Příloha č. 1
Specifikace plnění

Technická specifikace
„Provedení služeb bezpečnostního dohledu ICT infrastruktury organizace“

Předmět zakázky
Předmětem zakázky je zajištění služeb bezpečnostního dohledu ICT infrastruktury organizace k zajištění dohledu a provozu nástrojů pro vyhodnocování kybernetických bezpečnostních událostí ve výpočetních systémech a v komunikačních sítích, které zadavatel využívá nebo provozuje.

V následujících podkapitolách uvádíme soubor všech požadavků na předmětné služby. Tyto požadavky představují kompletní a současně minimální úroveň, kterou musí poskytovatelé služby splnit.

Předpokládaný harmonogram
Zadavatel požaduje od dodavatele služby napojení do služby do 5 pracovních dnů od účinnosti smlouvy (den jejího uveřejnění dle zákona č.34/2015 Sb. o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv) při poskytnutí nezbytné součinnosti zadavatele.

Ostatní požadavky zadavatele na plnění zakázky
Všichni účastníci projektu (realizační tým) musí být zaměstnanci poskytovatele služby.

Součinnost zadavatele
Zadavatel pro účely poskytování služby zpřístupní poskytovateli následující technologie:

- připojení technologie do ISP na jednotlivých pobočkách zadavatele;
- připojení LAN části infrastruktury na zařízení pro sběr analytických dat (Netflow/Sflow/IPFIX);
- nasměruje syslog data na smluvené IP adresy a porty tak, aby se data dostala šifrovaně až do systémů dodavatele za účelem analýzy těchto dat pro účely dohledu a reakce na incidenty.

Technická specifikace zajištění služby
Předmětem zakázky je zajištění služeb bezpečnostního dohledu ICT infrastruktury, a to především:

- formou služby provozovat centralizovanou správu, ukládání a vyhodnocování logů v nezměnitelné podobě z libovolných síťových aktivních prvků, operačních systémů a používaného aplikačního software, tj. především z routerů dodaných poskytovatelem na všech pobočkách a nástroje EDR používaného zadavatelem. Implementace systému bude provedena

v souladu s *ust. §§ 21 a 22 Detekce kybernetických bezpečnostních událostí a zaznamenávání událostí vyhlášky č. 409/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností.*

- formou služby provozovat centralizovanou správu, ukládání a vyhodnocování komunikačních spojení a výkonnostních parametrů datové sítě, tj. nástroj sběru a vyhodnocení NetFlow. Implementace systému bude provedena v souladu s *ust. §. 23 Vyhodnocování kybernetických bezpečnostních událostí vyhlášky č. 409/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností.*

Požadavky zadavatele jsou uvedeny ve sloupci „Minimální technické požadavky, které zadavatel požaduje“. Poskytovatel služby je povinen vyplnit, zda jím nabízený produkt/řešení tyto požadavky splňuje, a to v sloupci „Splnění požadavků Zadavatele“ (poskytovatel služby doplní prohlášení ANO nebo NE podle skutečnosti včetně odkazu na konkrétní část nabídky, ve které je možné ověřit splnění uvedeného požadavku).

Minimální technické požadavky, které Zadavatel požaduje		**Splnění požadavků Zadavatele (ANO/NE)**
	Požadavky na služby bezpečnostního dohledu ICT	
1.	Zadavatel předpokládá realizaci uvedených úloh prostředky a technologiemi poskytovatele nejméně v rozsahu poskytnutí řešení SIEM, NDR a dalších nástrojů využívajících Threat Intelligence Platform dat.	ANO
2.	Bezpečnostní dohledové centrum poskytovatele služby musí podporovat práci s nástroji zadavatele.	ANO
3.	Poskytovatel služby navrhne modifikaci relevantních procesů na straně zadavatele, včetně atributů a parametrů procesů potřebných pro doručení služby a řádné plnění. Konfigurační změny a úpravy prostředků zadavatele nutných pro připojení k službě provede poskytovatel služby vlastním nákladem jako součást služby a předá je do vlastnictví zadavatele.	ANO
4.	Poskytovatel služby navrhne konfiguraci SIEM řešení včetně atributů a parametrů potřebných pro splnění služby.	ANO
5.	Služba dohledového týmu bude zajišťována v ČJ	ANO
6.	Služba dohledu je zajišťována z území ČR.	ANO
7.	V rámci služby bude poskytovatelem služby vytvořeno bezpečné uložiště pro sdílení kompletních materiálů k poskytované službě.	ANO

8.	**Správa a dohled zdrojů** – zajištění Performance a Capacity management procesů.	ANO
9.	**Síťový dohled** – zajištění dohledu nad síťovým provozem, detekce anomálií a blokace podezřelého provozu.	ANO
10.	**Bezpečnostní dohled –** zajištění správy a provozu nástroje SIEM, NDR a XDR.	ANO
11.	**Incident management** – zajištění Operátorské činnosti, Incident handling, Incident Response.	ANO
12.	**Analýza incidentů** – zajištění odborné činnosti v detekci a lokalizaci příčin incidentů Analytikem ze strany poskytovatele služby.	ANO
13.	**Návrhy systematických opatření** – sestavení opatření v organizační a technické úrovni pro posouzení zadavatelem.	ANO
14.	**Návrhy řešení incidentů** – zajištění odborné činnosti pro kategorizaci na interní a externí příčiny incidentů a k nim příslušných opatření.	ANO
15.	**Reporting a analýza stavů, událostí a incidentů** – zajištění odborné činnosti pro doložení úrovně bezpečnosti vůči interním kontrolním procesům nebo pro doložení vůči externím kontrolním autoritám.	ANO
16.	**Sběr datových analytik o síťových tocích** bude využíván primárně prostřednictvím routerů na pobočkách zadavatele se zajištěným šifrováním přenosu dat do systému pro analýzu.	ANO
17.	**Kybernetická bezpečnost** – Personální zajištění služby pracovníky s odbornou způsobilostí vyhovující požadavkům na zajištění kybernetické bezpečnosti v souladu s požadavky *zákona 264/2025 Sb. o kybernetické bezpečnosti* v celém průběhu služby a všech jejích procesů a rutin.	ANO
18.	**Pokročilá analýza anomálií** bude postavena na systémech IDS/IPS, XDR a bude využívat obohacení dat ze zdrojů jako OSINT, CVE, MITRE ATTACK a dalších Threat Intelligence zdrojů.	ANO
19.	**Business Continuity** – Služba (včetně všech komponent, které využívá) musí být odolná proti výpadkům a poruchám. Všechny komponenty služby musí být schopny dlouhodobého provozu bez změny chování a úbytku výkonu.	ANO
20.	**Zajištění souladu s NIS2** - Všechny parametry služby musí zajistit na úrovni technologií i procesů splnění požadavků na zajištění potřebné míry informační bezpečnosti, zejména pak: Důvěrnost, Dostupnost, Nepopiratelnost, Autentizaci, Autorizaci.	ANO
21.	Pokud zadavatel z organizačních důvodů rozhodne pro in-sourcing části procesů nebo workflow (např. Zřízení analytického týmu, útvaru provozu bezpečnostní infrastruktury, Operation centra pro aplikace, systémy, databáze, datovou síť, bezpečnostní komponenty atp.) musí služba poskytovatele umožnit separaci na úrovní procesů, systémů, dat, přístupových oprávnění, včetně transferu historických dat a informací do prostředí zadavatele. Náklady na změnu hradí zadavatel. Požadavek na vydělení části služby do samostatné části, není důvodem k okamžité výpovědi smlouvy.	ANO

22.	**Adaptace a akceptace sdílených procesů** – Služba zajistí úpravu procesů na straně poskytovatele služby a návrh na jejich integraci s relevantními procesy na straně zadavatele.	ANO
23.	**SLA procesních vstupů a výstupů** – Služba zajistí monitoring procesů na straně poskytovatele služby a zadavatele.	ANO
24.	**Vizitace zadavatele v místě výkonu služby** – poskytovatel služby před podpisem smlouvy umožní zadavateli návštěvu vlastního bezpečnostního dohledového centra, aby si mohl ověřit splnění požadavků. Zjištění nedodržení požadavků je důvod pro vyloučení poskytovatele služby.	ANO
	Technické požadavky na službu	
25.	Poskytovatel služby provozuje vlastní *Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí*, který umožňuje napojení na technologie zadavatele.	ANO
26.	Rozhodné operace a manipulace jsou prováděny prostředky zadavatele a nástroje poskytovatele služby budou sloužit na jeho straně pro případnou agregaci informací v rámci jeho procesů. Žádný ze způsobů propojení nesmí omezit nebo narušit primární autonomní fungování celého řešení jen prostředky zadavatele.	ANO
27.	V rámci služby poskytovatel zajistí provozní monitoring bezpečnostních nástrojů zadavatele, dle předmětu zakázky, v rozsahu: • dostupnost a funkčnost bezpečnostních nástrojů, • vytíženost bezpečnostních nástrojů, • detekce vyčerpání kapacitních zdrojů u bezpečnostních nástrojů. V rámci služby poskytovatel zajistí funkční IDS/IPS systém na všech pobočkách zadavatele.	ANO
28.	V rámci služby poskytovatel zajišťuje nastavování bezpečnostních nástrojů zadavatele, dle předmětu zakázky, v rozsahu: • úprava a optimalizace korelačních pravidel, dle požadavku zadavatele nebo dle best-practice poskytovatele, • přidávání nových zařízení, • vytváření nových scénářů pro detekci, • úprava nastavení nástrojů, dle požadavku zadavatele nebo NÚKIB.	ANO
	Požadovaná podpora bezpečnostního dohledu	
29.	**Ticketovací systém** – služba s on-line přístupem pro kompletní správu požadavků, včetně uchování historie požadavků a jejich řešení.	ANO
30.	Přístup zadavatele k podpoře *provozu systémů* – HotLine v rozsahu 24/7.	ANO
31.	Přístup zadavatele k podpoře *Incident Response* – HotLine, telefon/ email na členy CSIRT v rozsahu 24/7.	ANO
32.	Zakládání tiketů, proaktivní komunikace o jejich řešení. Komunikace s třetí stranou jako NBÚ, NÚKIB, kooperující CSIRT atd.	ANO
33.	Přístup *administrátorů zadavatele* ke sledovaným parametrům služby prostřednictvím grafického rozhraní (GUI – dashboard apod.), alespoň v režimu čtení nebo v přístupové roli *Auditor*.	ANO
34.	**Notifikace/Eskalace** – Informování odpovědných osob zadavatele o vzniku	ANO

	bezpečnostního incidentu v reálném čase za pomocí základních komunikačních nástrojů (mail / SMS / telefon).	
35.	**Vulnerability management** – služba kontinuálního skenování aktiv zadavatele definovaných danou sítí/sítěmi a zranitelností relevantních pro daná aktiva. Minimálně na začátku poskytování služby budou provedeny plné skeny a dále alespoň 1x v průběhu 12 měsíců skeny rozdílové. Poskytovatel bude vždy doručovat technický protokol s výsledky těchto skenů.	ANO
36.	**Vulnerability management** – Relevance ***zranitelnosti*** – U aktiv musí být ověřena relevantnost incidentů pro dané aktivum vulnerability scannerem.	ANO
37.	**Reporty – Rozšířený *reporting*** – detailní report o událostech a incidentech s návrhy systematických opatření alespoň 2x v průběhu 12 měsíců. Vzdálená prezentace reportu, např. formou videokonference. Prezentace reportů v rozsahu min. 30 minut - max. 3 hod.	ANO
38.	**Reporty** – ***Standard*** – poskytovatel v rámci služby zpracuje a poskytne zadavateli každý měsíc Report, ve kterém je popsáno: • průběh realizace Plnění služby za uplynulé období; • provedené služby za uplynulé období; • návrh doporučených opatření pro další období pro zvýšení bezpečnosti, dostupnosti a v prevenci eliminace incidentů.	ANO
39.	**Technologie sběru dat** – Služba zajistí užití nástroje SIEM a nástroje monitoringu síťového provozu jako základního zdroje dat a bude s ním komunikovat průmyslově standardními protokoly. Navrhované řešení poskytovatele zahrnuje služby: • zajišťuje na straně zadavatele sběr, přenos a uložení logů a jejich vyhodnocování v rámci nástroje SIEM. Služba SOC poskytovatele služby plní roli federativní komponenty k výkonu operátorské činnosti v rámci služby. • zajišťuje na straně zadavatele sběr dat typu NetFlow a jejich vyhodnocení v rámci nástroje poskytovatele. • zajišťuje na straně zadavatele sběr logů a jejich vyhodnocení v rámci nástroje poskytovatele. • zajišťuje na straně zadavatele sběr logů a jejich vyhodnocení v rámci nástroje SIEM poskytovatele. • poskytovatel má na své straně služby ve svém komunikačním bodu Internetu zařazenu komponentu „DDoS“ ochrana. • má interní úložiště s minimální propustností 1Gbit/s s využitím VPN v redundantní konfiguraci. • má bezpečné interní uložiště s minimální propustností 1 Gbit/s	ANO

	s využitím VPN v redundantní konfiguraci. • má k dispozici interní uložiště v objemu dostačujícím na uchování dat v souladu se zákonnou úpravou (ZoKB). • umí efektivně detekovat nové nebo dosud neznámé hrozby či transakční záznamy, a identifikovat jejich relevanci k provozní nebo bezpečnostní kategorii u zadavatele.	
40.	**Base line analýza** – Služba zajistí porovnání neobvyklých počtů určitých událostí oproti jinému období z minulosti.	ANO
41.	**Členění aktiv** – Aktiva musí: • být možno rozdělit: o podle jejich důležitosti v procesech zadavatele; o podle typu a povahy generování dat: ▪ Log data na struktuře Syslog přes UDP/TCP ve standardu IETF, ▪ NetFlow ve standardu IETF. ▪ Transakční záznamy – SIP, DNS, DHCP, FRAUD ve standardu IETF • mít uživatelsky definovatelné kategorie a parametry podle požadavků zadavatele.	ANO
42.	**Kategorizace aktiv** – Služba zajistí jednotnou evidenci a vyhodnocení kategorie aktiv, podle povahy aktiva (viz bod 46.). Podle těchto kategorií bude poskytovatel služby utvářet další pravidla nebo reporty v prostředcích zadavatele.	ANO
43.	**Manuální parsovací pravidla** – Služba zajistí generování parsovacích pravidel a reportů v prostředcích zadavatele.	ANO
44.	**Historická korelace** – Služba zajistí ověření nového korelačního pravidla proti historickým datům.	ANO
45.	**Režim Maintenance** – Služba musí být schopna běhu v režimu údržby ohlášenou zadavatelem, kdy se údržbou dotčených zdrojů/aktiv nebudou vyhlašovat alerty.	ANO
46.	**Služba Monitoringu a detekce** • Průběžné sledování provozu prostředí zadavatele. • Real-time analýza situace v napojených zařízeních podle skupin, kategorií zařízení a podle kontextu log záznamů nebo událostí. • Real-time odborné posouzení bezpečnostní situace a provozního stavu. V případě anomálie posouzení její relevance a závažnosti. • Posouzení kontextu anomálie a příčin vzniku situace s případnou eskalací problému zadavatele na analytického specialistu poskytovatele služby.	ANO

47.	**Služba včasné výstrahy a reakce na nestandardní situace v provozu bezpečnostních systémů** • Zpracování analytických scénářů na aktuální kybernetické hrozby. • Posouzení eskalovaného problému Zadavatele analytickým specialistou poskytovatele. • Detekce a vyhodnocení závažnosti identifikovaných anomálií. • Posouzení a případná eskalace nestandardní situace v provozu Zadavatele na službu včasné výstrahy a reakce na incident v rámci bezpečnostních struktur ČR.	ANO
48.	**Služba bezpečného zálohování** – součástí služby je zajištění uložení tzv. nesmazatelných záloh k lokálnímu partnerovi v objemu dostatečném pro zajištění plnění předmětu zakázky a zákonných požadavků na imutabilní storage poskytovatele služby. Zálohy musí být uchovávány nejméně po dobu vyžadovanou právními předpisy. Služba bezpečných záloh zajišťovaných Poskytovatelem zahrnuje: • Správu záloh fyzických serverů, • Správu záloh virtuálních serverů, • Monitoring úspěšnosti záloh a report v případě přerušení zálohovacího procesu s následkem nedoručení záloh.	ANO
	SLA	
49.	Poskytovatel služby musí provozovat vlastní bezpečnostní dohledovou službu v režimu 24x7x365	ANO
50.	Pro každý kybernetický incident (dle §2 odst. 2 písm. f) ZokB) prochází poskytovatel služby následným postupem k určení kategorií kybernetických bezpečnostních incidentů podle následků a negativních projevů pro doporučení opatření či součinnosti v následné reakci: <u>Fáze Detekce</u> • Monitoring prostředí vymezeného zadavatelem. • Dohledování bezpečnostní situace zadavatele. • Detekce anomálie – rozpoznání odchylky od běžného stavu nebo od zadavatelem normovaného stavu. <u>Fáze Přiřazení</u> • Klasifikace anomálie – určení závažnosti ve škále: o False-Positive Alarm – způsobuje falešný alarm z důvodu: ▪ chyby v úsudku míry závažnosti anomálie; ▪ nepřesnosti rozpoznání odchylky vzniklé při dohledování a monitoringu v předchozí fázi Detekce. o Bezpečnostní událost – anomálie, která může způsobit narušení bezpečnosti: ▪ informací v informačních systémech zadavatele; ▪ služeb zadavatele; ▪ a integrity datových sítí zadavatele. o Bezpečnostní incident – anomálie, která narušila či narušuje	ANO

	bezpečnost: ▪ informací v informačních systémech zadavatele; ▪ služeb zadavatele; ▪ a integritu datových sítí zadavatele nebo jiných subjektů. <u>Fáze Analýza</u> • Vyhodnocení anomálie – vyhodnocení relevance: o k systémům zadavatele; o k procesům zadavatele; o k zákonným normám ČR vztažených na zadavatele. • Klasifikace incidentu – začlenění incidentu do bezpečnostního typu kategorie dle určení zadavatelem: o Podle příčiny: ▪ incident způsobený kybernetickým útokem nebo jinou událostí vedoucí k průniku do systému nebo k omezení dostupnosti služeb; ▪ incident způsobený škodlivým kódem; ▪ incident způsobený překonáním technických opatření; ▪ incident způsobený porušením organizačních opatření; ▪ incident spojený s projevem trvale působících hrozeb; ▪ ostatní incidenty způsobené kybernetickým útokem. o Podle dopadu: ▪ incident způsobující narušení důvěrnosti aktiv; ▪ incident způsobující narušení integrity aktiv; ▪ incident způsobující narušení dostupnosti aktiv; ▪ incident způsobující kombinaci výše uvedených dopadů. • Kategorizace incidentu – začlenění incidentu podle významnosti.	
51.	**Kategorie III** – do 60 minut – velmi závažný kybernetický bezpečnostní incident, při kterém je přímo a významně narušena bezpečnost poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje neprodlené zásahy obsluhy s tím, že musí být všemi dostupnými prostředky zabráněno dalšímu šíření kybernetického bezpečnostního incidentu, včetně minimalizace vzniklých i potenciálních škod.	ANO
52.	**Kategorie II** – do 2 hodin – závažný kybernetický bezpečnostní incident, při kterém je narušena bezpečnost poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje neprodlené zásahy obsluhy s tím, že musí být vhodnými prostředky zabráněno dalšímu šíření kybernetického incidentu včetně minimalizace vzniklých škod.	ANO
53.	**Kategorie I** – do 24 hodin – méně závažný kybernetický bezpečnostní incident, při kterém dochází k méně významnému narušení bezpečnosti poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje zásahy obsluhy s tím, že musí být vhodnými prostředky omezeno další šíření kybernetického bezpečnostního incidentu včetně minimalizace vzniklých škod. Jedná se	ANO

	o bezpečnostní incidenty, které nespadají do kategorií III a II.	