**Technická specifikace předmětu zakázky**

Obsah

[*1.* Sdílené služby kybernetické bezpečnosti 3](#_Toc166164210)

[*1.1.* Zaznamenávání a ukládání logů a detekce bezpečnostních událostí 3](#_Toc166164211)

[*1.2.* Analýza datových toků a detekce bezpečnostních událostí 9](#_Toc166164212)

[*1.3.* Dohledové centrum - SOC 14](#_Toc166164213)

[*2.* Služby poradenství a podpory, resp. „Služby spojené s implementací IS“ 19](#_Toc166164214)

[*2.1.* Předimplementační analýza 19](#_Toc166164215)

[*2.2.* Prováděcí dokumentace 19](#_Toc166164216)

[*2.3.* Projektové vedení dodávky 20](#_Toc166164217)

[*2.4.* Dokumentace 20](#_Toc166164218)

[*2.5.* Provádění prací 20](#_Toc166164219)

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. *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.
   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.
   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.
   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. *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.
   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:
   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.
   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. *Projektové vedení dodávky* – Dodavatel zajistí řízení, koordinaci a dokumentaci postupu dodávky včetně řízení rizik a změn dodávky a poskytování pravidelných zpráv o průběhu dodávky.
   4. *Dokumentace skutečného provedení* – Dodavatel v průběhu celé dodávky zajistí zpracování dokumentace dodaných řešení v požadovaném rozsahu.

## 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

## 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 | [doplní účastník] | [doplní účastník] | public |
| 2 | Řešení nesmí nijak zasahovat do sbíraných systémů. | [doplní účastník] | [doplní účastník] | public |
| 3 | Řešení musí být schopno trvale zpracovávat 10000 EPS | [doplní účastník] | [doplní účastník] | public |
| 4 | Řešení musí umožnit uchování log záznamů (RAW formát) po dobu minimálně 13 měsíců | [doplní účastník] | [doplní účastník] | public |
| 5 | Řešení musí poskytnout vysokou dostupnost sběru logů (sběračů). | [doplní účastník] | [doplní účastník] | 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. | [doplní účastník] | [doplní účastník] | public |
| 7 | Řešení musí podporovat bezagentový sběr logů (sběr bez nutnosti instalovat agenta na cílový systém) | [doplní účastník] | [doplní účastník] | public |
| 8 | Řešení musí podporovat načítání log souborů (jedno a víceřádkové textové logy), kde tyto soubory budou mít stanovenou strukturu a význam dat. | [doplní účastník] | [doplní účastník] | public |
| 9 | Komponenta sbírající logy je posílá dále zašifrovaně a komprimovaně a umožňuje regulovat šířku užívaného pásma. | [doplní účastník] | [doplní účastník] | 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. | [doplní účastník] | [doplní účastník] | NDA |
| 11 | Architektura produktu obsahuje realtime procesory pro sběr a analýzu událostí včetně fulltext databáze pro ukládání a analýzu dat. | [doplní účastník] | [doplní účastník] | public |
| 12 | Řešení zvládá krátkodobé výkonové špičky (trvání 24 hodin) o objemu 7500 EPS. | [doplní účastník] | [doplní účastník] | NDA |
| 13 | Řešení musí obsahovat možnost minimálně 1000 sběrných konektorů | [doplní účastník] | [doplní účastník] | public |
| 14 | Řešení nebude licenčně omezeno úložnou kapacitou. | [doplní účastník] | [doplní účastník] | public |
| 15 | Licence umožňuje dočasné překročení EPS limitu na dobu několika minut bez ztráty přijímaných událostí. | [doplní účastník] | [doplní účastník] | public |
| 16 | Možnost definovat na základě rolí uživatelům přístup k jednotlivým zařízením, jejich skupinám či síťovým segmentům. | [doplní účastník] | [doplní účastník] | public |
| 17 | Možnost uložení uživatelem vytvořených pohledů na data (dashboardů, pojmenovaných dotazů) pro budoucí zpracování. | [doplní účastník] | [doplní účastník] | 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. | [doplní účastník] | [doplní účastník] | public |
| 19 | Služba splňuje požadavky kladené evropskými a českými bezpečnostními normami – ISO 27001, GDPR a Zákona. | [doplní účastník] | [doplní účastník] | public |
| 20 | Řešení Služby bude poskytovat automaticky backup/recovery procesu. | [doplní účastník] | [doplní účastník] | public |
| 21 | Poskytovat interní kontroly stavu zařízení (healthcheck) a upozornění uživatele v případě problému. | [doplní účastník] | [doplní účastník] | public |
| 22 | Poskytování analytické a korelačních funkcí bez dalších zásahů a činností (out-of-the-box). | [doplní účastník] | [doplní účastník] | public |
| 23 | Systém musí umožňovat definici vlastního parseru pro jednotlivé zdroje logů a tím, že uživatelská konfigurace vlastních parserů pomocí vizuálního programovacího jazyka. | [doplní účastník] | [doplní účastník] | public |
| 24 | Požadujeme zajištění integrity nasbíraných dat, kdy data jsou kontrolována před neoprávněnou změnou nebo smazáním. | [doplní účastník] | [doplní účastník] | public |
| 25 | Požadujeme možnost nastavit více filtrů retenčních politik pro různé zdroje dat | [doplní účastník] | [doplní účastník] | public |
| 26 | Near-real-time analýza událostí | [doplní účastník] | [doplní účastník] | public |
| 27 | S ohledem k nastavení a provádění procesu získávání, zaznamenání a zpracování logů je přípustná detekce bezpečnostních událostí v řádu minut. | [doplní účastník] | [doplní účastník] | public |
| 28 | Analýza dlouhodobých trendů událostí | [doplní účastník] | [doplní účastník] | public |
| 29 | Pokročilé "drill-down" dohledávání v případě potřeby | [doplní účastník] | [doplní účastník] | public |
| 30 | Vyhledávací rozhraní systému správy logů musí poskytovat podporu jak pro zadání dotazu s použitím Booleovy logiky, tak pro zadání regulárními výrazy | [doplní účastník] | [doplní účastník] | public |
| 31 | Poskytování alertů na detekované anomálie, změny chování sítě a změny v generování logů a událostí | [doplní účastník] | [doplní účastník] | public |
| 32 | Korelační modul musí poskytovat již po instalaci (out-of-the-box) metody korelačních pravidel, která automatizují zjišťování incidentů | [doplní účastník] | [doplní účastník] | public |
| 33 | Korelační systém musí využívat i externí on-line reputační databázi pro vyhodnocování bezpečnostních rizik. | [doplní účastník] | [doplní účastník] | 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 | [doplní účastník] | [doplní účastník] | public |
| 35 | Řešení musí poskytnout alerting vycházející z detekovaných bezpečnostních hrozeb od monitorovaných zařízení | [doplní účastník] | [doplní účastník] | public |
| 36 | Požadujeme schopnost samostatného “učení” normálního stavu. Podle nastavené bezpečnostní politiky pak reagovat na vznik skupinových nebo kontextuálních anomálií. | [doplní účastník] | [doplní účastník] | public |
| 37 | Vykonávání akci v závislosti na přijatém logu jako např. zaslat email, notifikaci nebo spustit předem definovaný skript | [doplní účastník] | [doplní účastník] | public |
| 38 | Schopnost pracovat s IP geolokacemi (botnet kanály atp.) | [doplní účastník] | [doplní účastník] | public |
| 39 | Generování alertu při výpadku logů z konkrétního zařízení | [doplní účastník] | [doplní účastník] | public |
| 40 | Vestavěný mechanismus na klasifikaci systémů podle typu (např. mail server vs. databázový server) | [doplní účastník] | [doplní účastník] | public |
| 41 | Poskytování rozhraní pro reporting, pomocí kterého lze vytvářet nové sestavy bez nutnosti sestavovat SQL dotazy | [doplní účastník] | [doplní účastník] | 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) | [doplní účastník] | [doplní účastník] | public |
| 43 | Řešení musí obsahovat nativní podporu vysoké dostupnosti (HA) bez rozšiřujících komponent/software třetích stran. | [doplní účastník] | [doplní účastník] | public |
| 44 | Řešení musí nabízet přístup k datům skrze otevřené REST API pro integraci s dalšími systémy. | [doplní účastník] | [doplní účastník] | public |
| 45 | Řešení musí uchovávat logy v normalizovaném formátu, tak i „raw“ formátu. | [doplní účastník] | [doplní účastník] | public |
| 46 | Řešení musí být navázáno na národní centrum kybernetické bezpečnosti CSIRT a publikovat v konzoli jím aktuálně uveřejněné hrozby. | [doplní účastník] | [doplní účastník] | public |
| 47 | SIEM použitý v řešení musí být zařazen do 5 posledních studií agentury Gartner (tzv. magických kvadrantů) | [doplní účastník] | [doplní účastník] | 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 informační́ 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.

## 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. | **[vyplní účastník]** | **[vyplní účastník]** | NDA |
| Obecné | | | |  |
| Monitorování sítě | * Schopnost analyzovat provoz ze SPAN portu centrálních switchů, TAP 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%) | **[vyplní účastník]** | **[vyplní účastník]** | public |
| Komponenty | | | |  |
| Modul NetFlow sonda | * 2 kusy sondy * Realizováno hardware komponentami s instalaci do 19“ racku, každá sonda max. 1RU. (možná SW varianta) * 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. | **[vyplní účastník]** | **[vyplní účastník]** | 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. * 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. | **[vyplní účastník]** | **[vyplní účastník]** | public |
| 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.:   + Sledování komunikace systémů   + Sledování komunikace aplikací | **[vyplní účastník]** | **[vyplní účastník]** | 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. | **[vyplní účastník]** | **[vyplní účastník]** | public |
| Správa | | | |  |
| Víceuživatelský přístup | * Možnost definovat k jakým datům má jednotlivý uživatel přístup i v jednotlivých aplikačních modulech. | **[vyplní účastník]** | **[vyplní účastník]** | public |
| Webové rozhraní | * Uživatelsky definovat dashboard. * Správu provádět prostřednictvím webového rozhraní. | **[vyplní účastník]** | **[vyplní účastník]** | public |
| Aktualizace | * Zařízení pravidelně samostatně aktualizuje znalostní bázi. | **[vyplní účastník]** | **[vyplní účastník]** | 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. | **[vyplní účastník]** | **[vyplní účastník]** | public |
| Zasílání logů do SIEM | * Zasílání logů o detekovaných událostech ze všech detekčních modulů s možností uživatelské konfigurace přes GUI * Konfigurovatelný obsah logů | **[vyplní účastník]** | **[vyplní účastník]** | 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.

## 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 | **[vyplní účastník]** | **[vyplní účastník]** | public |
| 2. | Poskytovatel musí uvést adresu, kde jsou ukládána data SOC k prokázání zpracování dat v působnosti právních norem ČR | **[vyplní účastník]** | **[vyplní účastník]** | public |
| 3. | Informace o provozu a potenciálních zranitelnostech informačních systémů umožní zavádění preventivních opatření a předcházení případným bezpečnostním incidentům. | **[vyplní účastník]** | **[vyplní účastník]** | public |
| 4. | Zavedením systému zadavatel získá schopnost detekce bezpečnostních incidentů a informace pro jejich rychlejší a efektivnější řešení. | **[vyplní účastník]** | **[vyplní účastník]** | 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. | **[vyplní účastník]** | **[vyplní účastník]** | 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. | **[vyplní účastník]** | **[vyplní účastník]** | 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. | **[vyplní účastník]** | **[vyplní účastník]** | public |
| 8. | Vytvoření bezpečného sdíleného uložiště pro sdílení kompletních materiálů k poskytované službě. | **[vyplní účastník]** | **[vyplní účastník]** | 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. | **[vyplní účastník]** | **[vyplní účastník]** | 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. | **[vyplní účastník]** | **[vyplní účastník]** | public |
| 11. | Předimplementační analýza bude obsahovat následující oblasti specifické pro SOC:   * + - * 1. specifikace profilu pro každý napojovaný zdroj dat, včetně určení vhodné úrovně detailu logování, odpovídající jeho roli v infrastruktuře,         2. 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),         3. doporučení nastavení logování pro jednotlivé zdroje,         4. výběr událostí a parametry jejich záznamů a metody sběru z jednotlivých zdrojů,         5. návrh parserů pro zdroje, které nebudou systémem přímo podporovány,         6. návrh doplňování logovaných informací z dalších zdrojů pro zlepšení jejich relevantnosti či srozumitelnosti,         7. metody a pravidla identifikace, zpracování a vyhodnocování událostí, návrhy korelací,         8. pravidla pro vznik varováni, upozornění, incidentů včetně priority,         9. doporučenou strukturu oprávnění a řízení přístupových práv         10. proaktivní a reaktivní procesy (aktivity, role, výstupy, doba odezvy) v případě výskytu varování, upozornění, incidentu a apod.         11. popis zajištění autentičnosti logů,         12. definice pohledů na události v konzoli uživatelů (např. setřídění událostí podle zdroje, typu, priority, stupně důležitosti, času vzniku apod.),         13. návrh zálohování konfigurace a dat,         14. návrh průběhu Zkušebního provozu pro ověření funkčnosti systému v reálném provozu,         15. návrh retence logů a archivů,         16. návrh způsobu napojení řešení na monitorovací systém dodavatele a definice procesů reakce, které jsou v souladu s platnou legislativou a bezpečnostní politikou ISKÚ,         17. 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). | **[vyplní účastník]** | **[vyplní účastník]** | public |
| 12. | Součástí dodávky bude návrh změn konfigurací dotčených a souvisejících systémů, koordinace provedení změn s provozovateli systémů a ověření správné konfigurace. | **[vyplní účastník]** | **[vyplní účastník]** | 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. | **[vyplní účastník]** | **[vyplní účastník]** | 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). | **[vyplní účastník]** | **[vyplní účastník]** | 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. | **[vyplní účastník]** | **[vyplní účastník]** | public |
| 16. | Helpdeskový systém s on-line přístupem pro kompletní správu požadavků včetně uchování historie požadavků a jejich řešení. | **[vyplní účastník]** | **[vyplní účastník]** | public |
| 17. | Rozšířený monitoring a specifické služby provozního zajištění komodity SOC:   * + - * 1. Provádění monitoringu systému a zpracovávaných dat v rozsahu potřebném pro provádění následujících služeb.         2. Informování odpovědných osob zadavatele o vzniku bezpečnostního incidentu v reálném čase za pomocí základních komunikačních nástrojů (mail / SMS / tel).         3. Zahájení řešení bezpečnostního incidentu do 4 hodin od vzniku, řízení souvisejících činností správců a případných dalších dotčených osob.         4. Zakládání tiketů, proaktivní komunikace o jejich řešení. Komunikace s třetí stranou jako NBÚ, NUKIB, CSIRT atd.         5. Rozšířený reporting – detailní report o událostech a incidentech s návrhy systematických opatření 1x měsíčně. Vzdálená prezentace reportu např. formou videokonference.         6. 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.         7. Přístup administrátorů zadavatele ke sledovaným parametrům alespoň v režimu čtení prostřednictvím grafického rozhraní (GUI – dashboard apod.). | **[vyplní účastník]** | **[vyplní účastník]** | public |
| 18. | Dodavatel zpracuje a poskytne zadavateli každý měsíc Report, ve kterém je popsán průběh realizace Plnění za uplynulé období, provedené služby a návrh doporučených opatření pro další období pro zvýšení bezpečnosti, dostupnosti a prevenci incidentů. | **[vyplní účastník]** | **[vyplní účastník]** | public |
| **SLA** |  | **[vyplní účastník]** | **[vyplní účastník]** | public |
| 19. | Přístup k podpoře služby - HotLine/Ticket systém – 24 x 7 | **[vyplní účastník]** | **[vyplní účastník]** | public |
| 20. | Přístup k webovému portálu služby – 24 x 7 | **[vyplní účastník]** | **[vyplní účastník]** | public |
| 21. | Reakční čas na mimořádnou událost – do 60 minut | **[vyplní účastník]** | **[vyplní účastník]** | 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. | **[vyplní účastník]** | **[vyplní účastník]** | 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. | **[vyplní účastník]** | **[vyplní účastník]** | public |

**Doba poskytování služby:**

Dohledové centrum bude poskytováno formou služby po dobu 60 měsíců.

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

## 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.**

## 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:
   1. Detailní popis cílového stavu včetně funkcionalit jednotlivých částí dodávky.
   2. Nutné a doporučené optimalizační a konfigurační změny dodávaných systému i všech navázaných systémů TCK (vSphere, LAN, SAN, zálohování, monitorování atd.).
   3. Způsob zajištění potřebného HW a SW.
   4. Způsob zajištění koordinace realizace předmětu plnění s běžným provozem.
   5. Detailní návrh a popis postupu implementace předmětu plnění.
   6. Detailní popis zajištění bezpečnosti informací.
   7. Detailní harmonogram realizace včetně uvedení kritických milníků.
   8. Návrh designu síťového a bezpečnostního řešení a jeho konfigurace.
   9. Návrh designu aplikačních řešení.
   10. Vazby na stávající systémy a jejich konfigurace.
   11. Návrh akceptačních kritérií a akceptačních testů.

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

## 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:
   1. věcné plnění dané smlouvou,
   2. řízení postupu prací s ohledem na závazný harmonogram projektu,
   3. 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.

## 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.

## 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