Středočeský kraj

SMLOUVA O DÍLO

„Zajištění kybernetické bezpečnosti informačních systémů krajského úřadu – dohledové centrum SOC“

(dále jen „smlouva“)

uzavřená ve smyslu ust. § 2586 a násl. zákona č. 89/2012 Sb., občanského zákoníku, ve znění pozdějších předpisů, (dále jen „ObčZ“)

pod evidenčním číslem objednatele: ***S-6364/OBŘ/2024***

Objednatel:

Středočeský kraj

se sídlem:	Zborovská 81/11, 150 21 Praha 5 - Smíchov
IČO:	70891095
ID datové schránky:	keebyyf
zastoupen:	Mgr. Petra Pecková, hejtmanka Středočeského kraje
bankovní spojení:	PPF, a.s.
číslo účtu:	

Zhotovitel:

O2 Czech Republic a.s.

se sídlem:	Praha 4 - Michle, Za Brumlovkou 266/2, PSČ 14022
IČO:	60193336
DIČ:	CZ60193336
zastoupen:	Petr Krutký, Key Account Manager, na základě pověření

zapsaná v Obchodním rejstříku vedeném u Městského soudu v Praze spisová značka B 2322

tel.:  fax.: - e-mail: 

bankovní spojení:	Komerční banka, a.s.
číslo účtu:	

dále společně jako „smluvní strany“

I.

Preambule

Tato smlouva je uzavírána na základě výsledku zadávacího řízení s názvem „**Zajištění kybernetické bezpečnosti informačních systémů krajského úřadu – dohledové centrum SOC**“ uveřejněným ve věstníku veřejných zakázek pod evidenčním číslem Z2024-030252 a na profilu zadavatele.

II.

Předmět smlouvy

1) Předmětem smlouvy je závazek zhotovitele provést pro objednatele dílo spočívající v zajištění služeb komplexního monitoringu ICT prostředků, kontroly činností všech registrovaných uživatelů na všech úrovních zpracování dat, sledování datového provozu informační infrastruktury, registrování útoků na prostředky ICT a průběžné odhalování případných interních a externích útočníků na ICT Krajského úřadu Středočeského kraje. Nedílnou součástí předmětu této smlouvy je rovněž zajištění pravidelných auditů kybernetické bezpečnosti. Vše v rozsahu dle zadávací dokumentace veřejné zakázky „Zajištění kybernetické bezpečnosti informačních systémů krajského úřadu – dohledové centrum SOC“, zejména přílohy č. 1 zadávací dokumentace (Technická specifikace veřejné zakázky) a dále nabídky zhotovitele a této smlouvy (dále „dílo“). Dílo bude zahrnovat zejména:

- Zhotovení předimplementační analýzy a prováděcí dokumentace;
- Zajištění sdílených služeb kybernetické bezpečnosti. Tato služba bude zahrnovat další níže uvedené služby:
  (a) Zaznamenávání a ukládání logů a detekce bezpečnostních událostí
  (b) Analýza datových toků a detekce bezpečnostních událostí
  (c) Dohledové centrum - SOC
- Audit kybernetické bezpečnosti zahrnující:
  (a) Penetrační testování vybrané webové aplikace
  (b) Penetrační testování perimetru
  (c) Penetrační testování vnitřního systému

2) Podrobná specifikace technického řešení je uvedena v příloze č. 1 této smlouvy a tvoří její nedílnou součást.

3) Zhotovitel se zavazuje provést na svůj náklad a na své nebezpečí všechna související plnění a práce potřebné k včasnému a řádnému provedení díla.

III.

Doba a místo plnění, akceptace a předání díla

1) Místem plnění smlouvy je:

   a) sídlo objednatele Krajský úřad Středočeského kraje, Zborovská 81/11, 150 21 Praha 5 – Smíchov (Hlavní technologické centrum kraje – HTCK)

   b) Oblastní nemocnice Kladno, Vančurova 1548, 272 59 Kladno (Záložní technologické centrum kraje – ZTCK).

2) Dílo bude realizováno ve třech etapách, které jsou rozepsány níže.

3) **První etapa** - **Služby poradenství a podpory** - zahrnuje:

   a) Zajištění služeb poradenství a podpory dle kapitoly 2 Přílohy č. 1 této smlouvy, zejména zajištění předimplementační analýzy, prováděcí dokumentace a detailního harmonogramu realizace včetně uvedení kritických milníků

   b) Řádné provedení implementace díla bude ověřeno v rámci testovacího provozu v délce 1 měsíce ukončeného oboustranným podpisem akceptačního protokolu testovacího provozu.

c) Po ukončení testovacího provozu bude vyvoláno akceptační řízení, zakončené podpisem Akceptačního protokolu (AP), který podepíší oprávnění zástupci obou smluvních stran. Akceptační procedura zahrnuje ověření řádné implementace díla u objednatele v souladu se specifikací stanovenou touto smlouvou a jejími přílohami. Objednatel potvrdí plnou funkčnost díla nebo díla s vadami, které nebrání jeho řádnému užívání, které je zhotoveno v souladu s touto smlouvou a v souladu se schváleným harmonogramem dle odst. 3 písm. a) tohoto článku. Přílohou AP bude i soupis veškerých předávaných komponent v editovatelné podobě. Po úspěšném ukončení akceptačního řízení dojde k předání díla přejímacím řízením.

d) V případě, že akceptační řízení prokáže nezpůsobilost dodaného řešení nasazení do produkčního prostředí, zaznamenají se tyto nedostatky do akceptačního protokolu s termíny, v nichž je zhotovitel povinen vady a nedostatky odstranit a dílo k úspěšné akceptaci připravit. Poté se akceptační řízení opakuje dle odst. 3, písm. d) tohoto článku.

e) Vadou se pro účely této smlouvy rozumí odchylka v kvantitě, kvalitě, rozsahu, termínech nebo parametrech díla stanovených touto smlouvou, zadávací dokumentací a obecně závaznými předpisy.

f) Zhotovitel se zavazuje, že první etapu dokončí nejpozději **do 3 měsíců** od účinnosti smlouvy. Dokončením první etapy se rozumí podpis Akceptačního protokolu dle tohoto článku.

4) **Druhá etapa - Sdílené služby kybernetické bezpečnosti** – zahrnuje následující plnění po dobu 60 měsíců ode dne úspěšném ukončení akceptačního řízení.

4.1) Zajištění a poskytování sdílené služby kybernetické bezpečnosti, obsahující služby:

a. zaznamenávání a ukládání logů a detekce bezpečnostních událostí
b. analýza datových toků a detekce bezpečnostních událostí
c. dohledové centrum - SOC

4.2) Služby poskytované nad rámec zajištění a poskytování sdílené služby kybernetické bezpečnosti po dobu 60 měsíců ode dne dokončení první etapy (*výkony nad rámec služeb*)

a) služby musí být poskytovány po dobu 60 měsíců ode dne dokončení první etapy, a to v předpokládaném rozsahu až 50 člověkodní (též man-day, či MD).

b) Školení a konzultace odborných pracovníků (administrátorů) objednatele zajišťované zhotovitelem na základě výzvy objednatele zhotoviteli.

c) Do rozsahu 50 MD budou tyto služby plněny na základě výzvy objednatele zhotoviteli. Po vyčerpání limitu 50 MD budou další požadavky tohoto typu objednatelem zadávány na základě samostatně vystavených a podepsaných objednávek dle hodinové sazby specifikované v čl. IV, odst. 3 smlouvy.

d) Objednatel je oprávněn (nikoli povinen) tyto služby čerpat dle své potřeby, popřípadě nečerpat žádné z těchto služeb. Nečerpáním, nebo čerpáním v nižším rozsahu nevzniká zhotoviteli nárok na úhradu jakékoli újmy, popřípadě právo odstoupit od této (části) smlouvy. Zhotovitel bere na vědomí, že limit 50 MD nemusí být objednatelem za celou dobu trvání smlouvy vyčerpán. Objednateli budou vyúčtovány vždy jen skutečně odvedené služby a práce.

5) **Třetí etapa - Audit kybernetické bezpečnosti** – zahrnuje zajištění auditní činnosti vyplývající z Vyhlášky č. 82/2018 Sb. dle § 16 – Audit kybernetické bezpečnosti. Každý z níže uvedených bodů bude realizován v průběhu trvání této smlouvy, a to vždy v termínech po dohodě se zadavatelem.

a) Penetrační testování vybrané webové aplikace – zhotovitell provede penetrační test vybraných webových aplikací po dohodě s objednatelem. Testování bude prováděno formou gray box, dle standardu OWASP. Hodnocení bude provedeno pomocí hodnotícího systému NIST CVSSv3 (nebo vyšší).

b) Penetrační testování perimetru – Zhotovitel provede penetrační testování perimetru. Testování bude prováděno formou gray box. Test bude proveden prostřednictvím simulace útoku na vybrané informační systémy Objednatele.

c) Penetrační testování vnitřního systému – Zhotovitel provede penetrační testování vnitřní infrastruktury. Testování bude prováděno formou gray box.

IV.

Cena a platební podmínky

1) Cena díla je stanovena na základě nabídkové ceny zhotovitele, kalkulované v rámci zadávacího řízení na předmět plnění dle této smlouvy. Celková cena díla je stanovena dohodou smluvních stran jako cena nejvýše přípustná.

2) **Celková cena díla je uvedena v příloze č. 2 této smlouvy.**

3) **Zhotovitel garantuje po celou dobu trvání této smlouvy hodinovou sazbu svých výkonů nad rámec poskytovaných služeb, poskytovaných na základě výzvy objednatele ve výši 1 805,63 Kč bez DPH (slovy: jeden tisíc osm set pět korun českých šedesát tři haléřů) za 1 hodinu takových prací. To platí i pro objednávky zadávané po vyčerpání limitu 50 MD. DPH bude účtováno ve výši dle platných účetních zákonů.**

4) Cena díla je stanovena jako nejvýše přípustná cena a zahrnuje všechny poplatky a veškeré další náklady spojené s plněním předmětu této smlouvy.

5) Cena díla zahrnuje také veškeré náklady spojené s rozhraními (integracemi), vzniklými na straně zhotovitele, popř. vyvolanými nutností obchodní spolupráce mezi zhotovitelem a dodavateli stávajících aplikací, na něž jsou integrace (rozhraní) požadovány. Požadavek objednatele je, aby zhotovitel uvedl a zahrnul do ceny plnění veškeré náklady spojené jak s vytvořením rozhraní, tak jejich udržováním v rámci záruční doby, zejména při změnách vyvolaných updatem aplikací zhotovitele a to jak v souvislosti se změnami legislativy, tak v souvislosti s inovacemi aplikací zhotovitele, a to vč. úprav vzniklých na straně zhotovitele, popř. vyvolaných nutností obchodní spolupráce mezi zhotovitelem a dodavateli stávajících aplikací, na něž je integrace požadována.

6) Cenu díla je možné překročit pouze v souvislosti se změnou daňových předpisů upravujících výši DPH, přičemž v takovém případě bude ke kupní ceně připočteno DPH ve výši stanovené zákonem č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů (dále jen „zákon o dani z přidané hodnoty). Dojde-li ke zvýšení sazby DPH, bude ke smlouvě uzavřen dodatek.

7) Cena díla bude objednatelem uhrazena v korunách českých (CZK) na základě daňového dokladu (dále jen „faktura“) doručeného zhotoviteli. **Odměna za první etapu bude hrazena po akceptaci díla (tj. po podpisu Akceptačního protokolu oběma stranami). Odměna za druhou etapu bude hrazena v poměrných částkách vždy za uplynulé tři kalendářní měsíce, odměna za třetí etapu bude hrazena vždy po realizaci jednotlivého testování, odměna za výkony nad rámec podpory bude zhotovitelem fakturována vždy za skutečně odvedené práce a služby**.

8) **Přílohou faktury za první etapu musí být kopie Akceptačního protokolu podepsaného osobami oprávněnými jednat za smluvní strany ve věcech realizace díla. Přílohou faktury za třetí etapu musí být výstup provedeného penetračního testu. Přílohou faktury za výkony nad rámec podpory musí být vždy seznam služeb a prací poskytnutých zhotovitelem za uplynulé období a přehled vyčerpaných hodin výkonů nad rámec podpory z limitu 50 MD.**

9) Faktura, musí obsahovat všechny náležitosti řádného daňového dokladu ve smyslu zákona o dani z přidané hodnoty.

10) V případě, že faktura bude obsahovat věcné či formální nesprávnosti, popřípadě nebude obsahovat všechny zákonné náležitosti nebo přílohu dle předchozího odstavce, je objednatel oprávněn ji vrátit ve lhůtě splatnosti zpět zhotoviteli k doplnění či opravě, aniž se tak dostane do prodlení se splatností. Lhůta splatnosti počíná běžet znovu od opětovného doručení náležitě doplněné či opravené faktury objednateli.

11) Splatnost faktury se sjednává na 60 dnů ode dne doručení faktury objednateli. Faktura se považuje za splacenou odepsáním fakturované částky z účtu objednatele.

12) Faktura bude uhrazena na účet zhotovitele uvedený v záhlaví této smlouvy. Pokud by zhotovitel v období od data, kdy podepsal smlouvu, do vystavení faktury změnil číslo bankovního účtu, musí tuto skutečnost sdělit objednateli nejpozději s předloženou fakturou. Toto sdělení musí být podepsané osobou zhotovitele oprávněnou k jednání ve věcech smluvních, nebo jím zmocněnou osobou. Při splnění této podmínky není změna účtu podnětem k uzavření dodatku ke smlouvě. Kupní cena pak bude uhrazena na bankovní účet uvedený na faktuře.

13) Objednatel neposkytuje zhotoviteli zálohy na cenu díla.

14) Zhotovitel prohlašuje, že není veden v registru nespolehlivých plátců, a zavazuje se po dobu trvání této Smlouvy řádně a včas platit DPH. Pokud FÚ vyzve objednatele k placení DPH nezaplacené zhotovitelem při realizaci této smlouvy, zhotovitel se zavazuje zaplatit objednateli smluvní pokutu ve výši odpovídající nezaplacenému DPH. Pokuta je splatná ve lhůtě do 30 dnů ode dne doručení vyúčtování o smluvní pokutě.

V.

Práva a povinnosti smluvních stran

1) Zhotovitel je povinen dodat objednateli úplné a funkční dílo, v množství, jakosti, provedení a termínu dohodnutých touto smlouvou. Dílo musí být realizováno v souladu s touto smlouvu a jejími přílohami, v souladu s platnými právními předpisy a příslušnými normami, jakož i v souladu s interními předpisy objednatele díla.

2) Objednatel se zavazuje dílo řádně a včas dodané zhotovitelem převzít a zaplatit za něj sjednanou kupní cenu způsobem a v termínu sjednaném touto smlouvou.

3) Zhotovitel prohlašuje, že ke dni uzavření této Smlouvy má uzavřenou pojistnou smlouvu, jejímž předmětem je pojištění odpovědnosti zhotovitele za škodu způsobenou zhotovitelem do výše limitu pojistného plnění v částce minimálně 10.000.000,- Kč z jedné pojistné události ročně. Kopie pojistné smlouvy dodavatele, resp. akceptovaný návrh na uzavření pojistné smlouvy ze strany pojišťovny dle tohoto článku byl předán objednateli před podpisem této smlouvy, jako jedna z podmínek pro uzavření smlouvy dle ust. § 104 písm. a) zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů. Zhotovitel se zavazuje na žádost objednatele bezodkladně, nejpozději však ve lhůtě do 5 pracovních dnů od doručení písemné výzvy objednatele, předložit objednateli pojistný certifikát prokazující existenci a účinnost této pojistné smlouvy. Zhotovitel se zavazuje, že pojistná smlouva dle věty první tohoto článku zůstane v účinnosti v tomto rozsahu po celou dobu trvání povinností zhotovitele dle této smlouvy.

4) Zhotovitel je povinen neprodleně písemně vyrozumět objednatele o případném ohrožení doby plnění a o všech skutečnostech, které mohou řádné a včasné plnění předmětu této smlouvy znemožnit, a to nejpozději do 3 dnů ode dne, kdy se zhotovitel dozví o takové skutečnosti.

5) Zhotovitel není oprávněn postoupit jakákoliv práva anebo povinnosti vyplývající z této smlouvy na třetí osoby bez předchozího písemného souhlasu objednatele. Uplatní-li třetí osoba své právo k

dílu nebo jeho části, zhotovitel se zavazuje bez zbytečného odkladu a na vlastní náklady učinit potřebná opatření k ochraně výkonu práv objednatele.

6) Objednatel může oprávnění plynoucí z licence poskytnout zcela nebo z části třetí osobě.

7) Práva a povinnosti uvedené v tomto článku trvají i po ukončení tohoto smluvního vztahu, a to i v případě, že by došlo k předčasnému ukončení smlouvy.

8) Každá ze stran nese odpovědnost za způsobenou škodu v rámci platných právních předpisů a této smlouvy. Obě strany se zavazují vyvíjet maximální úsilí k předcházení škodám a k minimalizaci vzniklých škod.

9) Žádná ze stran neodpovídá za škodu, která vznikla v důsledku neúplného, věcně nesprávného nebo jinak chybného zadání, které obdržela od druhé strany. Žádná ze smluvních stran není odpovědná za nesplnění svého závazku v důsledku prodlení druhé smluvní strany nebo v důsledku nastalých okolností vylučujících odpovědnost.

10) Obě smluvní strany odpovídají za škodu, kterou způsobí druhé straně porušením svých povinností dohodnutých touto smlouvou při provádění předmětu plnění této smlouvy a za podmínek daných touto smlouvou či povinností, které vyplývají už ze samotného předmětu plnění smlouvy. Zhotovitel se zavazuje uhradit objednateli případnou škodu, která vznikne z důvodu nedodání Díla či jeho části ze strany zhotovitele a kterou bude muset objednatel vynaložit, aby Dílo bylo zrealizováno či dokončeno.

VI.

Oprávněné osoby

1) Oprávněnými osobami při realizaci plnění jsou

   ❖ **za objednatele**

   a) ve věcech smluvních: viz záhlaví této smlouvy

   b) ve věcech realizace díla: Mgr. Michal Holý; 

   c) ve věcech technických: Bc. Petr Staněk, 

   ❖ **za zhotovitele**

   a) ve věcech smluvních: Petr Krutký; 

   b) ve věcech realizace díla: Ing. Petr Mlateček; 

   c) ve věcech technických: Petr Matějka; 

2) V případě změny kontaktních osob musí být o této skutečnosti druhá smluvní strana neprodleně písemně informována. Za splnění této povinnosti se považuje i e-mail potvrzený druhou smluvní stranou. Účinnost změny nastává okamžikem doručení písemného oznámení příslušné smluvní straně. Změna kontaktní osoby není důvodem k uzavření dodatku.

3) Veškerá korespondence, pokyny, oznámení, žádosti, záznamy a jiné dokumenty vzniklé na základě této smlouvy mezi smluvními stranami nebo v souvislosti s ní budou vyhotoveny v písemné formě v českém jazyce a doručují se buď osobně, doporučenou poštou nebo prostřednictvím datové schránky, na adresu sídla či ID datové schránky objednatele, uvedené v záhlaví této smlouvy. Smluvní strany se v případě doručování zásilek formou doporučených dopisů dohodly tak, že zásilka je považována za doručenou 3. pracovní den bezprostředně následující po dni jejího

odeslání prostřednictvím držitele poštovní licence na adresu příslušné smluvní strany dle záhlaví této smlouvy.

4) Zhotovitel se zavazuje zajistit, že osoby uvedené zhotovitelem v jeho nabídce (v seznamu techniků) dle čl. 6.3.2 zadávací dokumentace zadávacího řízení, jež předcházelo uzavření této smlouvy, se budou podílet na plnění této smlouvy a budou odpovídat za realizaci díla, a to ve funkcích, v jakých byly v seznamu uvedeny. Výměna takové osoby je možná pouze s písemným souhlasem objednatele a za předpokladu, že nová osoba bude splňovat kvalifikační předpoklady uvedené v zadávací dokumentaci.

5) Změna poddodavatelů oproti obsahu nabídky podané zhotovitelem v zadávacím řízení na uzavření této smlouvy, je možná pouze na základě písemného souhlasu objednatele. Objednatel se zavazuje, že takový souhlas nebude odpírat v případě, že nový poddodavatel bude splňovat veškeré kvalifikační požadavky a odbornost, které splňoval původní poddodavatel a z informací, kterými bude objednatel v dané situaci disponovat, nebude vyplývat obava, že nový poddodavatel by mohl provést jemu svěřenou část díla vadně nebo jiným způsobem narušit realizaci díla dle této Smlouvy. Zhotovitel se zavazuje, že část díla spočívající v poskytování služeb dohledového centra SOC bude realizovat vlastními kapacitami, nikoli prostřednictvím poddodavatelů.

VII.

Záruky

1) Zhotovitel se zavazuje, že dílo bude prosté podstatných vad a bude mít vlastnosti dle obecně závazných právních předpisů, této smlouvy a zadávací dokumentace veřejné zakázky uvedené v preambuli této smlouvy, dále bude mít vlastnosti první jakosti provedení a bude proveden v souladu s ověřenou technickou praxí.

2) Zhotovitel se zavazuje, že **záruční doba činí 60 měsíců**, je poskytována na všechny části díla a **je garantovaná výrobcem**. Na vyžádání objednatele předloží zhotovitel objednateli písemný doklad, který potvrdí, že je záruka skutečně zajištěna v souladu s jeho zadáním a touto smlouvou.

3) Záruční doba začíná běžet dnem dokončení akceptačního řízení v rámci první etapy.

4) Zhotovitel odpovídá za vady, které má předmět plnění v době dokončení akceptačního řízení v rámci první etapy a za vady, které vzniknou nebo se objeví v průběhu záruční doby dle odst. 2) tohoto článku smlouvy s výjimkou běžných opotřebení, vad způsobených nesprávnou obsluhou, vad způsobených vyšší mocí nebo třetími osobami a vad spotřebního materiálu.

5) Objednatel je oprávněn reklamovat v záruční době dle odst. 2) tohoto článku smlouvy vady předmětu díla u zhotovitele, a to písemnou formou. V reklamaci musí být popsána vada předmětu díla, určen nárok objednatele z vady předmětu díla, případně požadavek na způsob odstranění vad, a to včetně termínu pro odstranění vad zhotovitelem. Za písemnou formu je považováno také nahlášení standardními prostředky technické podpory provozu, např. e-mailem nebo prostřednictvím HelpDesku/ hot-line.

6) Objednatel má právo volby způsobu odstranění důsledku vadného plnění. V případě vady zboží má objednatel nárok zejména na

   - odstranění vady opravou, je-li vada opravou odstranitelná;
   - přiměřenou slevu z ceny díla;
   - odstoupení od smlouvy (viz čl. X).

7) Zhotovitel se zavazuje od okamžiku oznámení vady předmětu díla či jeho části zahájit odstraňování vady či jeho části, a to i tehdy, neuznává-li zhotovitel odpovědnost za vady či příčiny, které ji vyvolaly, a vady odstranit v technicky co nejkratší lhůtě, a současně zahájit reklamační řízení

v místě provádění předmětu díla. O reklamačním řízení budou objednatelem pořizovány písemné zápisy ve dvojím vyhotovení, z nichž jeden stejnopis obdrží každá ze smluvních stran. Bude-li v reklamačním řízení vada uznána jako reklamační vada, bude odstranění vady předmětu díla či jeho části provedeno bezúplatně.

8) Reklamaci uplatní objednatel u zhotovitele nejpozději poslední den záruční doby. I reklamace odeslaná objednatelem poslední den záruční doby se považuje za uplatněnou včas.

9) Uplatnění reklamačních práv objednatelem, jakož i plnění jim odpovídajících povinností zhotovitele, není podmíněno ani jinak spojeno s poskytnutím jakékoli další úplaty zhotoviteli ani jiné osobě.

10) Uplatněním práv z odpovědnosti za vady není dotčeno právo objednateli na náhradu škody.

VIII.

Sankční ujednání

1. Pro případ prodlení zhotovitele s plněním předmětu smlouvy zaplatí zhotovitel objednateli smluvní pokutu ve výši 0,05 % z celkové ceny díla za každý i započatý den prodlení, maximálně však do výše odpovídající ceně za první etapu.
2. Pro případ prodlení zhotovitele s odstraněním vad uvedených v předávacím protokolu dle čl. III odst. 4) písm. d) této smlouvy zaplatí zhotovitel objednateli smluvní pokutu ve výši 0,025 % z celkové ceny díla za každý i započatý den prodlení, maximálně však do výše odpovídající polovině ceny za první etapu.
3. V případě porušení povinnosti zhotovitele uvedené v čl. VI odst. 4) a odst. 5) této smlouvy zaplatí zhotovitel objednateli smluvní pokutu ve výši 15.000,- Kč za každé jednotlivé porušení této povinnosti.
4. Smluvní strany sjednávají pro případ porušení povinnosti o ochraně informací čl. X. této smlouvy smluvní pokutu ve výši 100.000,- Kč za každý případ.
5. V případě, že objednatel bude v prodlení se zaplacením faktury poskytovateli podle čl. IV., je objednatel povinen zaplatit zhotoviteli zákonný úrok z prodlení z fakturované částky za každý den prodlení dle aktuálně platné legislativy.
6. Za porušení povinnosti uzavřít pojistnou smlouvu (čl. V. – Práva a povinnosti smluvních) zaplatí zhotovitel objednateli smluvní pokutu ve výši 0,05 % z minimální výše limitu pojistného plnění uvedené v článku V., odstavci 3 této smlouvy za každý, byť jen započatý den, v němž bude zhotovitel v prodlení.
7. Nedodržení parametrů pro služby SLA opravňuje objednatele k sankcionování zhotovitele podle následujících podmínek:

Priorita	Výše smluvní pokuty	Poznámka
A - kritická	1.500,-	Za každou (i započatou) pracovní hodinu překročení lhůty pro vyřešení.
B - vysoká	1.000,-	Za každou (i započatou) pracovní hodinu překročení lhůty pro vyřešení
C - střední	500,-	Za každý další (i započatý) pracovní den překročení lhůty pro vyřešení

D - nízká	500,-	Za každý další (i započatý) pracovní den překročení lhůty pro vyřešení

Ceny smluvní pokuty jsou uvedeny bez DPH.

8. V případě podstatného porušení smlouvy má objednatel právo od smlouvy odstoupit (viz článek IX. Platnost a účinnost smlouvy).
9. Smluvní pokuty lze uložit opakovaně a za každý jednotlivý případ. Zaplacením smluvní pokuty není dotčeno právo smluvní strany na náhradu škody vzniklé porušením smluvní povinnosti, které se smluvní pokuta týká.
10. Smluvní pokuty stanovené dle tohoto článku jsou splatné do třiceti (30) dnů ode dne doručení výzvy k zaplacení smluvní pokuty povinné smluvní straně.
11. Smluvní pokuty dle této smlouvy může objednatel požadovat kumulativně, a to do maximální výše celkové ceny uvedené v článku IV. Smluvní pokutu je objednatel oprávněn započíst oproti splatným pohledávkám zhotovitele.

IX.

Platnost a účinnost smlouvy

1) Tato smlouva nabývá platnosti dnem podpisu poslední ze smluvních stran a účinnosti okamžikem jejího uveřejnění v registru smluv. Smluvní strany berou na vědomí, že tato smlouva vyžaduje uveřejnění v registru smluv podle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a registru smluv, ve znění pozdějších předpisů a s tímto uveřejněním souhlasí. Zaslání smlouvy do registru smluv se objednatel zavazuje zajistit neprodleně po podpisu smlouvy.
2) Platnost této smlouvy může být předčasně ukončena:
    a) písemnou dohodou smluvních stran;
    b) odstoupením objednatele od smlouvy v případě jejího opakovaného (tj. minimálně 2x) porušení ze strany zhotovitele nebo podstatného porušení ze strany zhotovitele;
    c) výpovědí zhotovitele, pokud bude objednatel přes písemné upozornění zhotovitele déle než 60 dnů od písemného upozornění v prodlení s plněním své platební povinnosti vůči zhotoviteli.
3) Za podstatné porušení smlouvy ze strany zhotovitele se považuje zejména prodlení zhotovitele s předáním předmětu plnění První etapy delší než 30 dnů, porušení jakékoliv povinnosti zhotovitele vyplývající ze smlouvy a její nesplnění ani v dodatečné lhůtě (alespoň 5 dnů), kterou objednatel zhotoviteli poskytl (nevylučuje-li to charakter porušené povinnosti). Odstoupení od smlouvy ze strany objednatele není spojeno s uložením jakékoliv sankce k jeho tíži.
4) Výpovědní lhůta činí jeden měsíc a počíná běžet prvním dnem měsíce následujícího po měsíci, ve kterém byla písemná výpověď doručena druhé smluvní straně.
5) Odstoupení od smlouvy nabývá účinnosti dnem doručení písemného oznámení o odstoupení od smlouvy druhé smluvní straně na adresu jejího sídla uvedené v záhlaví této smlouvy. Smluvní strany se dohodly, že odstoupení od smlouvy se považuje za doručené 10. dnem od jejího uložení u provozovatele poštovních služeb, resp. výslovným odmítnutím přijetí odstoupení druhou stranou.
6) Dojde-li k předčasnému ukončení smlouvy, je zhotovitel oprávněn požadovat pouze uhrazení částky za řádně ukončenou a objednatelem akceptovanou etapu plnění.

7) Odstoupením od této smlouvy zanikají všechny závazky smluvních stran z této smlouvy. V případě odstoupení od této smlouvy nezanikají nároky smluvních stran na náhradu škody a zaplacení smluvních pokut sjednaných pro případ porušení smluvních povinností vzniklé před skončením účinnosti této smlouvy, a ty závazky smluvních stran, které podle smlouvy nebo vzhledem ke své povaze mají trvat i nadále nebo u kterých tak stanoví ObčZ.

X.

Ochrana informací

1) Zhotovitel se zavazuje, že zachová jako citlivé informace zprávy týkající se vnitřních záležitostí smluvních stran a předmětu plnění smlouvy, pokud by jejich zveřejnění mohlo poškodit druhou stranu. Povinnost poskytovat informace podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, není tímto ustanovením dotčena.
2) Smluvní strany budou považovat za citlivé informace:
   a) informace jako citlivé označené,
   b) informace, u kterých se z povahy věci dá předpokládat, že se jedná o informace podléhající závazku mlčenlivosti nebo informace o objednateli, které by mohly z povahy věci být považovány za citlivé a které se dozvědí v souvislosti s plněním této smlouvy.
3) Smluvní strany se zavazují, že neuvolní třetí osobě informace druhé strany bez jejího souhlasu, a to v jakékoliv formě, a že podniknou všechny nezbytné kroky k zabezpečení těchto informací. Závazek mlčenlivosti a ochrany citlivých informací zůstává v platnosti po dobu 5 let po ukončení platnosti smlouvy.
4) Zhotovitel je povinen zabezpečit veškeré podklady mající charakter citlivé informace poskytnuté mu objednatelem proti odcizení nebo jinému zneužití.
5) Zhotovitel je povinen svého případného poddodavatele zavázat povinností mlčenlivosti a respektováním práv objednatele nejméně ve stejném rozsahu, v jakém je v závazkovém vztahu zavázán sám.
6) V souvislosti s důvěrností informací bere zhotovitel na vědomí, že je zákonnou povinností objednatele uveřejnit celé znění této smlouvy včetně všech jejich případných dodatků a seznamu subdodavatelů v souladu se zákonem. Splnění této, jakož i dalších zákonných povinností objednatele, není porušením důvěrnosti informací.
7) Povinnost zachovávat mlčenlivost se nevztahuje na informace:
   a) které jsou nebo se stanou všeobecně a veřejně přístupnými jinak, než porušením ustanovení tohoto odst. ze strany zhotovitele,
   b) které jsou zhotoviteli známy a byly mu volně k dispozici ještě před přijetím těchto informací od objednatele,
   c) které budou následně zhotoviteli sděleny bez závazku mlčenlivosti třetí stranou, jež rovněž není ve vztahu k nim nijak vázána,
   d) jejichž sdělení se vyžaduje ze zákona.
8) Za prokázané porušení ustanovení v tomto čl. má druhá smluvní strana právo požadovat náhradu takto vzniklé škody.

XI.

Závěrečná ustanovení

1) Vztahy mezi smluvními stranami se řídí českým právním řádem. Ve věcech smlouvou výslovně neupravených se právní vztahy z ní vznikající a vyplývající řídí příslušnými ustanoveními ObčZ a ostatními obecně závaznými právními předpisy. Rozhodčí řízení je vyloučeno. Smluvní strany sjednávají ve smyslu příslušných ustanovení občanského soudního řádu pro spory vyplývající z této smlouvy či s touto smlouvou související místní příslušnost Obvodního soudu pro Prahu 5, případně Městského soudu v Praze.
2) Nastanou-li u některé ze smluvních stran skutečnosti bránící řádnému plnění této smlouvy, je povinna to ihned bez zbytečného odkladu písemně oznámit druhé smluvní straně a vyvolat jednání objednatele a zhotovitele.
3) Vztahuje-li se důvod neplatnosti jen na některé ustanovení smlouvy, je neplatným pouze toto ustanovení, pokud z jeho povahy, obsahu anebo z okolností, za nichž bylo sjednáno, nevyplývá, že jej nelze oddělit od ostatního obsahu smlouvy. Smluvní strany se zavazují, že bezodkladně nahradí neplatné ustanovení této smlouvy jiným platným ustanovením svým obsahem podobným neplatnému ustanovení.
4) Veškeré nové závazky mezi stranami budou vznikat výhradně z této smlouvy o dílo a nahrazují původní závazky mezi stranami, a to v rozsahu, jak je specifikováno v této smlouvě.
5) Tato Smlouva je vyhotovena v elektronické podobě ve formátu PDF/A, a je podepsána zaručenými elektronickými podpisy smluvních stran založenými na kvalifikovaných certifikátech. Každá ze smluvních stran obdrží Smlouvu v elektronické podobě s uznávanými elektronickými podpisy.
6) Uzavření této Smlouvy bylo schváleno usnesením Rady Středočeského kraje č. 04-34/2024/RK ze dne 3. 10. 2024.
7) Smluvní strany prohlašují, že si Smlouvu před jejím podpisem přečetly, s obsahem souhlasí a na důkaz jejich svobodné, pravé a vážné vůle připojují oprávnění zástupci smluvních stran své elektronické podpisy.
8) Nedílnou součástí této smlouvy jsou následující přílohy:
   a) Příloha č. 1 – Technická specifikace předmětu zakázky (příloha č. 1 zadávací dokumentace)
   b) Příloha č. 2 – Podrobný položkový rozpočet

V Praze

Za Objednatele:

Dokument je podepsán elektronickým podpisem
Podepisující: **Mgr. Petra Pecková**
Organizace: Středočeský kraj
Sériové č. cert.: 22825699
Vydavatel cert.: PostSignum Qualified CA 4
Datum a čas: 21.10.2024 09:45:45
Důvod:
Místo:

.....

Mgr. Petra Pecková

hejtmanka Středočeského kraje

V Praze

Za Zhotovitele:

Petr Krutký

Digitálně podepsal Petr Krutký
Datum: 2024.10.17 10:53:54 +02'00'

.....

Petr Krutký, Key Account Manager

na základě pověření

O2 Czech Republic a.s.

Technická specifikace předmětu zakázky

Obsah

Předmětem veřejné zakázky je zajištění komplexního monitoringu ICT prostředků, kontrola činností všech registrovaných uživatelů na všech úrovních zpracování dat, sledování datového provozu informační infrastruktury, registrování útoků na prostředky ICT a průběžné odhalování případných interních a externích útočníků na ICT Krajského úřadu Středočeského kraje (dále také „KÚSK“). Nedílnou součástí veřejné zakázky je zajištění pravidelných auditů kybernetické bezpečnosti.

Za tím účelem budou v rámci veřejné zakázky pořízeny a v prostředí KÚSK implementovány odpovídající technologie a zajištěny vybrané služby externího dodavatele, a to v souladu se zákonem o kybernetické bezpečnosti a nařízením EP a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.

Řešení veřejné zakázky je koncipováno tak, aby naplnilo následující technická opatření dle Vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti (dále jen „Vyhláška“):

- § 16 Audit kybernetické bezpečnosti
- § 18 Bezpečnost komunikačních sítí
- § 22 Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů
- § 23 Detekce kybernetických bezpečnostních událostí
- § 24 Sběr a vyhodnocení kybernetických bezpečnostních událostí
- § 27 Zajišťování úrovně dostupnosti informací
- Sdílené dohledové centrum kybernetické bezpečnosti (SOC)

Dodavatelé, kteří se budou podílet na rozvoji, provozu nebo zajištění bezpečnosti významných informačních systémů, musí dle § 8 Vyhlášky, splňovat bezpečnostní požadavky pro dodavatele.

Záměrem zadavatele je nakoupit služby zařazené do 3 celků:

1. **Sdílené služby kybernetické bezpečnosti** – Jedná se o komplexní dodávku dílčích služeb po dobu 60 měsíců:

1.1. *Zaznamenávání a ukládání logů a detekce bezpečnostních událostí* – Dodavatel s využitím vlastních technologií zajistí sběr, ukládání, analýzu a bezpečné dlouhodobé uchování logů z vybraných systémů IT zadavatele. Současné dodavatel zajistí detekci bezpečnostních událostí v sledovaných systémech IT dodavatele a informování o nich.

1.2. *Analýza datových toků a detekce bezpečnostních událostí* – Dodavatel s využitím vlastních technologií zajistí sledování datových toků na výskyt anomálií a podezřelých aktivit a měření výkonových parametrů datových přenosů v síti IT zadavatele. Současně dodavatel zajistí záznam a uložení informací o sledovaných datových tocích, detekovaných událostech a stavech a o výsledcích měření sledovaných veličin.

1.3. *Dohledové centrum – SOC* – Dodavatel s využitím vlastních zdrojů zajistí provoz Bezpečnostního dohledového centra, které pro zadavatele bude provádět bezpečnostní dohled nad sledovanými systémy IT, identifikaci, hodnocení a řešení bezpečnostních incidentů včetně poskytnutí včasných informací odpovědným pracovníkům zadavatele, pravidelné reportování stavu kybernetické bezpečnosti sledovaných systémů IT a poskytování podpory v oblasti kybernetické bezpečnosti.

2. **Audit kybernetické bezpečnosti** – Jedná se o zajištění auditní činnosti vyplývající z Vyhlášky dle § 16 – Audit kybernetické bezpečnosti, každý uvedený bod bude realizován v průběhu trvání veřejné zakázky, vždy po dohodě se zadavatelem.

2.1. Penetrační testování vybrané webové aplikace – Dodavatel provede penetrační test vybraných webových aplikací po dohodě se zadavatelem. Testování bude prováděno formou gray box, dle standardu OWASP. Hodnocení provést pomocí hodnotícího systému NIST CVSSv3 (nebo vyšší).

2.2. Penetrační testování perimetru – Dodavatel provede penetrační testování perimetru. Testování bude prováděno formou gray box. Test bude proveden prostřednictvím simulace útoku na vybrané informační systémy Zadavatele.

2.3. Penetrační testování vnitřního systému – Dodavatel provede penetrační testování vnitřní infrastruktury. Testování bude prováděno formou gray box.

3. **Služby poradenství a podpory** – Jedná se o komplexní dodávku dílčích služeb, které směřují ke koordinaci a kvalitnímu provedení dodávky ostatních služeb:

3.1. *Předimplementační analýza* – Dodavatel zpracuje analýzu prostředí IT kraje, ve které popíše a vyhodnotí stav z hlediska zajištění kybernetické bezpečnosti podle §16, §17, §18, §22, §23, §24 a §27 Vyhlášky, identifikuje bezpečnostní rizika a slabá místa a navrhne opatření k odstranění neshod.

3.2. *Prováděcí dokumentace* – Dodavatel zpracuje prováděcí dokumentaci s detailním návrhem cílového stavu, s popisem aktivit potřebných pro řádnou implementaci jednotlivých služeb včetně implementace opatření navržených v předimplementační analýze a s návrhem harmonogramu implementačních prací. Součástí dokumentace bude také popis potřebných integrací do prostředí IT kraje.

3.3. *Projektové vedení dodávky* – Dodavatel zajistí řízení, koordinaci a dokumentaci postupu dodávky včetně řízení rizik a změn dodávky a poskytování pravidelných zpráv o průběhu dodávky.

3.4. *Dokumentace skutečného provedení* – Dodavatel v průběhu celé dodávky zajistí zpracování dokumentace dodaných řešení v požadovaném rozsahu.

1. Sdílené služby kybernetické bezpečnosti

Součástí služby jsou následující činnosti:

1. zaznamenávání a ukládání logů a detekce bezpečnostních událostí
2. analýza datových toků a detekce bezpečnostních událostí
3. dohledové centrum - SOC

1.1. Zaznamenávání a ukládání logů a detekce bezpečnostních událostí

Realizace tohoto opatření naplní, dle Vyhlášky, *§22 Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů, § 24 Sběr a vyhodnocování kybernetických bezpečnostních událostí.*

Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů zajistí tzv. log management. Mimo sběru logů řeší log management i zajištění jejich uložení v nezměněné podobě minimálně po zákonem definovanou dobu.

Security Information and Event Management (dále jen „SIEM“) je jedním ze základních stavebních prvků, který zajišťuje nutné bezpečnostní informace pro plnění povinností vyplývajících ze Zákona o kybernetické bezpečnosti a příslušných vyhlášek. Bez SIEM nástroje nelze reálně splnit požadavek na vyhodnocování kybernetických bezpečnostní události a následného hlášení kybernetického bezpečnostního incidentu dle § 7 a § 8 Zákona 181/2014 Sb., zákon o kybernetické bezpečnosti (dále jen „Zákon“).

Poptávané řešení bude dodáno formou rozšíření služby SOC o sběr, uložení, vyhodnocování logů a detekce kybernetických událostí, musí umožňovat efektivně reagovat na již proběhlé bezpečnostní incidenty.

Dále služba umožní dlouhodobé ukládání dat v nezpochybnitelné podobě pro potřeby shody s předpisy, požadavky pro forenzní analýzu, případné bezpečnostní audity a orgány ČR. Systém poskytuje i informace pro operační a provozní úseky, kterým bude umožněno snadnými dotazy proti uložené databázi s logy nalézat například podstatu možného bezpečnostního incidentu u aplikačního nebo infrastrukturního systému, okamžitě identifikovat podstatu identifikované hrozby, včetně rychlého dohledání událostí popisujících její příčinu. Poptávané řešení musí poskytovat vysokou dostupnost sběru a transportu logů minimálně na úrovni sběračů logů.

Navazující rozšiřující službou bude SIEM, který v reálném čase vyhodnotí bezpečnostní výjimky z uložené databáze a prezentuje data ve formě předdefinovaných reportů. Systém bude podporovat sběr všech potenciálních událostí a logů vznikajících v informačním systému KÚSK a zajistí jejich ukládání do centrálního zabezpečeného úložiště. Od systému bude požadováno, aby rychle vyhodnocoval velké množství dat, které okamžitě zpracuje.

Rozsahy a formy poskytovaných rozšiřujících služeb nesmí být pevně svázána s rozsahem a formou poskytované služby SOC.

Nabízené rozšíření služby SOC zajistí provozování celého systému tak, aby odpovídal všem relevantním zákonným normám a aktuálním trendům v dané oblasti a zadavatel nemusel investovat do dalších lidských zdrojů pro administraci, správu a podporu řešení.

Požadovaný účel služby:

Poskytnout komplexní službu pro zaznamenávání logů vznikajících na infrastruktuře KÚSK s důrazem na autonomní detekci bezpečnostních událostí v oblasti provozovaných VIS KÚSK na serverové části včetně možnosti jejich uložení do neměnné databáze. Zajistit poskytování služby dodavatelem v souladu s požadavky zadavatele a trendy v oboru.

Základní požadavky na službu:

Požadavky zadavatele jsou uvedeny ve sloupci „Minimální technické požadavky, které zadavatel požaduje“. Dodavatel je povinen vyplnit, zda jím nabízená služba tyto požadavky splňuje, a to v sloupci „Splnění požadavků zadavatele“ (dodavatel doplní prohlášení ANO nebo NE podle skutečnosti). Ve sloupci „Odkaz do nabídky“ dodavatel uvede odkaz na konkrétní část nabídky, ve které je možné ověřit splnění uvedeného požadavku. Následná smlouva s vybraným dodavatelem může být v této části upravena tak, aby obsahovala již pouze dodavatelem nabídnutou službu a její technické parametry.

Zadavatel požaduje, aby dodavatel zajistit na své náklady provoz SIEM. Dále zadavatel požaduje, aby parametry SIEMu byly minimálně níže uvedené. Důvodem požadavku, je přístup ke svému tenantu v rámci provozovaného SIEM, kdy se bude podílet zpracování jednotlivých událostí.

	Minimální technické požadavky, které zadavatel požaduje	**Splnění požadavků zadavatele (ANO/NE)**	**Odkaz do nabídky dodavatele, kde je možné ověřit splnění požadavku**	**Public/NDA**
	§22 Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů *§24 Sběr a vyhodnocování kybernetických bezpečnostních událostí*			
1	Řešení musí být funkčně i technicky odděleno od ostatních částí systému SIEM	ANO	Kap. 9.4.1 nabídky	public
2	Řešení nesmí nijak zasahovat do sbíraných systémů.	ANO	Kap. 9.4.1 nabídky	public
3	Řešení musí být schopno trvale zpracovávat 10000 EPS	ANO	Kap. 9.4.1 nabídky	public
4	Řešení musí umožnit uchování log záznamů (RAW formát) po dobu minimálně 13 měsíců	ANO	Kap. 9.4.1 nabídky	public
5	Řešení musí poskytnout vysokou dostupnost sběru logů (sběračů).	ANO	Kap. 9.4.1 nabídky	public
6	Řešení musí podporovat (sbírat, zpracovat a interpretovat) všechny typy logu a protokolů nezbytné pro zpracování dle Vyhlášky. Jmenovitě musí podporovat zejména následující typy logů a protokolů: TCP/UDP Syslog, WMI, SQL, FTP, S/TP/SCP, SNMP, ODBC/JDBC, CP-LEA, SDEE, log file protokol RAW, CEF, JSON RFC7159 a další. Windows Events Collection (WinRM/ RPC) - MS Windows 10 a vyšší, MS windows Server 2012 a vyšší, MS SQL 2008 a vyšší.	ANO	Kap. 9.4.1 nabídky	public
7	Řešení musí podporovat bezagentový sběr logů (sběr bez nutnosti instalovat agenta na cílový systém)	ANO	Kap. 9.4.1 nabídky	public

8	Řešení musí podporovat načítání log souborů (jedno a víceřádkové textové logy), kde tyto soubory budou mít stanovenou strukturu a význam dat.	ANO	Kap. 9.4.1 nabídky	public
9	Komponenta sbírající logy je posílá dále zašifrovaně a komprimovaně a umožňuje regulovat šířku užívaného pásma.	ANO	Kap. 9.4.1 nabídky	public
§ 24 Sběr a vyhodnocování kybernetických bezpečnostních událostí.				
10	Licence pro trvalé zpracování 1000 EPS v rámci celodenního průměru, která musí být rozšířitelná na 5000 EPS v celodenním průměru.	ANO	Kap. 9.4.1 nabídky	NDA
11	Architektura produktu obsahuje realtime procesory pro sběr a analýzu událostí včetně fulltext databáze pro ukládání a analýzu dat.	ANO	Kap. 9.4.1 nabídky	public
12	Řešení zvládá krátkodobé výkonové špičky (trvání 24 hodin) o objemu 7500 EPS.	ANO	Kap. 9.4.1 nabídky	NDA
13	Řešení musí obsahovat možnost minimálně 1000 sběrných konektorů	ANO	Kap. 9.4.1 nabídky	public
14	Řešení nebude licenčně omezeno úložnou kapacitou.	ANO	Kap. 9.4.1 nabídky	public
15	Licence umožňuje dočasné překročení EPS limitu na dobu několika minut bez ztráty přijímaných událostí.	ANO	Kap. 9.4.1 nabídky	public
16	Možnost definovat na základě rolí uživatelům přístup k jednotlivým zařízením, jejich skupinám či síťovým segmentům.	ANO	Kap. 9.4.1 nabídky	public
17	Možnost uložení uživatelem vytvořených pohledů na data (dashboardů, pojmenovaných dotazů) pro budoucí zpracování.	ANO	Kap. 9.4.1 nabídky	public
18	Systém umožňuje tvorbu pravidelných reportů podporujících řízení bezpečnosti podle standardu ISO 27001 s tím, že úroveň reportování bude specifikována v průběhu provozu SOC.	ANO	Kap. 9.4.1 nabídky	public
19	Služba splňuje požadavky kladené evropskými a českými bezpečnostními normami – ISO 27001, GDPR a Zákona.	ANO	Kap. 9.4.1 nabídky	public
20	Řešení Služby bude poskytovat automaticky backup/recovery procesu.	ANO	Kap. 9.4.1 nabídky	public
21	Poskytovat interní kontroly stavu zařízení (healthcheck) a upozornění uživatele v případě problému.	ANO	Kap. 9.4.1 nabídky	public
22	Poskytování analytické a korelačních funkcí bez dalších zásahů a činností (out-of-the-box).	ANO	Kap. 9.4.1 nabídky	public
23	Systém musí umožňovat definici vlastního parseru pro jednotlivé zdroje logů a tím, že uživatelská	ANO	Kap. 9.4.1 nabídky	public

	konfigurace vlastních parserů pomocí vizuálního programovacího jazyka.			
24	Požadujeme zajištění integrity nasbíraných dat, kdy data jsou kontrolována před neoprávněnou změnou nebo smazáním.	ANO	Kap. 9.4.1 nabídky	public
25	Požadujeme možnost nastavit více filtrů retenčních politik pro různé zdroje dat	ANO	Kap. 9.4.1 nabídky	public
26	Near-real-time analýza událostí	ANO	Kap. 9.4.1 nabídky	public
27	S ohledem k nastavení a provádění procesu získávání, zaznamenání a zpracování logů je přípustná detekce bezpečnostních událostí v řádu minut.	ANO	Kap. 9.4.1 nabídky	public
28	Analýza dlouhodobých trendů událostí	ANO	Kap. 9.4.1 nabídky	public
29	Pokročilé "drill-down" dohledávání v případě potřeby	ANO	Kap. 9.4.1 nabídky	public
30	Vyhledávací rozhraní systému správy logů musí poskytovat podporu jak pro zadání dotazu s použitím Booleovy logiky, tak pro zadání regulárními výrazy	ANO	Kap. 9.4.1 nabídky	public
31	Poskytování alertů na detekované anomálie, změny chování sítě a změny v generování logů a událostí	ANO	Kap. 9.4.1 nabídky	public
32	Korelační modul musí poskytovat již po instalaci (out-of-the-box) metody korelačních pravidel, která automatizují zjišťování incidentů	ANO	Kap. 9.4.1 nabídky	public
33	Korelační systém musí využívat i externí on-line reputační databázi pro vyhodnocování bezpečnostních rizik.	ANO	Kap. 9.4.1 nabídky	public
34	Systém musí být schopen využít detekované anomálie a informace ze sítě pro korelaci s logy do jednotných incidentů, pro zpřesnění kontextu a snížení false-positives	ANO	Kap. 9.4.1 nabídky	public
35	Řešení musí poskytnout alerting vycházející z detekovaných bezpečnostních hrozeb od monitorovaných zařízení	ANO	Kap. 9.4.1 nabídky	public
36	Požadujeme schopnost samostatného “učení” normálního stavu. Podle nastavené bezpečnostní politiky pak reagovat na vznik skupinových nebo kontextuálních anomálií.	ANO	Kap. 9.4.1 nabídky	public
37	Vykonávání akci v závislosti na přijatém logu jako např. zaslat email, notifikaci nebo spustit předem definovaný skript	ANO	Kap. 9.4.1 nabídky	public
38	Schopnost pracovat s IP geolokacemi (botnet kanály atp.)	ANO	Kap. 9.4.1 nabídky	public

39	Generování alertu při výpadku logů z konkrétního zařízení	ANO	Kap. 9.4.1 nabídky	public
40	Vestavěný mechanismus na klasifikaci systémů podle typu (např. mail server vs. databázový server)	ANO	Kap. 9.4.1 nabídky	public
41	Poskytování rozhraní pro reporting, pomocí kterého lze vytvářet nové sestavy bez nutnosti sestavovat SQL dotazy	ANO	Kap. 9.4.1 nabídky	public
42	Požadujeme pravidelnou, plánovanou tvorbu takových reportů minimálně ve formátech PDF a CSV + podporu alespoň jednoho běžně používaného formátu pro strojové čtení (XML či JSON)	ANO	Kap. 9.4.1 nabídky	public
43	Řešení musí obsahovat nativní podporu vysoké dostupnosti (HA) bez rozšiřujících komponent/software třetích stran.	ANO	Kap. 9.4.1 nabídky	public
44	Řešení musí nabízet přístup k datům skrze otevřené REST API pro integraci s dalšími systémy.	ANO	Kap. 9.4.1 nabídky	public
45	Řešení musí uchovávat logy v normalizovaném formátu, tak i „raw“ formátu.	ANO	Kap. 9.4.1 nabídky	public
46	Řešení musí být navázáno na národní centrum kybernetické bezpečnosti CSIRT a publikovat v konzoli jím aktuálně uveřejněné hrozby.	ANO	Kap. 9.4.1 nabídky	public

Další požadavky na rozšiřující službu SOC:

- Nabízená služba detekce bezpečnostních událostí musí:
  - naplnit požadavky pro významné informační systémy pro řešenou oblast ze Zákona a příslušných vyhlášek v platném znění a souvisejících část normy ČSN ISO/IEC 27001:2014 (nebo rovnocenné řešení).
  - zajistit dlouhodobé uschování logů pro předložení organizacím zabývajícím se bezpečností, zejména NÚKIB a orgánům činným v trestním řízení.
  - zajistit v rámci poskytování služby SIEM napojení „Primárních aktiv“, kterými jsou významné informační systémy (VIS) Krajského úřadu Středočeského kraje, pokud tato aktiva poskytují využitelné výstupy, které lze automatizovaně zpracovat:
    1. Spisová služba
    2. Ekonomický systém
    3. Emailová komunikace (O365)
    4. Webový portál
    5. Portál krizového řízení
  - zajistit v rámci poskytování služby SIEM napojení „Podpůrných aktiv“, kterými jsou bezpečnostní systémy a veškeré ICT prvky pro zajištění provozní dostupnosti, důvěrnosti a integrity informací:
    1. Ochrana perimetru a přístupy k perimetru sítí Internet/DMZ/LAN/WiFi
    2. Komponenty datové sítě (switch, router, hub, access point)
    3. Network Behavior Analyzer

4. Autentizační a autorizační systémy
5. Anti (mallware, spam, adware) systémy
6. Vulnerability management systém
7. Databázové systémy
8. Provozní dohledové systémy (Servery, Storage, Datová síť, Energy infrastruktura, Zálohování dat)
9. Zálohovací systémy
10. Operační systémy serverů – Unix a Windows
11. Virtualizační infrastruktura

Záruka a podpora (maintenance) výrobce:

Poskytovatel služby zajistí, že po celou dobu poskytování služby budou veškeré využité části kryté zárukou a podporou ze strany výrobce. Z tohoto důvodu zadavatel nepřipouští open sourcové řešení.

Doba poskytování služby:

Služba bude poskytována po dobu 60 měsíců.

1.2. Analýza datových toků a detekce bezpečnostních událostí

Realizace tohoto opatření naplní § 23 Detekce kybernetických bezpečnostních událostí Vyhlášky.

Jedná se o komplexní službu pro monitorování sítě KÚSK na základě datových toků, kterou umožní nástroje pro sledování provozu a zabezpečení sítě. Služba bude podporovat následná řešení vyskytujících se problémů a nestandardních stavů v síti, monitoring aktivit uživatelů a provozovaných SW aplikací. Služba umožní správcům pohled na využití síťového provozu na infrastruktuře KÚSK. Služba disponuje funkcí, která umožní sledovat výkonové parametry sítě a technologií analýzy datových toků včetně vyhodnocování chování sítě v návaznosti na aktuální hrozby a nestandardní stavy.

Rozsahy a formy poskytovaných rozšiřujících služeb nesmí být pevně svázána s rozsahem a formou poskytované služby SOC.

Nabízené rozšíření služby SOC zajistí provozování celého systému tak, aby odpovídal všem relevantním zákonným normám a aktuálním trendům v dané oblasti a zadavatel nemusel investovat do dalších lidských zdrojů pro administraci, správu a podporu řešení.

Požadovaný účel služby:

Poskytnout komplexní službu pro zaznamenávání aplikačních logů vznikajících na infrastruktuře KÚSK s důrazem na autonomní detekci bezpečnostních událostí v oblasti provozovaných VIS KÚSK na serverové části včetně možnosti jejich uložení do neměnné databáze. Zajistit poskytování služby dodavatelem v souladu s požadavky zadavatele a trendy v oboru.

Základní služby:

Požadavky zadavatele jsou uvedeny ve sloupci „Minimální technické požadavky, které zadavatel požaduje“. Dodavatel je povinen vyplnit, zda jím nabízená služba tyto požadavky splňuje, a to v sloupci „Splnění požadavků zadavatele“ (dodavatel doplní prohlášení ANO nebo NE podle skutečnosti). Ve sloupci „Odkaz do nabídky“ dodavatel uvede odkaz na konkrétní část nabídky, ve které je možné ověřit splnění uvedeného požadavku. Následná smlouva s vybraným dodavatelem může být v této části upravena tak, aby obsahovala již pouze dodavatelem nabídnutou službu a její technické parametry.

Minimální technické požadavky, které zadavatel požaduje		**Splnění požadavků zadavatele (ANO/NE)**	**Odkaz do nabídky dodavatele, kde je možné ověřit splnění požadavku**	**Public/NDA**
Část	**Popis**			
Řešení	▪ V rámci monitoringu infrastruktury KÚSK se předpokládá využití: ○ 1x Kolektor a detekční moduly. ○ 2x Modul sonda. ○ Dále jako zdroj budou připojeny alespoň 2x core přepínače.	ANO	Kap. 9.4.2 nabídky	NDA
Obecné				
Monitorování sítě	▪ Schopnost analyzovat provoz ze SPAN portu centrálních switchů, TAP	ANO	Kap. 9.4.2 nabídky	public

	zařízení nebo zdrojů NetFlow dat. ▪ Protokoly NetFlow v9 a IPFIX nebo ekvivaletní. ▪ Podpora pro IPv4, IPv6, VLAN, MPLS ▪ Neviditelné na L3 vrstvě (monitorovací porty nemají IP, je zcela pasivní. ▪ Zaznamenávání vybrané komunikace do formátu PCAP z celé sítě. ▪ Řešení, které významným způsobem nezatíží datové linky zadavatele (nárůst provozu o max 5%)			
Komponenty				
Modul NetFlow sonda	▪ 2 kusy sondy ▪ Realizováno hardware komponentami s instalaci do 19“ racku, každá sonda max. 1RU. ▪ Zabezpečená vzdálená správa, dohled a konfigurace. ▪ Podpora standardu NSEL, monitorování MAC adres. ▪ Fyzická monitorovací rozhraní minimálně 2x 10Gbps pro každou sondu ▪ Sondy poskytnou na každém monitorovacím portu monitorování v rychlosti 10 Gbps ▪ Podpora pro příjem a analýzu HTTP/HTTPS provozu. ▪ Pasivní zapojení monitorovacích portů přes TAP. ▪ Zpracování všech FLOWs – nesamplované. ▪ Monitoring zpoždění sítě a odezvy aplikace.	ANO	Kap. 9.4.2 nabídky	public
Modul detekce anomálií na síti	▪ Nástroj bude poskytován na kolektoru, kde bude dostupné grafické rozhraní a které bude i zdrojem pro reporting událostí pro rozšiřující službu SIEM. ▪ Sběr a zpracování statistik o síťovém provozu.	ANO	Kap. 9.4.2 nabídky	public

	▪ Sbírání informací z netflow sond. ▪ Detekce nežádoucích vzorů chování na síti (útoky, anomálie datového provozu, nežádoucí aplikace, detekce virů a botnetů ve vnitřní síti, detekce odchozího spamu, provozních problémů). ▪ Detekce anomálií vzhledem k dlouhodobému profilu chování zařízení na síti. ▪ Předdefinovaná sada pravidel pro odhalování obecných anomálií v síti. ▪ Vyhodnocování na základě implementace standardu Bidirectional flows (RFC 5103). ▪ Integrace informací ze služeb DNS, DHCP, WHOIS, geolokační služby.			
Modul analýzy a monitorování komunikace aplikací a systémů	▪ Pro naplnění zákona č.110/2019 Sb. Zákon o zpracování osobních údajů v aktuálním znění má řešení detekovat a lokalizovat aktuální změny komunikace systémů, aplikací a uživatelů pracujících se zákonně klasifikovanými informacemi, tj.: o Sledování komunikace systémů o Sledování komunikace aplikací	ANO	Kap. 9.4.2 nabídky	public
Modul analýzy a monitorování výkonosti	▪ Sledování provozní výkonnosti datové sítě, minimálně Round Trip Time ▪ Sledování provozní výkonnosti všech aplikací z provozu datové sítě, především reakce databází a WWW strojů.	ANO	Kap. 9.4.2 nabídky	public
<u>Správa</u>				
Víceuživatelský přístup	▪ Možnost definovat k jakým datům má jednotlivý uživatel přístup i v jednotlivých aplikačních modulech.	ANO	Kap. 9.4.2 nabídky	public

Webové rozhraní	▪ Uživatelsky definovat dashboard. ▪ Správu provádět prostřednictvím webového rozhraní.	ANO	Kap. 9.4.2 nabídky	public
Aktualizace	▪ Zařízení pravidelně samostatně aktualizuje znalostní bázi.	ANO	Kap. 9.4.2 nabídky	public
Reporty				
Generování	▪ Vytvářet krátkodobé i dlouhodobé grafy a přehledy s různými typy pohledů rozdělených do kategorií podle objemu (počet přenesených bytů, toků, paketů), IP provozu (TCP, UDP, ICMP, ostatní) nebo protokolu (http, IMAP, SSH), aplikačních protokolů atp. ▪ Generování statistik a podrobných výpisů nad volitelnými časovými intervaly. ▪ Export reportů a grafů alespoň do PDF.	ANO	Kap. 9.4.2 nabídky	public
Zasílání logů do SIEM	▪ Zasílání logů o detekovaných událostech ze všech detekčních modulů s možností uživatelské konfigurace přes GUI ▪ Konfigurovatelný obsah logů	ANO	Kap. 9.4.2 nabídky	public

Dílčí cíle služby:

- Navrhnout řešení služby dle požadavků výše.
- Navrhnout a popsat architekturu, včetně potřebného HW a potřebného SW, včetně požadované integrace do prostředí Zadavatele.
- Naplnit požadavky pro významné informační systémy pro řešenou oblast ze Zákona a příslušných vyhlášek v platném znění a souvisejících část normy ČSN ISO/IEC 27001:2014 (nebo rovnocenné řešení).

Záruka a podpora (maintenance) výrobce:

Poskytovatel služby zajistí, že po celou dobu poskytování služby budou veškeré využité části kryté zárukou a podporou ze strany výrobce. Z tohoto důvodu zadavatel nepřipouští open sourcové řešení.

Doba poskytování služby:

Služba bude poskytována po dobu 60 měsíců.

1.3. Dohledové centrum - SOC

Předmětem poptávky je komplexní řešení pro centralizovanou správu, ukládání a vyhodnocování logů v nezměnitelné podobě z libovolných síťových aktivních prvků, operačních systémů a používaného aplikačního software provozované formou služby Sdíleného dohledového centra kybernetické bezpečnosti (SOC – Security Operation Centra). Implementace systému bude v provedena v souladu s § 22 a § 24 Vyhlášky v *platném znění*.

Požadovaný účel implementace opatření:

Zajištění externě provozované / dodávané služby dohledového ICT bezpečnostního centra - SOC.

Základní požadavky implementace systému:

Požadavky zadavatele jsou uvedeny ve sloupci „Minimální technické požadavky, které zadavatel požaduje“. Dodavatel je povinen vyplnit, zda jím nabízený produkt / řešení tyto požadavky splňuje, a to v sloupci „Splnění požadavků zadavatele“ (dodavatel doplní prohlášení ANO nebo NE podle skutečnosti). Ve sloupci „Odkaz do nabídky“ dodavatel uvede odkaz na konkrétní část nabídky, ve které je možné ověřit splnění uvedeného požadavku. Následná smlouva s vybraným dodavatelem může být v této části upravena tak, aby obsahovala již pouze dodavatelem nabídnuté zařízení a jeho technické parametry.

Minimální technické požadavky, které zadavatel požaduje		**Splnění požadavků zadavatele (ANO/NE)**	**Odkaz do nabídky dodavatele, kde je možné ověřit splnění požadavku**	**Public/NDA**
Požadavky na SOC				
1.	Poskytovatel prokazatelně doloží, že provozuje CSIRT (CERT), který je registrovaný v databázi TF – CSIRT Trusted Introducer – úroveň Accredited nebo vyšší / anebo u jiné obdobné organizace zabývající se bezpečnostními incidenty a reakcemi na ně, přičemž registrace u těchto organizací potvrzuje schopnost poskytovatele reagovat na bezpečnostní incidenty a spolupracovat s dalšími CSIRTy a potvrzuje schopnost poskytovatele poskytovat kvalitní služby, a to vše na úrovní srovnatelné alespoň s úrovni Accredited v rámci databáze TF – CSIRT Trusted Introducer.	ANO	Kap. 9.4.3 nabídky	public
2.	Poskytovatel musí uvést adresu, kde jsou ukládána data SOC k prokázání zpracování dat v působnosti právních norem ČR	ANO	Kap. 9.4.3 nabídky	public
3.	Informace o provozu a potenciálních zranitelnostech informačních systémů umožní zavádění preventivních opatření a předcházení případným bezpečnostním incidentům.	ANO	Kap. 9.4.3 nabídky	public
4.	Zavedením systému zadavatel získá schopnost detekce bezpečnostních incidentů a informace pro jejich rychlejší a efektivnější řešení.	ANO	Kap. 9.4.3 nabídky	public

5.	Reporty systému budou sloužit pro přehlednou kontrolu stavu a chování informačních systémů a uživatelů za určité období (typicky 1 měsíc) a ke kontrole dodržování compliance („jednání v souladu s pravidly") organizace zadavatele.	ANO	Kap. 9.4.3 nabídky	public
6.	Pro případné auditní akce ze strany zadavatele systém umožní provádění tzv. NBA (Network Behavioral Analysis), tj. automatického trvalého monitorování síťového provozu nad prostředím sdíleného dohledového centra kybernetické bezpečnosti. Ze stejného důvodu bude nad významnými součástmi služby provozován nástroj pro audit a monitoring aktivit uživatelů.	ANO	Kap. 9.4.3 nabídky	public
7.	Data uložená v systému a systémem archivovaná budou zajištěna a zabezpečena před neoprávněnou změnou i pro účely vyšetřování případného bezpečnostního incidentu. Data / logy budou uskladněna v prostředí poskytnutém dodavatelem, a to minimálně na dobu požadovanou zákonem.	ANO	Kap. 9.4.3 nabídky	public
8.	Vytvoření bezpečného sdíleného uložiště pro sdílení kompletních materiálů k poskytované službě.	ANO	Kap. 9.4.3 nabídky	public
9.	Detailní analýza bude zahrnovat identifikaci zdrojů dat, jejichž provozně bezpečnostní informace bude nutné, popř. vhodné sbírat, korelovat a analyzovat. Analýza bude podléhat schválení zadavatelem.	ANO	Kap. 9.4.3 nabídky	public
10.	Zdroje dat budou vybrány z tzv. primárních a podpůrných (technických) aktiv zadavatele (zejm. se jedná o systémy a řešení poptávané v této veřejné zakázce). K jejich určení bude využito Vyhlášky č. 317/2014 Sb. o významných informačních systémech a jejich určujících kritérií přiměřeně uzpůsobených a aplikovaných na prostředí zadavatele (zadavatel provozu celkem 4 významné informační systémy – GINIS, e-mail, elektronickou spisovou službu a Service Desk). Dále bude pro určení zdrojů dat využito vstupního osobního setkání (workshopu) se správci provozovaných informačních a komunikačních systémů v rozsahu jednoho pracovního dne.	ANO	Kap. 9.4.3 nabídky	public
11.	Předimplementační analýza bude obsahovat následující oblasti specifické pro SOC: (a) specifikace profilu pro každý napojovaný zdroj dat, včetně určení vhodné úrovně detailu logování, odpovídající jeho roli v infrastruktuře, (b) klasifikaci zdrojů informací pro stanovení priority události (stejná událost z různých zdrojů může mít různou prioritu) a z hlediska poskytovaných logů (obsažené informace, struktura logu),	ANO	Kap. 9.4.3 nabídky	public

	(c) doporučení nastavení logování pro jednotlivé zdroje, (d) výběr událostí a parametry jejich záznamů a metody sběru z jednotlivých zdrojů, (e) návrh parserů pro zdroje, které nebudou systémem přímo podporovány, (f) návrh doplňování logovaných informací z dalších zdrojů pro zlepšení jejich relevantnosti či srozumitelnosti, (g) metody a pravidla identifikace, zpracování a vyhodnocování událostí, návrhy korelací, (h) pravidla pro vznik varováni, upozornění, incidentů včetně priority, (i) doporučenou strukturu oprávnění a řízení přístupových práv (j) proaktivní a reaktivní procesy (aktivity, role, výstupy, doba odezvy) v případě výskytu varování, upozornění, incidentu a apod. (k) popis zajištění autentičnosti logů, (l) definice pohledů na události v konzoli uživatelů (např. setřídění událostí podle zdroje, typu, priority, stupně důležitosti, času vzniku apod.), (m) návrh zálohování konfigurace a dat, (n) návrh průběhu Zkušebního provozu pro ověření funkčnosti systému v reálném provozu, (o) návrh retence logů a archivů, (p) návrh způsobu napojení řešení na monitorovací systém dodavatele a definice procesů reakce, které jsou v souladu s platnou legislativou a bezpečnostní politikou ISKÚ, (q) popis monitorovaných aktivit přispívajících k naplnění požadavků dle zákona č.110/2019 Sb. v aktuálním znění a k naplnění požadavků dle nařízení Evropského parlamentu a Rady (EU) 2016/679 (GDPR).			
12.	Součástí dodávky bude návrh změn konfigurací dotčených a souvisejících systémů, koordinace provedení změn s provozovateli systémů a ověření správné konfigurace.	ANO	Kap. 9.4.3 nabídky	public
13.	Součástí dodávky bude návrh a provedení funkčních testů (musí zahrnovat výkonové testy, testy archivace/obnovy logů a ověření detekce neoprávněně modifikace logů). Návrh podléhá schválení zadavatele.	ANO	Kap. 9.4.3 nabídky	public

Požadovaná podpora SOC				
14.	Průběžné monitorování IT prvků dodaných v rámci této veřejné zakázky, popř. prvků IT, které mohou ovlivnit jejich chod. Počet sledovaných parametrů nesmí být prakticky omezen (min. stovky).	ANO	Kap. 9.4.3 nabídky	public
15.	Monitoring bude probíhat minimálně dle výstupů ze služby pro zaznamenávání a ukládání logů a detekce bezpečnostních událostí (SIEM), systému analýzy datových toků a detekce bezpečnostních událostí, systému pro pokročilý provozní dohled a firewallů zadavatele.	ANO	Kap. 9.4.3 nabídky	public
16.	Helpdeskový systém s on-line přístupem pro kompletní správu požadavků včetně uchování historie požadavků a jejich řešení.	ANO	Kap. 9.4.3 nabídky	public
17.	Rozšířený monitoring a specifické služby provozního zajištění komodity SOC: (r) Provádění monitoringu systému a zpracovávaných dat v rozsahu potřebném pro provádění následujících služeb. (s) Informování odpovědných osob zadavatele o vzniku bezpečnostního incidentu v reálném čase za pomocí základních komunikačních nástrojů (mail / SMS / tel). (t) Zahájení řešení bezpečnostního incidentu do 4 hodin od vzniku, řízení souvisejících činností správců a případných dalších dotčených osob. (u) Zakládání tiketů, proaktivní komunikace o jejich řešení. Komunikace s třetí stranou jako NBÚ, NUKIB, CSIRT atd. (v) Rozšířený reporting – detailní report o událostech a incidentech s návrhy systematických opatření 1x měsíčně. Vzdálená prezentace reportu např. formou videokonference. (w) Kontinuální skenování aktiv definovaných danou sítí/sítěmi a zranitelností relevantních pro daná aktiva. Minimálně na začátku poskytování služby budou provedeny plné skeny a dále vždy 1x měsíčně skeny rozdílové. (x) Přístup administrátorů zadavatele ke sledovaným parametrům alespoň v režimu čtení prostřednictvím grafického rozhraní (GUI – dashboard apod.).	ANO	Kap. 9.4.3 nabídky	public
18.	Dodavatel zpracuje a poskytne zadavateli každý měsíc Report, ve kterém je popsán průběh realizace Plnění za uplynulé období, provedené	ANO	Kap. 9.4.3 nabídky	public

	služby a návrh doporučených opatření pro další období pro zvýšení bezpečnosti, dostupnosti a prevenci incidentů.			
SLA		ANO	Kap. 9.4.3 nabídky	public
19.	Přístup k podpoře služby - HotLine/Ticket systém – 24 x 7	ANO	Kap. 9.4.3 nabídky	public
20.	Přístup k webovému portálu služby – 24 x 7	ANO	Kap. 9.4.3 nabídky	public
21.	Reakční čas na mimořádnou událost – do 60 minut	ANO	Kap. 9.4.3 nabídky	public
22.	**Služba Monitoringu a detekce - Zajištění Operátorské úrovně** Průběžné sledování provozu prostředí objednatele. Real-time analýza situace v napojených zařízeních podle skupin, kategorií zařízení a podle kontextu log záznamů nebo událostí. Posouzení kontextu anomálie a příčin vzniku situace s případnou eskalací problému objednatele na analytického specialistu dodavatele.	ANO	Kap. 9.4.3 nabídky	public
23.	**Služba reakce na nestandardní situace v provozu bezpečnostních systémů – Zajištění analytické úrovně** Zpracování analytických scénářů na aktuální kybernetické hrozby. Posouzení eskalovaného problému objednatele analytickým specialistou. Detekce a vyhodnocení závažnosti identifikovaných anomálií. Posouzení a ve spolupráci se Zadavatelem případná eskalace nestandardní situace v provozu objednatele na službu včasné výstrahy a reakce na incident v rámci bezpečnostních struktur ČR. 1x za měsíc předání analytického reportu za uplynulé období do 10 pracovního dne v následném měsíci interpretující stav bezpečnosti prostředí, účinnost nápravných opatření a seznam eskalace incidentů.	ANO	Kap. 9.4.3 nabídky	public

<u>Doba poskytování služby</u>:

Dohledové centrum bude poskytováno formou služby po dobu 60 měsíců.

2. Služby poradenství a podpory, resp. „Služby spojené s implementací IS“

2.1. Předimplementační analýza

Před implementací řešení zpracuje dodavatel předimplementační analýzu, minimálně pro následující oblasti a pro oblasti specifické pro jednotlivé dodávané produkty a služby:

1. Detailní popis stávajícího stavu, identifikaci slabých míst a bezpečnostních rizik, včetně vazeb na HW a SW systémy TCK.
2. Způsob začlenění nabízených komodit do prostředí TCK, popis začlenění nabízených / dodávaných služeb do procesů zadavatele.
3. Síťová infrastruktura ve vztahu k plánovanému využití.
4. SAN infrastruktura ve vztahu k plánovanému využití.
5. Virtualizační infrastruktura (serverová, disková) ve vztahu k plánovanému využití.
6. Integrace nabízených softwarových systémů.
7. Rekonfigurace stávajících systémů.
8. Dopady implementace na dostupnost a funkčnost stávajících služeb.
9. Požadované součinnosti zadavatele a jejich rozsah.
10. Návrh opatření k odstranění neshod zjištěných v průběhu analýzy.

Výstupem předimplementační analýzy bude písemná zpráva, která podléhá schválení zadavatelem.

2.2. Prováděcí dokumentace

Po schválení předimplementační analýzy zpracuje dodavatel prováděcí dokumentaci minimálně pro následující oblasti a pro oblasti specifické pro jednotlivé dodávané produkty a služby:

1. Dodavatel před zahájením implementačních prací zpracuje prováděcí dokumentaci, která bude vycházet ze schválené předimplementační analýzy a bude zahrnovat všechny aktivity potřebné pro řádné zajištění implementace předmětu plnění veřejné zakázky do stávajícího prostředí TCK.
2. Prováděcí dokumentace musí být před zahájením prací schválena zadavatelem.
3. Prováděcí dokumentace musí zohlednit podmínky stávajícího stavu, požadavky cílového stavu a musí obsahovat minimálně tyto části:
    a. Detailní popis cílového stavu včetně funkcionalit jednotlivých částí dodávky.
    b. Nutné a doporučené optimalizační a konfigurační změny dodávaných systému i všech navázaných systémů TCK (vSphere, LAN, SAN, zálohování, monitorování atd.).
    c. Způsob zajištění potřebného HW a SW.
    d. Způsob zajištění koordinace realizace předmětu plnění s běžným provozem.
    e. Detailní návrh a popis postupu implementace předmětu plnění.
    f. Detailní popis zajištění bezpečnosti informací.
    g. Detailní harmonogram realizace včetně uvedení kritických milníků.
    h. Návrh designu síťového a bezpečnostního řešení a jeho konfigurace.
    i. Návrh designu aplikačních řešení.
    j. Vazby na stávající systémy a jejich konfigurace.

k. Návrh akceptačních kritérií a akceptačních testů.

Výstupem prováděcí dokumentace bude písemná zpráva, která podléhá schválení zadavatelem.

2.3. Projektové vedení dodávky

V průběhu celého plnění veřejné zakázky (dodávka řešení) zajistí dodavatel projektové vedení dodávky:

S ohledem na rozsah projektu a dopad jeho zavedení do produkčního provozu je požadováno aplikování základních principů projektového řízení ze strany dodavatele. Jedná se o následující aktivity:

1. Řízení projektových prací v souladu s uzavřenou smlouvu s ohledem na:
    a. věcné plnění dané smlouvou,
    b. řízení postupu prací s ohledem na závazný harmonogram projektu,
    c. dodržování termínů a milníků harmonogramu.
2. Zpracování pravdivých, úplných a věcně jasných a vypovídajících zápisů z konzultačních schůzek a pracovních jednání.
3. Prezenční účast odpovědné osoby dodavatele na kontrolních dnech v sídle zadavatele, případně se souhlasem obou smluvních stran formou videokonference nebo telekonference.
4. Reporting projektu na úrovni pravidelných dvoutýdenních písemných zpráv směrem k odpovědné osobě zadavatele.
5. Řízení rizik projektu.
6. Řízení změn na projektu – v případě odsouhlasení změn spolupráce při implementaci změn do projektu, komunikace s realizačním týmem.

2.4. Dokumentace

Zadavatel požaduje v rámci plnění zpracování a dodání konečné a úplné dokumentace k dodanému řešení v následující skladbě:

1. Uživatelská dokumentace – v rozsahu konkrétních nasazených funkcionalit u zadavatele.
2. Administrátorská dokumentace – správa a konfigurace v rozsahu konkrétního (nasazeného) řešení. Dokumentace musí být zpracována v takovém rozsahu, který umožní odborným IT pracovníkům zadavatele systémy spravovat a udržovat bez jakékoliv součinnosti dodavatele (s výjimkou mimořádných událostí a chyb v dodaném SW a HW).
3. Bezpečnostní dokumentace – příručka bezpečnostního správce informačních systémů.
4. Integrační dokumentace – dokumentace všech nasazených a dodaných rozhraní k informačním systémům.

2.5. Provádění prací

Zadavatel požaduje, aby v rámci plnění zakázky práce probíhaly:

1. V souladu se všemi běžnými zákonnými předpisy týkajícími se bezpečnosti práce
2. Dle zadavatelem schválené prováděcí dokumentace
3. Byly vždy řádně dokumentovány
4. A práce, které generují riziko pro technologie, infrastrukturu, či prostředí zadavatele, byly explicitně schvalovány pověřenou osobou zadavatele

Podrobný nabídkový (položkový) rozpočet				
1. Sdílené služby kybernetické bezpečnosti (2. etapa)				
Název položky	**Počet měsíců**	**Jednotková cena bez DPH**		**Cena celkem bez DPH**
Zaznamenávání a ukládání logů a detekce bezpečnostních událostí (služba)	60	149 500,00 Kč		8 970 000,00 Kč
Analýza datových toků a detekce bezpečnostních událostí (služba)				
Dohledové centrum - SOC (služba)				
Celkem	**-**		**-**	**8 970 000,00 Kč**
2. Audit kybernetické bezpečnosti (3. etapa)				
Název položky	**Počet kusů**	**Jednotková cena bez DPH**		**Cena celkem bez DPH**
Penetrační testování vybrané webové aplikace	1	187 500,00 Kč		187 500,00 Kč
Penetrační testování perimetru	1	62 500,00 Kč		62 500,00 Kč
Penetrační testování vnitřního systému	1	187 500,00 Kč		187 500,00 Kč
Celkem	**-**		**-**	**437 500,00 Kč**
3. Služby poradenství a podpory (1. etapa)				
Název položky	**Počet kusů**	**Cena bez DPH**		**Cena celkem bez DPH**
Předimplementační analýza	1	100 000,00 Kč		100 000,00 Kč
Prováděcí dokumentace	1	94 620,00 Kč		94 620,00 Kč
Projektové vedení dodávky	1	161 730,00 Kč		161 730,00 Kč
Dokumentace	1	14 670,00 Kč		14 670,00 Kč
Provádění prací	1	200 000,00 Kč		200 000,00 Kč
Celkem	**-**		**-**	**571 020,00 Kč**
4. Výkony poskytované nad rámec služeb dle smlouvy				
Název položky	**Počet MD**	**Jednotková cena bez DPH (1 MD)**		**Cena celkem bez DPH**
Výkony nad rámec služeb dle smlouvy	50	14 445,00 Kč		722 250,00 Kč
Celkem	**-**		**-**	**722 250,00 Kč**

NABÍDKOVÁ CENA CELKEM	**10 700 770,00 Kč**