástí nabízeného řešené EDR je i integrovaný nástroj v EDR řešení pro vzdálené zasílání příkazů přímo z konzole.
EDR11	Součástí nabízeného řešení EDR je možnost izolace zařízení od sítě.
EDR12	Součástí nabízeného řešení EDR je možnost tvorby vlastních IoC.
EDR13	Nabízené řešení splňuje požadavek na možnost škálování množství historických dat vyhodnocených v EDR: • až 3 měsíce pro raw-data • až 3 roky pro detekované incidenty
EDR14	Nabízené řešení splňuje požadavek na funkcionalitu “Učící režim“ pro automatizované vytváření výjimek k detekčním pravidlům.
EDR15	Součástí nabízeného řešení EDR jsou indikátory útoku pracující s behaviorální detekcí.
EDR16	Součástí nabízeného řešení EDR je funkcionalita indikátorů útoku pracující s reputací.
EDR17	Nabízeného řešené EDR umožnuje analýzu vektorů útoku.
EDR18	Řešení EDR, které nabízím má schopnost detekce škodlivých spustitelných souborů: • skriptů, • exploitů, • rootkitů, • síťových útoků, • zneužití WMI nástrojů, • bezsouborového malwaru • škodlivých systémových ovladačů / kernel modulů. • pokusů o dump přihlašovacích údajů uživatele
EDR19	Součástí řešení je i schopnost detekovat laterální pohyb útočníka.
EDR20	Nabízené řešení EDR umožnuje analýzu procesů, veškerých spustitelných souborů a DLL knihoven.
EDR21	Řešení obsahuje funkcionalitu náhledu na spuštěné skripty použité při detekované události.
EDR22	Součástí řešení je možnost zabezpečeného vzdáleného spojení přes servery výrobce do konzole EDR.
EDR23	Nabízené řešení EDR má schopnost automatizovaného response úkonu pro jednotlivá detekční pravidla v podobě: • izolace stanice, • blokace hash souboru, • blokace a vyčištění sítě od konkrétního souboru, • ukončení procesu, • restart počítače, • vypnutí počítače.

ID	Popis splnění požadavku
EDR24	Součástí řešení EDR je podpora automatického vyřešení incidentu administrátorem.
EDR25	Nabízené řešení EDR umožnuje prioritizaci vzniklých incidentů.
EDR26	Součástí řešení je možnost stažení spustitelných souborů ze stanic pro bližší analýzu ve formátu archivu opatřeným heslem.
EDR27	Nabízené řešení EDR obsahuje integrace a zobrazení detekcí provedených antimalware produktem.
EDR28	Součástí řešení je funkcionalita generování tzv. forest / full execution tree model.
EDR29	Nabízené řešení EDR umožnuje vyhledávání pomocí nově vytvořených IoC nad historickými daty.
EDR30	Nabízení řešení je provázáno s technikami popsanými v knowledge base MITRE ATT&CK.
EDR31	Nabízené řešení EDR obsahuje integrovaný vyhledávač VirusTotal s možnost rozšíření o vlastní vyhledávač.

Požadavky na management konzolí

ID	Popis splnění požadavku
MK01	Součástí nabízeného řešení je Management konzole pro správu všech řešení v rámci nabízeného balíku, Provedení webové konzole. Možnost instalace na Windows i Unix.
MK02	Součástí nabízeného řešení je předpřipravená virtual appliance pro virtuální prostředí VMware, Microsoft Hyper-V a Microsoft Azure.
MK03	Součástí nabízeného řešení je Server/proxy architektura pro síťovou pružnost – snížení zátěže při stahování aktualizací detekčních modulů výrobce.
MK04	Součástí nabízeného řešení je možnost probuzení klientů pomocí Wake On Lan.
MK05	Nabízené řešení obsahuje funkcionalitu Vzdálené vypnutí, restart počítače nebo odhlášení všech uživatelů.
MK06	Nabízené řešení má možnost konfigurace virtual appliance přes uživatelsky přívětivé webové rozhraní.
MK07	Součástí řešení je nezávislý management agent pro platformy Windows, Linux a MacOS.
MK08	Součástí řešení je management agent pro architektury na platformách Windows a MacOS: • x86, • x64, • ARM64
MK09	Součástí nabízení funkcionality je nezávislý agent (pracuje i offline) vzdálené správy pro zajištění komunikace a ovládání operačního systému klienta.
MK10	Součástí nabízeného řešení je offline uplatňování politik a spouštění úloh při výskytu definované události (například: odpojení od sítě při nalezení škodlivého kódu).
MK11	Nabízené řešení obsahuje administrace v nejpoužívanějších jazycích včetně češtiny.
MK12	Nabízené řešení má široké možnosti konfigurace oprávnění administrátorů (například možnost správy pouze části infrastruktury, které konkrétnímu administrátorovi podléhá).
MK13	Nabízení řešení je zabezpečeno pro přístup administrátorů do vzdálené správy pomocí 2FA.
MK14	Součástí nabízení funkcionality je štítků/tagování pro snazší správu a vyhledávání.

ID	Popis splnění požadavku
MK15	Nabízené řešení umožnuje správu karantény s možností vzdáleného vymazání / obnovení / obnovení a vyloučení objektu z detekce.
MK16	Vzdálené získání zachyceného škodlivého souboru z klienta je součástí nabízeného řešení.
MK17	Funkce detekce nespravovaných (rizikových) počítačů komunikujících na síti je součástí nabízeného řešení.
MK18	Součástí řešení je i podpora pro instalace a odinstalace aplikací 3. stran.
MK19	Funkce vyčítání informací o verzích softwaru 3. stran je součástí nabízeného řešení.
MK20	Nabízení řešení umožňuje vyčítat informace o hardwaru na spravovaných zařízeních (CPU, RAM, diskové jednotky, grafické karty…).
MK21	Součástí řešení je možnost vyčíst sériové číslo zařízení.
MK22	Možnost vyčíst volné místo na disku je součástí nabízené funkcionality.
MK23	Nabízené řešení obsahuje detekci aktivního šifrování BitLocker na spravované stanici.
MK24	Zobrazení časové informace o posledním bootu stanice, je funkce, kterou obsahuje nabízené řešení.
MK25	Funkcionalita odeslání zprávy na počítač / mobilní zařízení, které se následně zobrazí uživateli na obrazovce je součástí nabízeného řešení.
MK26	Součástí řešení je vzdálená odinstalace antivirového řešení 3. strany.
MK27	Vzdálené spuštění jakéhokoli příkazu na cílové stanici pomocí Příkazového řádku je funkce, kterou obsahuje námi nabízené řešení.
MK28	Součástí nabízeného řešení jsou i dynamické skupiny pro možnost definování podmínek, za kterých dojde k automatickému zařazení klienta do požadované skupiny a automatickému uplatnění klientské úlohy.
MK29	Funkce automatické zasílání upozornění při dosažení definovaného počtu nebo procent ovlivněných klientů, je součástí nabízeného řešení. (například: 5 % všech počítačů / 50 klientů hlásí problémy).
MK30	Nabízené řešení podporuje SNMP Trap, Syslogu a qRadar SIEM.
MK31	Nabízení řešení podporuje formáty pro Syslog zprávy: • CEF • JSON • LEEF
MK32	Nabízení řešení podporuje instalaci skriptem – např. *.bat, *.sh, *.ini (GPO, SSCM…).
MK33	Součástí nabízené funkcionality je rychlé připojení na klienta pomocí RDP z konzole pro vzdálenou správu
MK34	Součástí nabízeného řešení je i možnost reportování stavu klientů chráněných jinými bezpečnostními programy.
MK35	Nabízení řešení má schopnost zaslat reporty a upozornění na e-mail.
MK36	Nabízená konzole podporuje multidoménové prostředí (schopnost pracovat s více AD strukturami).
MK37	Nabízená konzole podporuje multitenantní prostředí (schopnost v jedné konzoli spravovat více počítačových struktur).
MK38	Součástí nabízené funkcionality je i podpora VDI prostředí (Citrix, VMware, SCCM, apod.)
MK39	Nabízené řešení podporuje klonovaní počítačů za pomocí golden image.

ID	Popis splnění požadavku
MK40	Podpora instančních klonů, je součástí nabízeného řešení.
MK41	Podpora obnovy identity počítače pro VDI prostředí na základě FQDN, je součástí nabízené funkcionality.
MK42	Součástí řešení je i možnost definovat vícero jmenných vzorů klonovaných počítačů pro VDI prostředí.
MK43	Součástí nabízeného řešení je i přidání zařízení do vzdálené správy pomocí: • synchronizace s Active Directory, • ruční přidání pomocí dle IP adresy nebo názvu zařízení, • pomocí síťového skenu nechráněných zařízení v síti • Import skrze csv soubor.

Požadavky na MFA

ID	Název požadavku	Popis splnění požadavku
MFA01	Způsoby doručení OTP (One Time Password):	V nabízením řešení lze OTP doručit: • aplikací v mobilním zařízení, • e-mailem, • bezpečnostním tokenem, • SMS zprávou, (poznámka: Včetně možnosti konfigurace vlastní SMS brány pro doručení OTP kódu) • vlastní aplikací.
MFA02	Další možnosti ověření	Další možnosti ověření v nabízeném řešení jsou: • FIDO • Push Authnetication
MFA03	Existence aplikace výrobce s podporou Push-Notifications	Součástí nabízeného řešení jsou aplikace výrobce s podporou Push-Notifications pro platformy: • iOS • Android • watchOS, wear OS
MFA04	Požadavky na aplikaci výrobce (aplikace podporující push notifikace)	Nabízené řešení splňuje tyto požadavky na aplikaci výrobce (aplikace podporující push notifikace) • Mobilní aplikace v hlavních jazykových lokalizacích včetně češtiny • Přístup do mobilní aplikace ochráněn PINem / biometrikou • Možnost generovat OTP v off-line prostředí (bez internetové připojení, bez GSM spojení)
MFA05	Podporovaná zařízení	Nabízení řešení MFA podporuje: • Hardwarové tokeny HOTP splňující standard OATH • Hardwarové tokeny certifikované výrobcem • Kompletně softwarové řešení – bez nutnosti nákupu dalšího hardwaru • Podpora time based hardwarových tokenů (PSKC) • Self-enrollment uživatelů

ID	Název požadavku	Popis splnění požadavku
MFA06	Chráněné služby	Součástí řešení jsou tyto chráněné služby: • Přihlášení do webových aplikací společnosti Microsoft (OWA, SharePoint…), • Přihlášení přes RDP, • Exchange Control Panel & Exchange Administrator Center, • VMware Horizon View, • VPN služby využívajících protokol RADIUS (Cisco, Citrix, Fortinet, Juniper, Microsoft, OpenVPN…), • cloudové služby Office 365, G Suite, identity providerů (podpora SAML protokolu, podpora AD FS) • Lokálního přihlášení do Windows, Linux, macOS účtů • Vyžádání 2FA v nouzovém režimu Windows • Vyžádání 2FA při vyvolání UAC dialogu ve Windows • Vyžádání 2FA při uzamčeném účtu
MFA07	Správa řešení	Nabízení řešení nabízí tyto možnosti správy: • Webové konzole • Přístup do konzole lze chránit 2FA ověřením • Podpora multitenantního provozu (možnost spravovat vícero uživatelských struktur v jedné konzoli) • Podpora synchronizace uživatelských účtů z Active Directory • Možnost tvorby výjimek pro vnitřní sítě, kde není 2FA vyžadováno • Umožnit uživatelům přihlášení bez použití 2FA pro vybrané služby • Konzole umožňuje generovat Master recovery klíče pro konkrétní chráněné služby • Centrální správa a přidělování hardwarových tokenů jednotlivým uživatelům • Možnost reportování o úspěšných/ neúspěšných přihlášení uživatelů, způsobu použité autentizace (SMS, Push, OTP)
MFA08	Podpora integrace systémů třetích stran	Součástí nabízeného řešení je podpora integrace systémů třetích stran prostřednictvím: • API • SDK výrobce (Java, PHP, .NET, Windows Script Host)
MFA09	Shoda se standardy	Nabízení řešení je v souladu se standardem ISO027001.
MFA10	Limitace počtu offline přihlášení	Nabízené řešení umožnuje definovat maximální počet offline přihlášení.

2.4 Log Management systém

Na základě požadavku zadavatele a dle Přílohy 1.1.1 Technické specifikace: „Funkční a nefunkční požadavky částí plnění veřejné zakázky“ pro část LM Systém nabízí dodavatel produkt od společnosti ONE IDENTITY, a to konkrétně **Syslog-ng™ Store Box (SSB)** v celkovém objemu **250 ks licencí** určených pro monitorování jednotlivých zdrojů logů, a to v podobě virtuální appliance nasazené na dodávané servery.

Zadavatel již tento systém používá ve formě HW appliance a přechod na VA appliance tak nebude znamenat nutnost přeškolení personálu na nový typ řešení a komplikovanou migraci ze stávajícího řešení. Zadavatel tak získá modernější podobu stávajícího řešení, které již aktivně používá.

Popis řešení

Syslog-ng™Store Box (SSB) je zařízení pro správu logů s vysokým výkonem a spolehlivostí, které vychází z výhod syslog-ng™Premium Edition. SSB umožňuje sbírat a indexovat logová data, provádět složité vyhledávání, zabezpečit citlivé informace pomocí detailních přístupových politik, generovat zprávy pro prokázání souladu a předávat logová data nástrojům pro analýzu od třetích stran.

Výkon nabízeného řešení

SSB používá syslog-ng™Premium Edition jako agenty pro sběr logů. Instalátory jsou k dispozici pro více než 50 platforem, včetně nejoblíbenějších distribucí Linuxu, komerčních verzí UNIXu a Windows. Možná je také bezagentový sběr dat a přímé napojení na SSB.

V závislosti na své konfiguraci může syslog-ng™sbírat až 650 000 zpráv za sekundu. Indexační motor syslog-ng™Store Box je optimalizován pro výkon. V závislosti na přesné konfiguraci může jedno zařízení syslog-ng™Store Box sbírat a indexovat až 100 000 zpráv za sekundu po delší dobu.

Jedno zařízení SSB může sbírat logové zprávy z více než 10 000 zdrojů, když je nasazeno v konfiguraci klient-přeposílání.

Díky plnotextovému vyhledávání SSB můžete procházet miliardy logů během několika sekund prostřednictvím intuitivního webového uživatelské rozhraní. Zástupné znaky a Booleovské operátory vám umožňují provádět složité vyhledávání a hloubkově se zabývat výsledky. Nabízí automatickou funkci vyhledávání pro rychlejší detekci anomálií.

Soulad s předpisy a standardy

SSB dokáže vyhledávat v příchozích logových datech a posílat upozornění, když je detekována kritická událost. Uživatelé mohou snadno vytvářet přizpůsobené zprávy pro prokázání souladu s normami a předpisy, jako jsou PCI-DSS, ISO 27001, SOX a HIPAA.

SSB nabízí flexibilní schopnosti filtrování na základě meta-dat a obsahu zpráv k omezení vznikajícího šumu v prostředí s vysokým provozem a segmentaci dat pro lepší vyhledávání a analýzu.

PatternDB™ může klasifikovat přicházející logy v reálném čase na základě obsahu zpráv, extrahovat pojmenované informační prvky z nestrukturovaných logových zpráv, což vám umožní agregovat různé formáty logů pro vyhledávání a generování statistik.

Schopnosti parsování a přepisování vám umožňují transformovat a normalizovat logy na základě filtrů a výsledků PatternDB™ pro efektivní vyhledávání a analýzu.

Kapacita úložiště a uložení logů

S pomocí SSB lze ukládat velké množství logových dat, vytvářet automatizované zásady uchovávání a zálohovat data na vzdálené servery. Největší zařízení SSB může uchovávat až 40 terabajtů nekomprimovaných dat.

SSB poskytuje automatické archivování dat na vzdálené servery. Data na vzdáleném serveru zůstávají přístupná a vyhledatelná; několik terabajtů auditových stop lze přistupovat přes webové rozhraní SSB. SSB využívá vzdálený server jako síťový disk prostřednictvím protokolu Network File System (NFS) nebo protokolu Server Message Block (SMB/CIFS).

Je také možné přeposílat logy do analytických nástrojů od třetích stran nebo získávat data z SSB prostřednictvím jeho rozhraní REST API. K rozhraní API můžete přistupovat pomocí protokolu RESTful přes HTTPS, což znamená, že můžete použít jakýkoli programovací jazyk s přístupem k RESTful HTTPS klientovi k integraci SSB do svého prostředí, včetně populárních jazyků jako Java a Python.

Zabezpečení přenosu

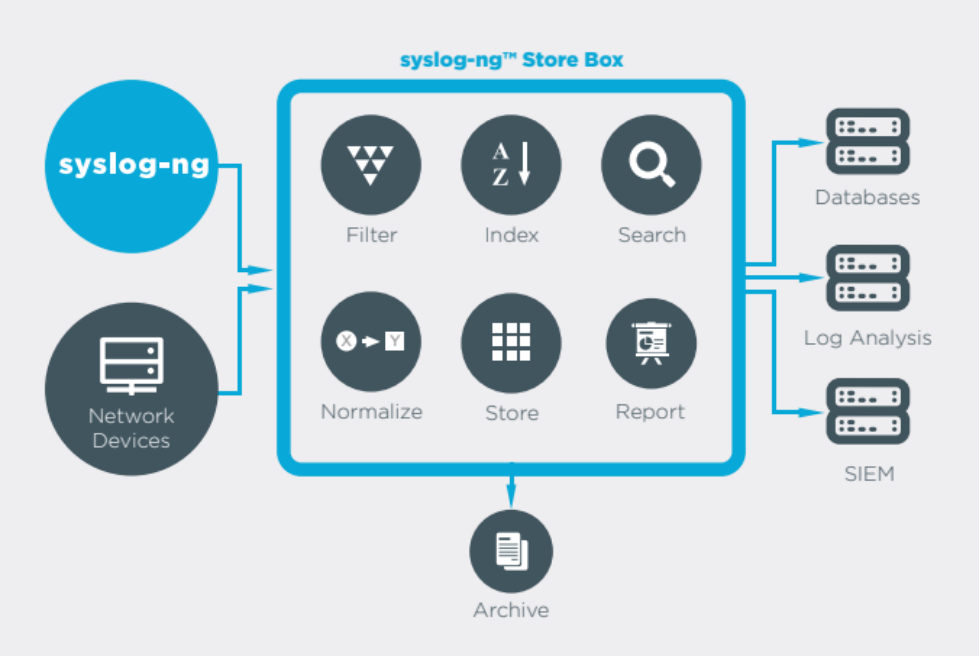
Logy mohou být přenášeny z klientů syslog-ng™ Premium Edition na SSB pomocí šifrování Transport Layer Security (TLS), což chrání veškerá citlivá data. TLS umožňuje vzájemnou autentizaci hostitele a serveru pomocí certifikátů X.509.

Logstore zařízení SSB ukládá logovací data ve šifrovaných, komprimovaných a časově razítkovaných binárních souborech, omezujíc přístup pouze na autorizované osoby.

Nastavení autentizace, autorizace a účtování (Authentication, Authorization and Accounting) poskytuje detailní řízení přístupu, omezující přístup k konfiguraci SSB a uloženým logům na základě oprávnění uživatelských skupin.

SSB lze integrovat s databázemi LDAP a RADIUS.

High-level architektura



Jedná se o komplexní řešení, které je optimalizováno pro použití společně se SIEM.

Součástí nabízeného plnění je rovněž support/servisní podpora na dobu 5 let. Podpora zahrnuje všechny updaty i upgrady, telefonickou nebo emailovou podporu výrobce v rozsahu nejméně 8x5 (8-16 hod. po-pá).

2.4.1 Funkční a nefunkční požadavky na Log Management systém

Nabízené plnění zajistí naplnění požadovaných funkčních a nefunkčních požadavků v následujícím rozsahu:

ID	Název požadavku	Popis splnění požadavku
LM01	Konfigurovatelnost přes GUI	Řešení je konfigurovatelné a ovládané přes webové GUI rozhraní.
LM02	Podpora HA	Řešení podporuje zapojení pro High Availability, tj. vysokou dostupnost.

LM03	Podpora vstupních protokolů	Řešení podporuje vstupní protokoly (sources ~ zdrojů log záznamů) a přenos dat:
		• SNMP
		• syslog:
		  ○ UDP (dle RFC 3164)
		  ○ TCP
		  ○ IETF (RFC 5424) + TLS
		• Aktivní sběr logů z databází (přes ODBC).
		• Agent/Client pro sběr log záznamů jak pro prostředí Windows, tak i pro prostředí Linux/Unix (HP-UX, Solaris, …)/AIX:
		  ○ sběr Windows EVT záznamů i z kontejnerů Windows Server.
		  ○ sběr AIX/Solaris/HP-UX/IRIX auditních OS záznamů.
		  ○ sběr textových logů ze souborů.
		  ○ přenos log dat (tj. forward přes syslog) šifrovaným kanálem.
		Podpora RELAY funkce (tj. přeposílací servery, např. pro infrastrukturu v DMZ)

LM04	Podpora BUFFER/CACHE	Řešení podporuje BUFFER/CACHE na výstupu jak u Agenta, tak pro RELAY, a také pro Server/Appliance
LM05	Výstupní protokoly	Řešení podporuje výstupní protokoly (destinations ~ umístění log záznamů): • syslog (UDP, TCP, IETF). • zápis logových dat napřímo do databází (ODBC). • zápis logových dat do JSON formátu. • SNMP Trap.
LM06	Pokročilé filtrování	Řešení umožňuje konfiguraci pokročilého filtrování logových záznamů (jakýkoli vstup logových dat prochází libovolnou sadou filtrů na libovolný výstup).
LM07	Ukládání log dat:	Řešení podporuje ukládání log dat: • Textové úložiště v originálním (RAW) formátu. • Šifrované úložiště (logspace) s podporou šifrování privátním klíčem/certifikátem a TSA podpisem, pro zajištění právních potřeb forenzního šetření. • Podpora indexace logových dat pro rychlé vyhledávání údajů i v nestrukturovaných v datech (položka message u syslog protokolu). • Podpora komprimace jako součást daného úložiště.
LM08	Řízení přístupů (AAA)	Řešení umožňuje řízení přístupů k LM: • řízení přístupu na úrovni jednotlivých úložišť (logspace). • podpora GROUP managementu. • podpora autentizace přes RADIUS. • Podpora lokální /externí databáze uživatelů – LDAP

ID	Název požadavku	Popis splnění požadavku
LM09	Zálohování, Archivace, Export, Sdílení log dat	Součástí řešení LM je i Zálohování, Archivace, Export, Sdílení log dat: • nezávislé zálohovací politiky jak pro konfiguraci, tak pro jednotlivá úložiště (logspace). • nezávislé archivační (data retention) politiky pro jednotlivá úložiště log dat. • podpora exportu/sdílení log dat v originálním i ve strukturovaném tvaru
LM10	Alerting	Součástí řešení LM je alerting: • RATE alerting (detekce změn „nestandardního chování zdrojů logových záznamů“ pro nastavené limitní hladiny datových přenosů v čase). • Výskyt definovaného slova/znaku v logu (Např. „error“, „fail“ nebo „alert“). • Artificial Ignorance – funkcionalita, která identifikuje, co je informačně nezajímavé a potlačuje eskalaci. Nebo identifikuje, co informačně systém Log managementu ještě nikdy neviděl a eskaluje anomálii.
LM11	Nezávislost na SIEM	Řešení je koncipováno jako čistý Log Management, nejedná se tedy o Event Management – pro plnou funkci není potřeba tvorby parserů. Řešení není provázáno na SIEM a je plně nezávislé jak fyzicky, tak logicky na SIEM řešeních. Nejedná se tedy o ALL-IN-ONE řešení, s konfigurací pro Log Management.
LM12	Vyhledávání a Reporting:	Řešení umožňuje: • Rychlé vyhledávání na základě fulltext indexace (vyhledávaní bez nutnosti tvorby parserů), tedy velké objemy dat se neprohledávají formou „grep like“ prohledávání po řádcích. • Umožnění vytváření vlastních analytických pohledů. • Dashboardy/Statistiky Log management infrastruktury. • Uživatelsky konfigurovatelný reporting strukturovaných dat (timestamp, facility, priority, tag, program, hostname, atd.). • Definice vlastních vyhledávacích filtrů a „pohledů“. • Podpora přístupů pro pohledy (co pohled to jiná skupina uživatelů).
LM16	Peering	Řešení podporuje peering: • Možnost přepojit více Log Management serverů a vyhledávání nad nimi přes jedno rozhraní. • Definice vyhledávacích filtrů a „pohledů“ nad „peeringovými“ servery. • Podpora přístupů pro pohledy (co pohled to jiná skupina uživatelů).
LM14	API rozhraní	Řešení umožňuje vyhledávání přes REST API rozhraní

2.5 PAM systém (Privileged Access Management)

Na základě požadavku zadavatele a dle Přílohy 1.1.1 Technické specifikace: „Funkční a nefunkční požadavky částí plnění veřejné zakázky“ pro část PAM Systém nabízí dodavatel produkt od společnosti ONE IDENTITY a to konkrétně **One Identity Safeguard for Privileged Sessions** (PAM) v celkovém objemu **25 ks SYSTEM licencí** určených pro monitorování privilegovaných uživatelů přistupujících k jednotlivým systémům zadavatele bez omezení počtu přistupujících uživatelů a to v podobě virtuální appliance nasazené na dodávané servery.

Zadavatel již tento systém používá ve formě HW appliance a přechod na VA appliance tak nebude znamenat nutnost přeškolení personálu na nový typ řešení a komplikovanou migraci ze stávajícího řešení. Zadavatel tak získá modernější podobu stávajícího řešení, které již aktivně používá.

Popis řešení

Nabízené řešení řeší problematiku s uděloványím nekontrolovaného privilegovaného přístupu interním administrátorům, externím dodavatelům, smluvním pracovníkům a poskytovatelům služeb může představovat významné riziko.

One Identity Safeguard for Privileged Sessions slouží pro kontrolu, monitoring a záznam privilegované relace administrátorů, vzdálených dodavatelů a dalších vysoce rizikových uživatelů.

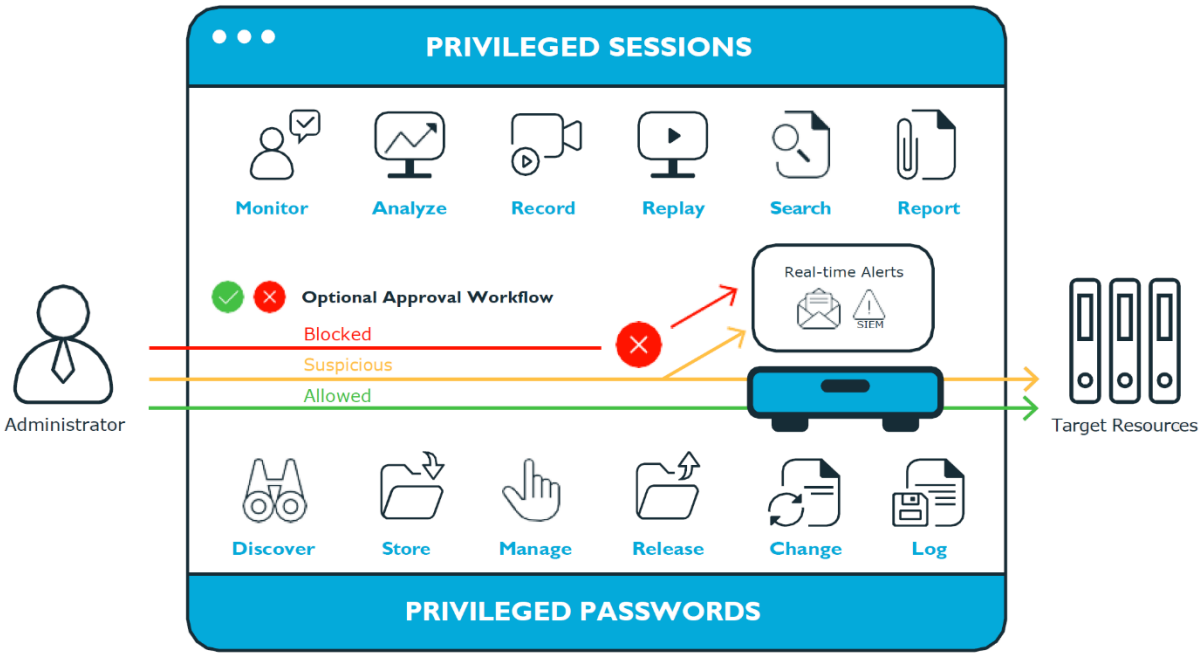
Obsah zaznamenaných relací je indexován, což usnadňuje vyhledávání událostí a automatizuje vytváření reportů.

Přesně dle požadavků One Identity Safeguard for Privileged Sessions funguje jako proxy server, který provádí inspekci síťového provozu na úrovni aplikačního protokolu. Tato kontrola vytváří efektivní ochranu proti útokům tím, že odmítá veškerý provoz porušující protokol.

V **transparentním režimu** jsou změny v síti minimální a uživatelé nemusí měnit svůj stávající pracovní postup ani klientské aplikace. Součástí bezpečnostních opatření jsou například požadavek na předběžnou autorizaci uživatele, omezení přístupu na konkrétní zdroje nebo zasílání upozornění při překročení stanoveného časového limitu připojení.

Safeguard také umožňuje **monitorování relací v reálném čase** a provádění různých akcí – pokud je detekován rizikový příkaz nebo spuštěna nebezpečná aplikace, může systém odeslat upozornění nebo okamžitě ukončit relaci. Pravidla pracovního postupu lze konfigurovat tak, aby byla přísnější podle vašich bezpečnostních požadavků.

Přesnější specifikace nasazení bude uvedena v rámci projektu. Dle požadavků zadavatele bude dodána VA appliance řešení a toto řešení bude provozováno na virtualizaci zákazníka.



Součástí nabízeného plnění je rovněž support/servisní podpora na dobu 5 let. Podpora zahrnuje všechny updaty i upgrady, telefonickou nebo emailovou podporu výrobce v rozsahu nejméně 8x5 (8-16 hod. po-pá).

2.5.1 Funkční a nefunkční požadavky na PAM

Nabízené plnění zajistí naplnění požadovaných funkčních a nefunkčních požadavků v následujícím rozsahu:

ID	Popis splnění požadavku
PAM01	Řešení podporuje zapojení pro High Availability, tj. vysoká dostupnost.
PAM02	Řešení je konfigurovatelné a ovládané přes webové GUI rozhraní.
PAM03	Řešení je bezagentové.
PAM04	Řešení je nezávislé na verzi OS cílových serverů.
PAM05	Řešení podporuje práci přes tyto protokoly: • Microsoft RDP • Citrix ICA • SSH • VNC i z SSL • TELNET i z SSL • HTTP/S • MS-SQL • SUDO log
PAM06	Řešení zahrnuje podporu aktualizace systému přes rozhraní produktu
PAM07	Součástí plnění jsou pravidelně vydávané aktualizace výrobcem. Minimálně 2x ročně.
PAM08	Řešení v rámci daných protokolů rozlišuje jejich kanály (např. CLIPBOARD, REMOTE PRINTER, REMOTE DISK atd.), u kterých je možné definovat: • Časové okna • Uživatelské skupiny • Rozsahy IP adres • Blokaci
PAM0910	Řešení je schopné detekovat pokusy o spuštění aplikace/příkazu a ukončit spojení uživatele.
PAM11	Řešení je schopné zaznamenat použité příkazy, titulky oken a použité aplikace
PAM12	Řešení je schopné analyzovat stisknuté klávesy a provádět behaviorální analýzu s cílem odhalit zneužití uživatelského účtu
PAM13	Řešení je schopné detekovat použití neautorizovaných skriptů
PAM14	Řešení má vestavěny mechanismus pro automatické skórování potencionálně rizikového chování privilegovaného uživatele (použití neobvyklé sekvence příkazů, odlišné chování při použití klávesnice a myši)
PAM15	Řešení umožňuje tvorbu black listů a white listů

ID	Popis splnění požadavku
PAM16	Vlastnosti Auditní stopy: • Přehráváni jako video s přesnou časovou stopou ze signalizací „hluchých míst“ kde se nic neděje. • Šifrování auditní stopy. • TSA časové razítko. • Možnost přehrání online i offilne • Možnost exportu dat v originální formátu
PAM17	Řízení přístupů „sessions“: • Řešení je schopné řídit přístupy v rámci „session“ dle ověření vůči LDAP/RADIUS. • Řešení podporuje možnost dvoufaktorové autentizace pro „session“. • Řešení podporuje režim „čtyř očí“. • Řešení podporuje integraci s externími programy typu ERPM, IDM. • Řešení zahrnuje API pro integraci s HelpDesk/ServiceDesk systémy.
PAM18	Řešení podporuje logování jak interních akcí, tak informací o „sessions“ pomocí syslog protokolu, podpora TLS nad syslog protokolem.
PAM19	Zálohování, Archivace, Export, Sdílení log dat: • Řešení zahrnuje nezávislé zálohovací politiky jak pro konfiguraci/interní databázi, tak pro jednotlivé „sessions“. • Řešení zahrnuje nezávislé archivační (data retention) politiky pro jednotlivé úložiště auditních dat. • Řešení zahrnuje podporu exportu auditních stop a exportu strukturovaných metadat. • Řešení zahrnuje podporu archivace na externí úložiště • Řešení zahrnuje podporu automatizovaného zálohování dat
PAM20	Řešení poskytuje indexaci pro rychlé vyhledávaní nejen informací o získaných „session“ dat, ale taky o jejich obsahu (taky nazývané content, nebo OCR indexace).
PAM21	Přístupy k samotnému systému: • Řešení podporuje GROUP management. • Řešení podporuje autentizaci přes RADIUS. • Řešení podporuje lokální /externí databázi uživatelů – LDAP.
PAM22	Reporting zahrnuje: • Dashboardy/Statistiky o „sessions“. • Uživatelsky konfigurovatelný reporting strukturovaných dat. • Možnost tvorby vlastních reportů nad content informacemi formou tvorby SQL QUERY dotazů. • API pro reporting do externích SW. • Řešení umožňuje Full text search.

2.6 SIEM systém (Security Information and Event Management)

Na základě požadavku zadavatele a dle Přílohy 1.1.1 Technické specifikace: „Funkční a nefunkční požadavky částí plnění veřejné zakázky“ pro část SIEM Systém nabízí dodavatel produkt od společnosti OPENTEXT, a to konkrétně **ArcSight Enterprise Security Manager Standard Edition** v celkovém objemu **1000 EPS**

určených pro vyhodnocení kybernetických bezpečnostních událostí a incidentů, a to v podobě virtuální appliance a obslužných serverů, které budou nasazené na dodávané servery.

Zadavatel již tento systém používá ve formě HW appliance a přechod na VA appliance tak nebude znamenat nutnost přeškolení personálu na nový typ řešení a komplikovanou migraci ze stávajícího řešení. Zadavatel tak získá modernější podobu stávajícího řešení, které již aktivně používá.

Licence je rozšiřitelná na 5000 EPS v celodenním průměru bez nutnosti upgradu HW, jen pomocí aktivace rozšiřující či nové licence. Cena za rozšíření není předmětem nabídky.

Systém SIEM podporuje současnou práci min. 10 uživatelů. Licence zahrnuje možnost mít minimálně 1000 sběrných konektorů, včetně vlastních custom logů (možnost doplnit další lokality, zdroje událostí apod.).

Popis řešení

OpenText Enterprise Security Manager (ESM) je výkonný a adaptabilní systém pro správu bezpečnostních informací a událostí (SIEM), který nabízí komplexní sběr dat a analýzu hrozeb v reálném čase. Jeho cílem je pomoci bezpečnostním týmům rychleji detekovat a reagovat na kybernetické hrozby, čímž se snižuje riziko narušení bezpečnosti a zlepšuje celková efektivita bezpečnostních operací.

Klíčové funkce OpenText ESM:

Detekce hrozeb v reálném čase: Díky pokročilému korelačnímu enginu dokáže ESM identifikovat a eskalovat známé hrozby okamžitě po jejich výskytu, což umožňuje analytikům bezpečnosti reagovat na incidenty dříve, než dojde k poškození.

Nativní SOAR integrace: ESM obsahuje integrované řešení pro orchestraci, automatizaci a reakci na bezpečnostní události (SOAR), které automatizuje procesy triáže, vyšetřování a reakce. To zahrnuje předdefinované playbooky a více než 120 integračních pluginů, což zvyšuje efektivitu a snižuje zátěž bezpečnostních týmů.

Široká viditelnost událostí v rámci podniku: ESM využívá technologii sběru událostí OpenText Security Open Data Platform (SODP), která umožňuje obohacení a analýzu dat z více než 450 různých typů zdrojů bezpečnostních událostí. To zahrnuje nativní podporu pro cloudové zdroje a možnost vytváření vlastních konektorů pro specifické potřeby organizace.

Automatizovaná reakce na hrozby: Díky nativní integraci SOAR může ESM automatizovat reakce na detekované hrozby pomocí vizuálních workflow playbooků, což zkracuje dobu expozice hrozbám a zvyšuje návratnost investic do bezpečnostních technologií.

Škálovatelnost a přizpůsobivost: ESM je navržen tak, aby vyhovoval rostoucím a měnícím se potřebám organizací. Podporuje integraci s mnoha třetími stranami, jako jsou EDR systémy, ticketovací systémy a identity repozitáře, což maximalizuje návratnost investic a umožňuje přizpůsobení specifickým bezpečnostním požadavkům.

Implementací OpenText Enterprise Security Manager získají organizace robustní platformu pro detekci a reakci na hrozby, která zlepšuje efektivitu bezpečnostních operací, snižuje riziko narušení a zajišťuje shodu s předpisy.

Součástí řešení je rovněž support/servisní podpora na dobu 5 let. Podpora bude zahrnovat všechny updaty i upgrady a telefonickou nebo emailovou podporu v rozsahu nejméně 8x5 (8-16 hod., po-pá).

2.6.1 Funkční a nefunkční požadavky na SIEM

Nabízené plnění zajistí naplnění požadovaných funkčních a nefunkčních požadavků v následujícím rozsahu:

ID	Popis splnění požadavku
SIEM01	Všechny potřebné komponenty jsou součástí dodaného systému SIEM, včetně databáze.
SIEM02	Log Management je fyzicky i logicky nezávislý na SIEMu. Při nedostupnosti SIEMu je Log Management plně funkční a obsahuje všechny logy v RAW formátu. Při nedostupnosti Log Managementu je SIEM plně funkční a obsahuje všechny potřebné logy v normalizovaném formátu. Vrstva zajišťující sběr je fyzicky i logicky nezávislá na LM a SIEM. Při nedostupnosti jak SIEM, tak LM, vrstva nadále funguje nezávisle a zajišťuje jak sběr logů tak je možné ji konfigurovat.
SIEM03	Rozhraní všech komponent systému SIEM je dostupné v českém nebo anglickém jazyce. Dokumentace skutečného provedení je k dispozici v českém jazyce, ostatní buď v jazyce českém anebo anglickém.
SIEM04	Všechny požadované funkce se spravují a využívají přes společnou řídící konzoli (dále jen „Centrální správa“), která je rovněž přístupná přes webové rozhraní z fyzického i virtuálního PC s využitím Microsoft Edge a novějších, nebo jiným podobným způsobem. Prezentace dat musí být provedena v grafické podobě, prezentační rozhraní musí být multiplatformní nebo platformě nezávislé a plně funkční na platformách Windows, Linux, Apple OS.X.
SIEM05	Centrální správa systému SIEM podporuje GUI (Grafické uživatelské rozhraní), a skriptovací nástroje.
SIEM06	Veškerá konfigurace, definice zdrojů logů, definice korelačních pravidel, tvorba reportů atd., probíhá z grafického rozhraní systému SIEM.
SIEM07	Správa uživatelů systému SIEM je integrovatelná s Microsoft Active Directory a RADIUS, tj. systém k přihlášení využívá doménové účty s využitím SSO.
SIEM08	Řešení systému SIEM umožňuje přihlašování pomocí lokálních účtů pro případ neaktivního propojení s AD.
SIEM09	Řešení umožňuje přístup více uživatelů současně, a to jak na úrovni přístupu ke vstupním/zdrojovým datům systému, tak i k incidentům. Přístup uživatelů je založený na volně definovaných, oddělených rolích s možností granulárního přidělování práv v rámci každé role, dle zdrojových dat, identifikace monitorovaných zařízení, skupin zařízení a serverů, typu vstupních dat, apod. Role nejsou vázány na AD a jsou spravovány interně.
SIEM10	Řešení podporuje kompletní oddělení skupin uživatelů k odlišným datům a konfiguracím, kdy jednotlivé instance mají možnost vlastní konfigurace a správy (multi-tenant přístup). Řešení podporuje min. 10 tenantů.
SIEM11	Řešení systému SIEM umožňuje vyhledávání dle klíčových slov (řetězců) v názvech zdrojů, v korelačních pravidlech v uložených log záznamech a v auditních log záznamech systému (tedy vyhledávání v konfiguračních položkách a v „contentu“).
SIEM12	Řešení systému SIEM umožňuje zaznamenávat vlastní auditní logy po nastavitelnou dobu a tyto jsou chráněny proti modifikaci.
SIEM13	Řešení nativně podporuje protokoly IPv4, IPv6, jak při normalizaci vstupních dat, tak i při komunikaci se zdroji dat.
SIEM14	Systém umožňuje exportovat/importovat své nastavení do/ze souboru (definice dashboardů, reportů a korelačních pravidel – tedy „contentu“).
SIEM15	Systém obsahuje plně integrovaný nástroj pro řízení celého životní cyklu incidentu (ticketing).
SIEM16	Řešení systému SIEM srozumitelně a prokazatelně deklaruje vedení licenční politiky, a to včetně uvedení funkcionalit, které nejsou součástí základní licence a zda a za jakých podmínek je možné je dokupovat.

ID	Popis splnění požadavku
SIEM17	Řešení systému SIEM není licenčně omezen na počet generujících zařízení/zdrojů logů, na počtu evidovaných aktiv a na počtu uživatelů/konzolí.
SIEM18	Komponenta SIEM je schopna nárazově (minimálně po dobu 72h) zpracovat 7500 EPS, bez jakýchkoliv výkonnostních nebo licenčních omezení, včetně zachování plné funkcionality u všech komponent (bez ztráty logů), přičemž dodané řešení zajišťuje zpracování logů nejpozději v minutách od jejich vzniku.
SIEM19	Řešení systému SIEM technicky nelimituje počet událostí (například při překročení licence nebo výkonu zakoupeného řešení) za určité časové období, aby nedošlo k jejich zahození.
SIEM20	Kapacita interního úložného prostoru systému SIEM umožňuje interně uchovat normalizované log záznamy po dobu min. 4 měsíců.
SIEM21	Systém umožňuje uchovávání obou formátu logů formou záloh (archivace), a umožňuje obnovení vybraných částí logů a jejich zpřístupnění přes Centrální správu SIEM.
SIEM22	Výkonnost systému je dostatečná nejen pro sběr a korelaci logů, ale i pro přípravu reportů a alertů. Alert je zaslán nejpozději do 3 minut od vzniku, report obsahující 1000 řádek je vytvořen do 10 minut od začátku generování.
SIEM23	Řešení SIEM umožňuje používání regulárních výrazů na straně agentů (pokud budou využity) i serveru systému SIEM.
SIEM24	Řešení systému SIEM umožňuje Normalizaci/Parsování bezpečnostních událostí v systému SIEM do jednotného formátu (centrální logy musí mít stejný formát ze všech zdrojů) a doplnění o další detailní informace (např. doplnění jména uživatele na základě uživatelského účtu, doplnění jména stanice na základě IP adresy apod.).
SIEM25	Řešení systému SIEM umožňuje kategorizaci logů, kterou poskytuje univerzální taxonomii nezávislou na výrobci zdroje události, aby bylo možné homogenně vyhledávat, reportovat nebo porovnávat události z různých zařízení bez nutnosti detailní znalosti konkrétního logu.
SIEM26	Řešení systému SIEM umožňuje vyhodnocovat i vlastní provozní logy
SIEM27	Řešení systému SIEM umožňuje zobrazení a změnu nasazených korelačních pravidel, včetně pravidel dodaných výrobcem.
SIEM28	Řešení systému SIEM umožňuje export a import pravidel i parserů.
SIEM29	Řešení systému SIEM umožňuje definování / přidávání vlastních korelačních pravidel a log parserů bez nutnosti spolupráce s dodavatelem nebo výrobcem, např. pomocí wizardu nebo regulárních výrazů.
SIEM30	Řešení systému SIEM umožňuje real-time korelaci a korelaci v časovém okně několika hodin mezi událostmi z různých zdrojů (libovolných a nezávislých zdrojů předávajících data do systému).
SIEM31	Řešení systému SIEM umožňuje korelaci událostí dávkově importovaných do systému SIEM, tj. korelaci událostí, které nejsou zařazovány real-time, ale např. prostřednictvím importů logů 1x denně (scheduler correlations). SIEM umožňuje ověření nového korelačního pravidla proti historickým datům.
SIEM32	Řešení systému SIEM umožňuje automatické stanovení závažnosti událostí např. na základě předchozí činnosti zdroje / cíle nebo jiných dostupných informací.
SIEM33	Řešení systému SIEM umožňuje vyhledávání anomálií v událostech (např. nárůst počtu neúspěšných pokusů o přihlášení v určitém čase, neúspěšné pokusy o přihlášení v mimopracovní době apod.) nebo datových tocích (např. neobvyklé toky dat).

ID	Popis splnění požadavku
SIEM34	Řešení systému SIEM umožňuje ukládání logů v systému SIEM ve tvaru, ve kterém je možné jejich prohledávání, tj. poskytuje vyhledávání na základě regulárních nebo logických výrazů podle času a klíčových slov (např. jmen uživatelů, čísel /jmen událostí apod.).
SIEM35	Řešení systému SIEM umožňuje vyhledávání logů/eventů na základě „full-text“ indexace.
SIEM36	Řešení systému SIEM umožňuje na jakoukoliv událost navázat automatickou akci: • notifikaci přes mail s možností definovat pravidla pro zasílání na různé adresy podle kritičnosti, zdroje apod. • spuštění externího skriptu.
SIEM37	Řešení systému SIEM poskytuje zabudovanou "security knowledge" tj. předdefinovaná pravidla rozpoznávání a zpracování událostí a jejich pravidelné aktualizace od výrobce, min 4x ročně. Řešení obsahuje: • Generické politiky • Generická korelační pravidla • Generické předdefinované reporty, pokud budou k dispozici
SIEM38	Řešení systému SIEM obsahuje komplexní sadu funkcionalit a přednastavených korelačních pravidel, které řeší klasické hrozby a bezpečnostní rizika i sofistikované bezpečnostní problémy z různých oblastí: • útoky robotů, červů a virů (včetně chyb antivirů); • neoprávněný přístup k aplikacím (ověřování uživatelů, změny administrace a konfigurace); • chyby a změny v sítích (chyby a stavy síťových zařízení); • monitorování serverů a desktopů (administrace privilegovaných uživatelů, přístupy a změny konfigurace, odmítnutá připojení, úspěšné a chybné přihlašovací aktivity, varování systémů IPS/IDS a využívání šíře pásma); • uchvácení šíře pásma a porušení platných zásad (úspěšná a chybná přihlášení do systému, změny hesla, změny konfigurace); • masivní šifrování dat (ransomware); • vědomá snaha nebo neuvědomělá činnost vedoucí k odcizení nebo znehodnocení důvěrných dat (porušení logů SIEM, DLP události, porušení časových razítek apod.); • a další.
SIEM39	Řešení systému SIEM umožňuje porovnat neobvyklý počet určitých událostí oproti jinému období z minulosti – base line analýza.
SIEM40	Řešení systému SIEM je schopen provázat několik přístupových záznamů tak, aby byl schopen rozpoznat "admin hopping" = přihlášení z bodu A do D přes prostředníky B a C, za předpokladu, že přímý prostup není dovolen.
SIEM41	Reportovací nástroj podporuje trendový reporting nad velkými objemy dat ve velkém časovém období (1 rok) a tvorbu vlastních agregačních (sumarizačních) tabulek s možností nastavit různé sumarizační časové rámce (minimálně hodiny, dny).
SIEM42	Řešení systému SIEM poskytuje reporty i ve formě grafů a tabulek.
SIEM43	Řešení systému SIEM umožňuje vytvářet reporty ve formátech PDF, HTML a CSV, popř. dalších.
SIEM44	Řešení systému SIEM umožňuje export dat ve formátu XML nebo CSV.
SIEM45	Systém SIEM obsahuje analytické nástroje umožňující např. reportování, forenzní analýzu, analýzu změn, statistické reporty nad aktuálními i historickými daty.
SIEM46	Řešení systému SIEM umožňuje poskytovat pro každého uživatele vlastní personalizovaný dashboard.

ID	Popis splnění požadavku
SIEM47	Systém SIEM umožňuje poskytovat Drill-down analýzu v GUI tj. od obecnějších informací vedou linky na konkrétnější informace (např. z reportu o počtu bezpečnostních událostí podle jednotlivých typů OS je možné na jeden klik dostat report o počtu bezpečnostních událostí na jednotlivých hostech s daným OS a dále pokračovat na report o počtu bezpečnostních událostí v jednotlivých aplikacích / lozích / zdrojích na daném hostu apod.).
SIEM48	Řešení systému SIEM podporuje automatické spouštění definovaných reportů (měsíčně, týdně, denně, nebo v definovaném čase), ukládání na síťové úložiště a jejich zasílání e-mailem přímo ze systému.
SIEM49	Autentizace je oddělená od autorizace. Tj. při autentizaci vůči AD je autorizace řízená uvnitř SIEM pomocí rolí a ne pomocí skupin v AD.
SIEM50	Systém podporuje režim vysoké dostupnosti HA (High availability). Jak v řežimu active-active, tak active-passive.
SIEM51	Součástí SIEM nástroje je i komplexní řešení SOAR bez omezení na počet akcí nebo uživatelů.
SIEM52	Řešení poskytuje out-of-the box pracovní toky (Workflows) na automatizaci standardních toků incidentů (Incident flows) pro různí kategorie incidentů jako DDoS, Phishing, Malware...
SIEM53	Řešení systému SIEM poskytuje možnost graficky vytvářet pracovní toky (Workflow) anebo aktivity.
SIEM54	Řešení podporuje sdružení aktivit Incident Response podle fází a umožňuje schopnost stanovit pořadí aktivit, které se mají dokončit.
SIEM55	Řešení podporuje automatizované specifikování reakčních aktivit nebo aktivity na základě a/nebo podmínek
SIEM56	Řešení systému SIEM umožňuje notifikovat zainteresovaných lidí (Tvůrce incidentu, Analytik...) o průběhu incidentu (např. při aktualizaci, označení v časti incidentu, přiřazení aktivity na dokončení)
SIEM57	Řešení nabízí produktové a konfigurovatelné funkce Reportingu a Dashboardy.
SIEM58	Řešení poskytuje obohacení založené na typických interních údajích společnosti (např. Informace o aktivitách, uživatelích, odděleních, rolích).
SIEM59	Řešení integruje informace od interních a externích poskytovatelů (např. Threat Intelligence Feeds, nástroje SIEM, Endpoint).
SIEM60	Řešení nabízí plně zdokumentované REST API.

2.7 Svolávací systém = nástroj pro automatizaci komunikace (svolávání a distribuce informací) při řešení incidenčních workflow

Na základě požadavku zadavatele a dle Přílohy 1.1.1 Technické specifikace: „Funkční a nefunkční požadavky částí plnění veřejné zakázky“ pro část SIEM Systém nabízí dodavatel produkt **O2 KISS**.

Popis řešení

Krizový informační a svolávací systém (KISS) je zcela automatický systém pro svolávání či informování osob. Eviduje kontakty osob (zaměstnanci, spolupracovníci, externisté …), kterým je schopen předat potřebné informace v různých formách komunikace (automatické volání TTS, SMS, e-mail). Jednotlivé typy komunikace vyjadřují přání uživatele a rovněž určují stupeň naléhavosti předávané informace.

Mezi prioritní typy komunikace patří automatické zavolání a „přeříkání“ konkrétní informace pomocí modulu TTS (Text To Speech). Svolavatel vybere skupinu kontaktů, napíše text sdělení a vše ostatní již zařídí SAIW. Umí předat informaci paralelně všem kontaktům najednou a výrazně tak zrychlit předání informace od svolavatele zvolené skupině kontaktů. Systém eviduje reakce příjemců – hovor bere/nebere, vzkaz si vyposlechl, potvrdil přijetí zprávy či zvolil konkrétní odpověď z několika variant (DTMF volbou). Na základě reakce volaného je systém schopen dále postupovat dle předem definovaného scénáře, např. pokud volaný nebere, tak mu informaci pošle formou SMS nebo bude volat náhradníka (kontakt, který je definovaný jako zástupce pro případ nedostupnosti). Scénáře svolávání jsou jednou ze základních částí systému SAIW.

Uživatel si může sám definovat libovolné scénáře komunikace a svolávání, včetně podmínek a rozhodovacích uzlů. Scénáře jsou často využívány v krizových případech svolávání, kdy je např. nutné informovat o určité události konkrétní kontakty či konkrétní typy pracovních pozic. Např. při vážné nehodě je třeba svolat lékaře a pomocný personál, který v daný okamžik má službu. Těmto osobám pak sám zavolá a předá informaci o této události. Ve scénáři je jasně definováno, jaké osoby informovat, jakým kontaktům volat, jakým jen poslat informační SMS o události a jak postupovat v případě, že někdo nereaguje. Pro spuštění celé akce bylo zapotřebí jen jednoduché spuštění konkrétního scénáře, který si uživatel předem nadefinoval do systému.

KISS obsahuje:

Modul Kontaktů: Modul Kontaktů eviduje kompletní seznamy firem a osob, které mohou být zapojeni do svolávání či informování systémem SAIW.

Modul Oslovení: Modul Oslovení poskytuje nástroje svolávání ve zjednodušené formě. Bez nutnosti použití konkrétního scénáře, je schopen uživatel oslovit vybranou skupinu kontaktů formou hlasu (TTS), SMS či e-mailem.

Modul Scénáře: Modul pro editaci a spouštění nadefinovaných krizových scénářů. Scénářem se rozumí předpis sekvenčních či paralelních komunikačních kroků, které mohou být podmíněny odpovědí na předchozí komunikační krok.

Modul Reporting: Modul poskytuje uživatelům systému KISS detailní pohled na svolávání, tj. informace o spuštěných scénářích, aktivních i dokončených či historii odpovědí.

Součástí řešení je rovněž support/servisní podpora na dobu 5 let. Podpora bude zahrnovat všechny updaty i upgrady a telefonickou nebo emailovou podporu v rozsahu nejméně 8x5 (8-16 hod., po-pá).

2.7.1 Funkční a nefunkční požadavky na Svolávací systém

Nabízené plnění zajistí naplnění požadovaných funkčních a nefunkčních požadavků v následujícím rozsahu:

ID	Popis splnění požadavku
SAIW01	Systém bude poskytovat funkce pro efektivní komunikaci a spolupráci mezi osobami odpovědnými za řešení incidentů a zúčastněnými stranami. Komunikace bude zajištěna v rozsahu: • Mailové notifikace • Rozesílání SMS • Automatizované hlasové volání
SAIW02	Systém bude mít možnost rozšíření komunikačních kanálů o whatsapp – existující funkcionalita

ID	Popis splnění požadavku
SAIW03	Systém bude poskytovat klienta pro mobilní zařízení typu Android, iOS. Systém bude umožňovat v chytrých telefonech umožňovat přijetí nebo zamítnutí výzvy, náhled do historie oslovení a scénářů, výběr stavu (připraven, mimo službu atd.), změnu hesla, reportování polohy. Chytrým telefonem se rozumí mobilní telefon, který používá mobilní operační systém Android nebo iOS,
SAIW04	Systém bude umět zakládat bezpečnostní komunikační scénáře = předpisy komunikačních kroků/úkonů (sestavení hlasového volání, odeslání SMS, příjem odpovědní SMS, odeslání PUSH notifikace, bude obsahovat funkci odeslání zprávy ve WhatsApp, příjem zprávy z WhatsApp) a pracovat se zpětnou vazbou (přijímám úkol / nepřijímám úkol)
SAIW05	Systém bude umět nabírat a vyhodnocovat zpětnou vazbu k zaslaným bezpečnostním incidentům čímž realizuje funkci rozhodovacího uzlu (ano/ne, resp. úspěch/neúspěch). Komunikační kroky lze provádět sekvenčně (jeden po druhém) či paralelně (současně na určitou množinu osob), následující komunikační kroky je možno definovat pro oba výsledky rozhodovacího uzlu a dále je možné podmínit je požadovanými parametry (odbornost, operační stav, dosažení potřebného skóre = situace, kdy výzvu přijme potřebný počet pracovníků.
SAIW06	Systém bude mít možnost spustit bezpečnostní komunikační scénář automaticky (bez zásahu lidské obsluhy) v případě mailového notifikačního alertu generovaného ze systémů NGFW neboLog Manager či SIEM. Událost či incident zaslaný z uvedených systémů automaticky spustí nadefinované bezpečnostní komunikační scénáře
SAIW07	Systém bude mít možnost spouštění předem nadefinovaných bezpečnostních komunikačních scénářů lidskou obsluhou odkudkoliv z webového prohlížeče, z mobilního telefonu: • Spuštěním zcela předpřipraveného bezpečnostní scénáře – ke spuštění stačí jeden klik • Doplněním proměnných v operačním dashboardu a následným spuštěním bezpečnostního komunikačních scénáře – dashboard lze ovládat jak z dotykové obrazovky, tak i z pracovní stanice
SAIW08	Systém bude mít možnost využití následujících komunikačních kanálů: • Mailové notifikace, • SMS zprávy s možností požadování odpovědní SMS • telefonický hovor s funkcí TTS (Text To Speech) s možností požadování odpovědi interaktivní DTMF volbou • Automatické zasílání varovných zpráv na PC stanice, vybavené samostatnou aplikací (tlustý klient), která umožňuje akustickou a optickou vizualizaci varovného hlášení na PC stanici
SAIW09	Systém bude poskytovat real-timový přehled o aktuálním stavu odpovědí, průběhu převzetí informace o incidentech včetně zachování evidence a záznamu historie (kompletní přehled o průběhu a historii informování)
SAIW10	Systém bude umožňovat tvorbu reportů obsahujících veškeré dostupné informace o komunikaci, vyrozumění a průběhu scénářů. Součástí reportu je i detailní historie odpovědí účastníků. Výběr z několika předdefinovaných reportů.
SAIW11	Systém bude mít možnost automatického vkládání dynamických informací do textu zprávy (datum a čas spuštění/jméno uživatele, který scénář spustil/druh a typ bezpečnostního incidentu …)
SAIW12	Systém bude mít možnost a podporu zadávání operačního stavu informované osoby („připraven / nepřipraven“; respektive „ve službě / mimo službu“ nebo respektive „v pohotovosti/ mimo pohotovost“
SAIW13	Systém automatizace komunikace SAIW bude provozován v režimu on-premis. Systém bude umístěn v infrastruktuře zákazníka. Nicméně komunikační služby SMS konektor a SIP trunk budou provozovány formou služby a systém automatizace komunikace na ně bude napojen. Součástí řešení je i volná měsíční kapacita 100 SMS a 30 min volání zdarma.

2.8 Integrace

SW zajišťující integraci bude dodán v rozsahu definovaném architekturou, která je specifikovaná v kapitole 4. s názvem „Technologická aplikační architektura řešení“ v dokumentu „Technická specifikace k veřejné zakázce „Modernizace a rozšíření bezpečnostní infrastruktury Kanceláře veřejného ochránce práv“, který tvoří v přílohu 1 zadávací dokumentace.

2.9 Služby SOC (Security Operation Centrum)

Na základě požadavku zadavatele a dle Přílohy 1.1.1 Technické specifikace: „Funkční a nefunkční požadavky částí plnění veřejné zakázky“ pro část SOC (Security Operation Centrum) nabízí dodavatel služby **Axenta CyberSOC**, které splňuje požadavky zadavatele.

Zadavatel již využívá a bude využívat moderní technologie pro detekci bezpečnostních událostí a monitoring kybernetické bezpečnosti. Tyto technologie budou napojeny do nabízeného bezpečnostního operačního centra. Připojení bude realizováno prostřednictvím virtuálního kolektorového serveru, který bude provozován na dodávaném hardware.

Popis nabízeného řešení

AXENTA CyberSOC je specializované centrum kybernetické bezpečnosti, které poskytuje zákazníkům eliminaci rizik spojených s kybernetickými hrozbami.

Toto centrum je vybaveno nejmodernější výkonnou technologií světových výrobců, která si poradí s účinnou ochranou zájmů a klíčových procesů všech jeho klientů. Již v základní službě bezpečnostního monitoringu je možno získat profesionální nástroje jako je Log Management, SIEM, ticketing a centrální dashboard v kombinaci s týmem odborníků a s procesy nad celou službou.

Centrum kybernetické bezpečnosti **AXENTA CyberSOC** pomáhá svým klientům naplnit požadavky Zákona o kybernetické bezpečnosti č. 181/2014 Sb. a vytváří podmínky pro úspěšnou certifikaci ISO 27 001. Služba zahrnuje nasazení bezpečnostních nástrojů a monitorovacích systémů tak, aby bylo dosaženo ochrany, včetně průběžných analýz, reportů a návrhů nových opatření. Službu lze současně využít při plnění technických opatření pro ochranu osobních údajů. Služba splňuje nároky nařízení GDPR.

Služby **AXENTA CyberSOC** jsou vhodné pro všechny typy organizací. Jeho klienty mohou být jak organizace z komerční sféry (výrobní podniky, výzkumné ústavy, finanční instituce, právní kanceláře, média atd.), tak i klienti z veřejné správy (úřady státní správy a samosprávy, zdravotnická zařízení, soudy, státní zastupitelství, vlastníci kritické a významné infrastruktury atd.), kteří si uvědomují náročnost a důležitost oblasti kybernetické bezpečnosti.

Součástí ceny SOC jsou všechny potřebné technologie a licence pro poskytování služby. Služba bude dostupná 99,9 % času z režimu 24x7. Výkonový rozsah licence pro LM/SIEM na straně SOC bude v rozsahu viz požadované parametry jednotlivých technologii výše (viz kapitoly 2 až 6). Čas ukládání dát pro ONLINE vyhledávaní je 100 dní, čas ukládaní dát pro OFFLINE archive je dalších 200 dní.

Výhody pro zákazníka:

AXENTA CyberSOC není blackbox nad daty zákazníka. Pomocí aplikace AXENTA CyberCopter jsou zákazníkovi dostupné všechny technologie v rámci poskytované služby a zákazník si tedy může sám prohledávat logy, psát korelace, pracovat s tickety a využívat customizované dashboardy.

Co zadavatel získá připojením do AXENTA CyberSOC:

- Efektivní ochranu zájmů společnosti a jejich klíčových procesů
- On-line přehled o stavu bezpečnosti IT v organizaci
- Posílení ICT bezpečnosti a prevenci kybernetických útoků
- Řízený přístup k řešení incidentů
- Pomocný nástroj k naplnění Zákona o kybernetické bezpečnosti č. 181/2014 Sb., Evropského nařízení GDPR o ochraně osobních údajů a pro různé certifikace (např. ISO 27 001)

2.9.1 Specifikace nabízené služby

V rámci nabídky nabízíme služby CyberSOC v rozsahu požadovaném v rámci výběrového řízení.

PROCESY

- Zpracování relevantních informací z hlediska bezpečnosti technologií zákazníka (aktiva, identity, zranitelnosti)
- Security as a Service – kybernetická bezpečnost jako služba, která je v souladu s GDPR a Zákonem o kybernetické bezpečnosti
- Vysoká dostupnost služeb díky technologii umístěné nezávisle ve dvou lokalitách (CZ a SK)
- Soulad s normou ISO 27 001
- Efektivní ochrana zájmů zákazníka (corporate identity, klíčové procesy)
- Pravidelné vyhledávání nedetekovaných událostí
- Reporting
- Threat Intelligence
- Cyber Copter – centrální dashboard

LIDÉ

- Provoz 8x5 (L1), Pohotovost 24x7
- Analytici L2 a L3
- CSIRT certifikovaný na stupeň „Accredited“ dle certifikační autority Trusted Introducer
- Sledování možných hrozeb a použití zero-day bezpečnostních informací pro prostředí zákazníka
- Komunikace v rámci pravidelných statusů
- Práce s komunitou MISP, STIX / TAXII, Cluster of cyber security
- Aktivní vyhledávání nových nebo neznámých hrozeb

TECHNOLOGIE

- Komplexní bezpečnostní monitoring prostředí zákazníka
- Detekce incidentů pomocí analytických nástrojů
- Napojení jednotlivých bezpečnostních technologií zákazníka
    - UBA, NDR, Real time correlation
    - EDR
    - LM
    - SIEM
    - Vulnerability Management
    - PAM
- Technologie na straně SOC
    - MISP
    - LM
    - SIEM
    - SOAR

- PAM
- Ticketovací nástroj pro zajištění reakce na incidenty
- Provozní monitoring
- Sběr, bezpečný přenos, šifrování logů a uchování auditních záznamů (předpokládá se využití forwardingu alertů směrem do SOC.
- Pokročilé možnosti vyhledávání a analýzy

AXENTA CyberSOC je „otevřeným komerčním SOC“ tzn. snažíme se o maximální pochopení potřeb zákazníka v oblasti kybernetické bezpečnosti a společně s ním hledáme nevhodnější způsob zajištění bezpečnostního dohledu. V praxi to znamená, že služba je vždy navrhována na míru dané společnosti.

Společnost AXENTA je implementátorem řešení v oblasti kybernetické bezpečnosti s 25 lety zkušeností zakladatelů, neposkytujeme tedy jen služby dohledového centra, ale máme několik týmů implementačních techniků certifikovaných na celou řadu technologií. Tyto týmy poskytují jak podporu našim zákazníkům připojeným do SOC, tak i vysoce odborné konzultace pracovníkům dohledu.

Implementační tým taktéž zajišťuje nasazení produktů pro monitoring bezpečnosti dle úrovně služby vybrané zákazníkem.

Před samotným návrhem struktury služby dochází k analýze současného stavu v dané organizaci pomocí kvalifikačního dotazníků, a to v oblastech techniky, procesů a zdrojů.

Následný on-boarding je řešen projektově s pravidelnými status meetingy. Nastavení procesů komunikace a předávání informací je přizpůsobeno danému typu společnosti a jeho personálním množnostem.

Na straně zákazníka je vyžadována součinnost osoby odpovědné za provoz infrastruktury, případně dodavatele jednotlivých systémů a osoby zodpovědné za bezpečnost (CISO/CSO, MKB, DPO).

Součástí dodávky budou specifikované fáze viz níže:

a. zodpovědnost za identifikaci a nahlášení bezpečnostních incidentů Zadavateli
b. analytické práce v případě výskytů incidentů, alertů
c. kompatibilita a integrace SIEM dodavatele se SIEM KVOP
d. technický monitoring v režimu 24x7, operátor v režimu on line 5x8 a v režimu pohotovosti 7x24

2.9.2 Funkční a nefunkční požadavky na SOC

Naplnění požadovaných funkčních a nefunkčních požadavků:

ID	Popis splnění požadavku
SOC01	Řešení je plnohodnotné – tedy služba, která obsahuje všechny potřebné technologie, procesy, znalosti a obsluhu.
SOC02	Řešení SOC obsahuje z pohledu technologií LM, SIEM, Security Ticketing, Security Dashboard a SOAR.
SOC03	SOC bude poskytovaný jako externí outsourcovaná služba – všechny technologie jsou provozované v prostředí zadavatele, dodavatel potřebné logy / data z těchto technologiích vyhodnocuje ve svém prostředí. Dodavatel vzal na vědomí, že zadavatel připouští alert forwarding směrem k SOC dodavatele.
SOC04	Všechna data budou přenášena do SOC-u v zabezpečené zašifrované formě a budou chráně vůči neoprávněným změnám/zásahům.
SOC05	Provoz SOCu L1 je zajišťován v režimu 8x5.

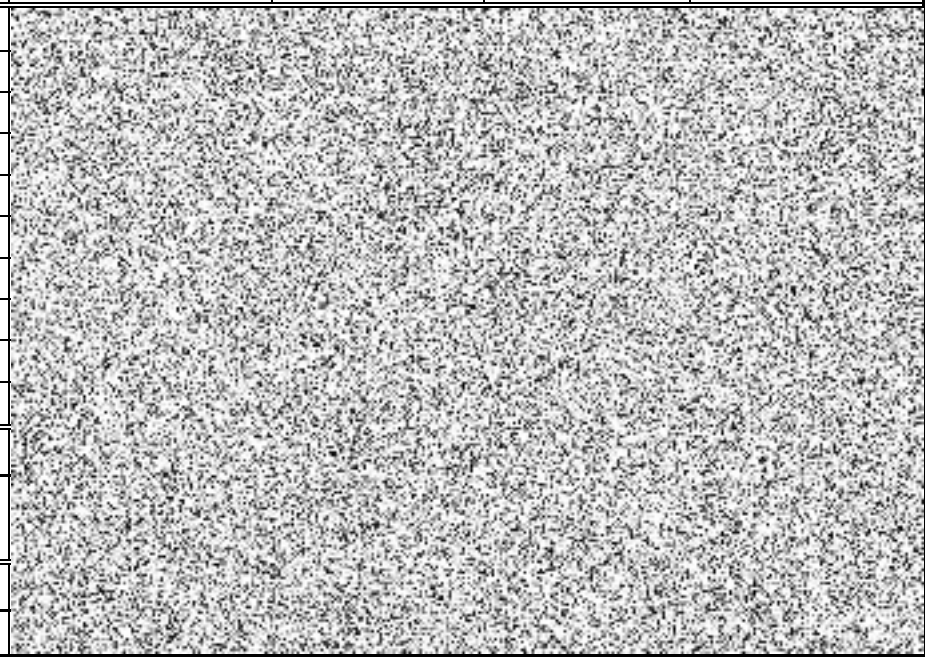
ID	Popis splnění požadavku
SOC06	Součástí SOC jsou služby certifikovaného CSIRT. CSIRT je a po dobu kontraktu bude certifikovaný minimálně na stupeň "Accredited".
SOC07	Služba SOC bude poskytována v režimu HA a provozovaná minimálně ve 2 geograficky oddělených lokalitách pro vykrytí případného výpadku.
SOC08	Provozovatel SOC je certifikovaný na ISO 27000.
SOC09	Všechny aktivity specialistů SOCu budou auditované na úrovni detailních aktivit (pohyby myší, práce s klávesnicí, obsah obrazovky), které vůči zadavateli vykonávají. Daný nástroj na zajištěni této auditní stopy je součástí technického řešení dodavatele.
SOC10	Řešení SOCu jako služby je v souladu se zákonem 181/2014 Sb o kybernetické bezpečnosti (ZoKB).
SOC11	Součástí řešení je real-time provozní monitoring dostupnosti informačních systémů, kritických aplikaci a síťových prvků s cílem zjistit výpadky procesů a funkčnosti systémů, narušení dostupnosti, včasného identifikovaní bezpečnostních incidentů, resp. omezení účinnosti bezpečnostních opatření.
SOC12	Řešení umí zpracovat i dočasné zvýšený přenos dat (peak) na síti bez jeho zahození/ignorováni.
SOC13	Řešení umožňuje rozšíření výkonnosti anebo připojeni monitorovaných zdrojů jen licenčním vypořádáním (škálovatelnost).
SOC14	Řešení je postavené jako otevřené pro zadavatele, zadavatel má přístup do všech částí/technologie minimálně v rozsahu READ ONLY.
SOC15	Součástí služby jsou specialisté bezpečnostního monitoringu v rozsahu L1, L2, L3.
SOC16	Součástí SOC jsou pravidelné schůzky/status meetingy 1x měsíčně.
SOC17	Součástí SOC je tvorba Knowledge Base a tvorba RUNBOOKS pro efektivní řešeni bezpečnostních událostí.
SOC18	Součástí SOCu je specializovaný portál, kde jsou dostupné všechny informace na jednom místě v podobě DASHBOARDU. Tento portál poskytuje dashboardy na míru (možnost konfigurace specialisty dodavatele), kde je možné zobrazit informace ze všech komponent SOCu.
SOC20	Řešení je schopné monitorovat, analyzovat a vyhodnocovat bezpečnostní události, hrozby, útoky a anomálie na základě netflow, pomoci přímého monitoringu v reálném čase, a to i na aplikační vrstvě ISO/OSI, resp. TCP/IP. Technologicky řešení monitoringu netflow zajistí zadavatel. Provozovatel SOC zajistí jeho napojení do dohledu a konzultace speciality certifikovaného na tuto technologii.
SOC21	Řešení umí identifikovat zero-day útoky.
SOC22	Řešení umožňuje automatické korelování událostí z vícerých zdrojů, vyhodnoceni incidentů a následné generovaní alertů, a to všechno v reálném čase.
SOC24	Řešení primárně využívá bez-agentový sběr logů. Instalace agenta bude využita jen v odůvodněných případech Např. pokud není technologicky možné zajistit sběr logů jiným způsobem.
SOC25	Databáze bude zabezpečená proti manipulaci, tak aby nebylo možné narušit integritu uložených záznamů.
SOC26	Řešení podporuje napojení různých zdrojů obohacujících informací (DNS, IDM, LDAP, ap.).
SOC27	Řešení nezpůsobí omezení funkcionality, kvality a narušení bezpečnosti jakýchkoliv jiných zařízení / systémů v síti.
SOC28	Řešení podporuje možnosti vícenásobné notifikace jednoho alertu.

ID	Popis splnění požadavku
SOC29	Řešení podporuje filtraci a agregaci už na úrovni sběru logů v prostředí zadavatele.
SOC30	Řešení zabezpečí normalizaci logů z různých zdrojů a formátů do jednotného formátu.
SOC31	Řešení je schopné zaznamenávat a vyhodnocovat následující detaily bezpečnostních událostí: typ nebo akce, datum a čas, ID systému, který událost zaznamenal, ID systému, kde k události došlo a ID uživatele nebo systému, který akci vyvolal.
SOC32	Řešení SOC využívá SOAR techniky a procesy pro orchestraci a zrychlení threat detection a incident response.
SOC33	Řešení je na úrovni Alertingu provázané s technikami popsanými v knowledge base MITRE ATT&CK.
SOC34	Součástí služby SOCu je měsíčný KPI reporting na míru zákazníka.
SOC35	Poskytovatel SOCu nabízí RestAPI (nebo podobné API) rozhraní pro výměnu informací o svých aktivitách, minimálně na úrovni ticketing nástroje.
SOC36	Služba SOCu bude po dobu kontraktu obsahovat funkcionalitu THREATS EXCHANGE, na úrovni MISP nebo vyšší.

Příloha č. 2 – Seznam realizačního týmu

Postavení v týmu	**Jméno a Příjmení**
Architekt	[redacted]
Vedoucí realizačního týmu – Projektový manažer	[redacted]
Auditor	[redacted]
Technický specialista č. 1	[redacted]
Technický specialista č.1	[redacted]
Technický specialista č. 2	[redacted]
Technický specialista č. 3	[redacted]
Technický specialista č. 4	[redacted]

Příloha č. 3 – Rozpis ceny plnění

Položka	Cena v Kč bez DPH	Sazba DPH v %	Výše DPH v Kč	Cena v Kč s DPH
Podrobný návrh cílového konceptu řešení				
Firewall				
NDR systém				
EDR systém				
LOG management systém				
PAM systém				
SIEM systém				
Svolávací systém SAIW				
Požadované služby a dodávky integrace				
SOC				
CELKEM DODÁVKA + IMPLEMENTACE				
Podpora provozu po dobu 5 let od akceptace předávacího protokolu*				
CELKEM PODPORA				
CELKEM				

* Před úplným předáním a převzetím díla je podpora provozu součástí ostatních oceněných položek.