Technická specifikace

1 Technický popis záměru zadavatele

1.1 Základní odůvodnění potřeby SOC v PNvD

Zadavatel je lůžkovým zdravotnickým zařízením poskytujícím akutní psychiatrickou péči v plném rozsahu. Pro potřeby zajištění vedení zdravotnické dokumentace i podpůrných procesů provozuje vlastními silami serverovou infrastrukturu pro běh zdravotnických i administrativních informačních systémů a rozsáhlou LAN, vč. klientských stanic. Správa ICT infrastruktury je zajišťována interními pracovníky oddělení výpočetní techniky.

Vyšší úroveň elektronizace a s tím spojené závislosti procesů nemocnice na ICT, spolu s nutností plnit legislativní povinnosti v oblasti kybernetické bezpečnosti, vedly odpovědné pracovníky zadavatele k podrobnější analýze potřeb v této oblasti a možnostech jejich saturace. Dle stávajících informací ohledně připravované legislativy (směrnice NIS2 a nový Zákon o kybernetické bezpečnosti) by se měla nově PNvD stát povinným subjektem s vyšším režimem povinností. Procesy governance kybernetické bezpečnosti jsou aktuálně v rámci PNvD rozšiřovány i o povinnosti vyplývající z výše zmíněné legislativy a rizikovosti provozovaných ICT aktiv tak, aby v době účinnosti nového ZoKB byly všechny povinnosti plněny.

Poskytování služby SOC (spolu s dalšími navázanými analytickými a detekčními nástroji) zajistí pro PNvD:

- odpovídající rychlost reakce na kybernetické události a jejich triáž,
- saturaci chybějících kompetencí v dynamické oblasti kybernetické bezpečnosti,
- zvýšení úrovně dohledu nad provozovanou infrastrukturou s využitím automatizace a pokročilých vyhodnocovacích algoritmů,
- potřebné vstupy pro procesy řízení kybernetických událostí, procesy řízení kontinuity činností a havarijní reakce.

1.2 Východisko pro výběrové řízení

V rámci výběrového řízení zadavatel požaduje zajištění monitoringu kybernetické bezpečnosti prostřednictvím služeb bezpečnostního dohledového centra (SOC).

Služba zajistí monitoring nad stávajícími informačními systémy a infrastrukturou dodavatele. Zadavatel požaduje, aby součástí dodávaného plnění bylo zajištění integrovaného přístupu k monitoringu a vyhodnocování kybernetické bezpečnosti ICT prostředí PNvD, které se bude sestávat z následujících technologií:

- EDR/XDR (Endpoint Detection and Response),
- NDR (Network Detection and Response),
- VM (Vulnerability Management),
- LM+SIEM (Log Management a Security information and Event Monitoring)
- SOAR (Security Orchestration and Response).

Dodávkou se rozumí:

- Úvodní analýza popisující podobu implementace technologií do prostředí ICT infrastruktury PNvD.
- Provedení samotné implementace spočívající v instalaci HW a SW prvků pro monitoring ICT infrastruktury a napojení na vzdálenou infastrukturu SOC.
- Nastavení procesů koordinace mezi SOC a pracovníky IT PNvD, především v oblasti procesů vyhodnocování a reakce na kybernetické události, vč. zaškolení a náležité dokumentace těchto procesů dle požadavků relevantní legislativy a příkladů dobré praxe.
- Spuštění a rutinní provoz dodávaného řešení po dobu minimálně 5 let.
- Poskytování doplňkových konzultací v oblasti informační bezpečnosti na základě objednávek a schválených výkazů práce.

1.3 Rozsah provozované infrastruktury

Níže uvádíme indikativní souhrn rozsahu provozované infrastruktury zadavatele (PNvD), který by měl sloužit jako podklad pro určení potřebných kapacit nabízeného řešení. V rámci této infrastruktury je požadován provoz služeb SOC.

Podrobný přehled o infastruktuře zadavatele a konfiguraci nabízeného řešení SOC si vítězný dodavatel udělá v rámci úvodní implementační analýzy.

Rozsah ICT infrastruktury

Provoz ICT infrastruktury je zajištěn interními silami vlastními správci – jak na straně síťové infrastruktury, tak serverové infrastruktury a úložišť. Provoz serverových technologií je zajištěn v rámci dvou vlastních serveroven. Místní síť je provedena s optickou páteří mezi pavilony s částečným zokruhováním. Fyzická přítomnost správců je v rámci pracovní doby, jinak v rámci stanovených telefonních pohotovostí.

Druh prvku	**Výrobce / technologie / OS**	**Počet**
Fyzický server	HP	10
Fyzické síťové úložiště	HP, Synology	5
Virtualizační hypervizor	Hyper-V	2
Virtuální server	Win 2019 DataCenter	40
Virtuální server	Linux	10
Firewall	FortiGate	2
Krajní switch	HPE	6
Switch	Aruba	40
Přístupový bod Wi-Fi	Ubiquiti: UniFi	10
Koncová stanice	HP, DELL	550
Síťové reprografické zařízení	CANON, BROTHER, RICOH	50

Výčet provozovaných informačních systémů (předpokládané napojení na log management)

Informační systém	**Výrobce / technologie / OS**	**Přibližný počet uživatelů**
NIS – část AKORD	STAPRO / SQL / WIN	600
NIS – část ENTERPRISE	STAPRO / SQL / WIN	300
NIS – část laboratoře	STAPRO / SQL / WIN	5
NIS – část lékárna	STAPRO / SQL / WIN	5
NIS – část PACS	OR-CZ / SQL / LINUX	4
Helios	ASSECO / SQL / WIN	40
Spisovka	SEYFOR / SQL / LINUX	200
ELDAX	SEYFOR / SQL / WIN	10
Stravovák	VIS / SQL / WIN	10
EISOD, DMS	MYCOM / SQL / WIN	200
Ambulantní IS Medicus	COMPUGROUP MEDICAL / FIREBIRD / WIN	8
Attendo – docházka	RSM / FIREBIRD / WIN	600
Avensio – mzdy	RSM / FIREBIRD / WIN	15
Envita – odpadové hospodářství	INISOFT / SQL / WIN	2

2 Požadavky na dodávané plnění (služby)

Informace k hodnocení nabídek a podobě zpracování nabídky

Potencionální dodavatel ve své nabídce popíše řešení dodávané služby tak, aby mohl zadavatel při hodnocení z předložené nabídky vyhodnotit, zda nabízené řešení plní předepsaný požadavek. Hodnocení je možné jen ve škále plní / neplní.

Dodávané řešení musí splnit všechny předepsané požadavky definované v kapitole 2 tohoto dokumentu. Variantní řešení nabídky není přípustné.

Do sloupce „Způsob naplnění“ uvede potencionální dodavatel stručný popis způsobu naplnění požadavku zadavatele i s případným odkazem na přílohy své nabídky, které popis způsobu naplnění vhodně doplňují nebo ilustrují. Odkaz musí být přesný, tedy např. na konkrétní kapitolu, paragraf nebo obrázek. Předkládané informace musí být jasně formulované a nebýt vzájemně v rozporu. Platí požadavek, že zadavatel musí být schopen při hodnocení z předložené nabídky vyhodnotit, zda nabízené řešení plní předepsaný požadavek. Hodnocení je možné jen ve škále plní / neplní. Předkládané dokumenty budou zpracované v českém jazyce. Originály produktových listů a dalších materiálů přímo převzatých od výrobců dílčích řešení mohou být zpracovány v anglickém jazyce, mohou však sloužit jen jako podpůrné a ilustrační.

2.1 Funkční požadavky na dodávané plnění

Označení	Požadavek zadavatele	Způsob naplnění
2.1 A	Nabízené řešení je komplexní, tedy zahrnuje v sobě jak technologickou část, tak navázané procesy pro sledování, vyhodnocování a interpretaci provozu a událostí v oblasti bezpečnosti. Řešení je designováno jako dostatečné kapacitní (výkonově, personálně) tak, aby byly splněny SLA požadavky definované v tomto dokumentu.	Ano, nabízené řešení je komplexní a zahrnuje jak pokročilé technologické komponenty, tak i integrované procesy pro sledování, vyhodnocování a interpretaci provozu a bezpečnostních událostí. Implementujeme moderní monitorovací nástroje spojené s automatizovanými systémy pro analýzu dat, což umožňuje rychlou detekci a reakci na potenciální hrozby. Řešení je navrženo s dostatečnou kapacitou jak po výkonové stránce, tak i personálním zajištěním, aby byly splněny veškeré definované SLA požadavky.
2.1 B	Nabízené řešení obsahuje tyto technologie: VM, EDR, NDR, LM, SIEM, Security Ticketing, Security Dashboard a SOAR.	Ano, součástí nabízeného řešení jsou všechny požadované technologie včetně VM, EDR, NDR,

		LM, SIEM, Security Ticketing, Security Dashboard a SOAR, popsány v kapitole 1.2.2 nabídky.
2.1 C	Nabízené řešení SOC bude poskytované jako externí outsourcovaná služba. Tedy všechny technologie budou provozované v prostředí dodavatele. Výjimkou jsou klienti a HW/SW sondy potřebné pro sběr dat nebo ochranu prostředí zadavatele. Výpočetní a interpretační část SOC je tedy na straně dodavatele a zadavatel nebude poskytovat na své infrastruktuře výpočetní výkon ani úložnou kapacitu pro potřeby SOC.	Ano, nabízené SOC řešení je poskytováno jako externí outsourcovaná služba. Veškerý hardware a software potřebný pro provoz služby, včetně SOC sondy, je součástí naší nabídky a je zahrnut v dodávaných službách.
2.1 D	Všechna data budou přenášena do externí infrastruktury dodavatele výhradně v zabezpečené zašifrované formě a musí být chráněna vůči neoprávněným změnám. Použité šifrovací algoritmy a technologie musí být v souladu s požadavky dokumentu „Minimální požadavky na kryptografické algoritmy“ zveřejněném na webu Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB).	Ano, veškerá data přenášena do naší externí infrastruktury budou výhradně v zabezpečené a zašifrované formě a budou chráněna proti neoprávněným změnám. Používáme šifrovací algoritmy AES a ChaCha20 v souladu s požadavky dokumentu „Minimální požadavky na kryptografické algoritmy“ zveřejněného na webu Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB)
2.1 E	Dodavatel se zavazuje v případě vyžádání poskytnout součinnost se zadavatelem při provádění analýzy rizik ICT aktiv, na které je v infrastruktuře zadavatele napojen. Tyto činnosti mohou být čerpány z hodinového rozpočtu určeného na konzultace.	Ano, zavazujeme se, že v případě vyžádání poskytneme součinnost při provádění analýzy rizik ICT aktiv. Tyto činnosti mohou být čerpány z hodinového rozpočtu určeného na konzultace.
2.1 F	Všechny aktivity specialistů SOC jsou auditované na úrovni detailních aktivit (pohyby myší, práce s klávesnicí, obsah obrazovky), které vůči zadavateli vykonávají. Daný nástroj na zajištěni této auditní stopy je součástí technického řešení dodavatele.	Ano, všechny aktivity, které provádějí naši SOC specialisté vůči zadavateli jsou detailně auditovány a nástroj pro zajištění této auditní stopy je součástí našeho technického řešení.
2.1 G	Dodávané řešení bude schopné monitorovat, analyzovat a vyhodnocovat bezpečnostní události, hrozby, útoky a anomálie na základě NetFlow, pomoci přímého monitoringu v reálném čase, a to i na aplikační vrstvě ISO/OSI, resp. TCP/IP. Technologicky řešení monitoringu NetFlow zajistí dodavatel.	Ano, součást nabízeného řešení je technologie Flowmon NDR s rozšířením ADS zahrnující také požadované monitorovací a detekční schopnosti na základě NetFlow v reálném čase a na aplikační vrstvě ISO/OSI modelu.

2.1 H	Dodavatel zajistí také kapacitu pro konzultace speciality certifikovaného na technologie zmíněné v bodě 2.1 B.	Ano, máme zajištěnu kapacitu certifikovaných specialistů jak prostřednictvím našich interních zdrojů v rámci SOITRON Group, tak i díky firemním partnerstvím u distributorů a výrobců příslušných technologií.
2.1 I	Nabízené řešení musí umět identifikovat zero-day útoky (např. na základě behaviorální analýzy).	Ano, nabízené řešení obsahuje komponenty behaviorální analýzy (Behavioral AI Engine jako součást SentinelOne EDR a také Flowmon ADS)
2.1 J	Nabízené řešení musí umožňovat automatické korelování událostí z více zdrojů, vyhodnocení incidentů a následné generovaní alertů, a to všechno v reálném čase.	Ano, nabízené řešení obsahuje technologickou platformu Wazuh SIEM která umožňuje automatické korelování událostí z více zdrojů, vyhodnocení incidentů a následné generovaní alertů, a to všechno v reálném čase.
2.1 K	Nabízené řešení musí primárně využívat bez-agentový sběr logů. Ten typ sběru je preferovaný. Instalace agenta bude umožněna jen v odůvodněných případech Např. pokud není technologicky možné zajistit sběr logů jiným způsobem.	Ano, nabízené řešení nabízí primárně bez-agentový sběr bezpečnostních událostí prostřednictvím NDR, či přímo ze zařízení protokoly Syslog a pod. Výjimkou, kde se s instalací agentských komponent počítá je řešení EDR.
2.1 L	Databáze musí být zabezpečená proti manipulaci, tak aby nebylo možné narušit integritu uložených záznamů.	Ano, používaná databáze je zabezpečena proti manipulaci tak, aby nebylo možné narušit integritu uložených záznamů. Toho dosahujeme implementací kryptografických technik, které zajišťují neměnnost záznamů. Přístup k databázi je omezen prostřednictvím autentizace a striktních přístupových práv. Všechny operace s daty jsou auditovány a zaznamenávány pro účely sledování a detekce neoprávněných aktivit. Navíc využíváme technologie jako je redundance a pravidelné zálohování, aby byla data chráněna i proti ztrátě či poškození.
2.1 M	Nabízené řešení bude podporovat napojení různých zdrojů obohacujících informací (DNS, IDM, LDAP, ap.).	Ano, nabízené řešení plně podporuje napojení na různé zdroje obohacujících informací, jako jsou DNS, IDM, LDAP a mnohá další.

2.1 N	Nabízené řešení nesmí způsobit omezení funkcionality, kvality a narušení bezpečnosti jiných zařízení / systémů v síti.	Ano, nabízené řešení je navrženo tak, aby neomezovalo funkcionalitu ani kvalitu ostatních zařízení či systémů ve vaší síti a nenarušovalo jejich bezpečnost. Používáme neinvazivní technologie a standardizované protokoly neovlivňující stávající infrastrukturu.
2.1 O	Nabízené řešení SOC využívá SOAR techniky a procesy pro orchestraci a zrychlení threat detection a incident response.	Ano, nabízené řešení a související SOC služby využívají SOAR techniky a procesy.
2.1 P	Služba SOC musí obsahovat funkcionalitu THREATS EXCHANGE, minimálně na úrovni MISP.	Ano, nabízená služba SOC provozuje a obsahuje také funkcionalitu „Threats Exchange“ formou MISP.

2.2 Kapacitní požadavky na dodávané plnění

Označení	**Požadavek zadavatele**	**Způsob naplnění**
2.2 A	Technologický návrh nabízeného řešení musí být proveden tak, aby nabízené řešení umělo zpracovat i dočasně zvýšený přenos dat (peak) na síti bez jeho zahození nebo ignorováni. Kapacitní a výkonové požadavky potřebné pro splnění tohoto požadavku si dodavatel upřesní v rámci své úvodní implementační analýzy.	Ano, používáme škálovatelnou infrastrukturu s dostatečnou rezervou výkonu a kapacity, která umožňuje zpracovat i náhlé nárůsty síťového provozu.
2.2 B	Nabízené řešení musí umožňovat rozšíření výkonnosti anebo připojení dalších monitorovaných zdrojů jen licenčním vypořádáním (zajištění bezproblémové škálovatelnosti). Součástí nabídky je popis zajištění tohoto požadavku v nabízeném licenčním ekosystému tak, aby mohl zadavatel vyhodnotit jeho naplnění.	Ano, všechny nabízené nástroje a služby mají dostatečnou technologickou rezervu a nejsou na hranici svých možností. V případě budoucích potřeb je lze dále rozšířit pouze dodatečným licencováním.
2.2 C	Výkonový rozsah licence pro LM/SIEM je minimálně 600 EPS nebo 30 GB/den.	Ano, nabízený LM/SIEM je založen na technologickém řešení Wazuh a není licenčně omezen na EPS a GB/den.
2.2 D	Rozsah licence do EDR řešení je 540 ks licence pro koncové stanice a servery.	Ano, nabízené řešení obsahuje také licence SentinelOne EDR pro 540ks koncových stanic a serverů.

2.2 E	Rozsah licence pro VM řešení je 128 ks pro skenované assety.	Ano, nabízené řešení obsahuje také licenci Tenable Nessus Professional pro skenování minimálně 128 assetů.
2.2 F	Výkon sondy pro NDR řešení včetně analýzy anomálního chování v síti je 1 ks sondy a minimálně 2x 1 GBE monitorovací rozhraní.	Ano, součástí řešení je sonda NDR Flowmon s 2x 1GBE monitorovacími rozhraní.
2.2 G	Požadovaný čas ukládání dat pro ON-LINE vyhledávaní je minimálně 200 dní.	Ano, požadovaný čas ukládání dat pro ON-LINE vyhledávaní je více než 200 dní.
2.2 H	Požadovaný čas ukládaní dat pro OFF-LINE archiv je minimálně dalších 400 dní.	Ano, požadovaný čas ukládání dat pro OFF-LINE vyhledávaní je více než 400 dní.

2.3 Požadavky na organizační zajištění dodávaných služeb

2.3.1 Realizační tým

Označení	**Požadavek zadavatele**	**Způsob naplnění**
2.3.1 A	Za stranu dodavatele bude definována osoba odpovědná za zakázku (vedoucí realizačního týmu, projektový manažer) mající povědomí o parametrech dodávaných služeb a prostředí dodavatele. Tato osoba bude zajišťovat komunikaci se zástupci zadavatele týkající se jejího dalšího rozvoje nebo změn a účastnit se také pravidelných schůzek dle bodu 2.5 A.	Ano, za naší stranu bude v rámci projektu definován celý realizační tým, včetně projektového manažera odpovědného za zakázku včetně komnikacie týkající se dalšího rozvoje, změn i pravidelních schůzek.
2.3.1 B	Součástí dodávaného plnění je i zajištění potřebných kapacit specialistů bezpečnostního monitoringu ve třech úrovních (L1, L2, L3). Dodavatel ve své nabídce popíše, jak je tato dostupnost zajištěna i s přesahem na požadovanou úroveň služeb.	Ano, disponujeme dostatečnými personálními kapacitami, a jsme schopni poskytovat veškeré odborné i organizační činnosti zmiňované v naší nabídce.
2.3.1 C	Zadavatel požaduje sestavení kvalifikovaného realizačního týmu pro zajištění poptávaného řešení. Zadavatel ve své nabídce popíše realizační tým a doloží požadované kompetence a praxi na jednotlivé pozice definované v bodech 2.3.1 D až 2.3.1. J potřebnými dokumenty – životopisy a certifikáty.	Ano, součástí realizačního týmu jsou specialisté s požadovanými kompetenci, blíže popsanými v přiložených CV a certifikátech.
2.3.1 D	**POZICE Architekt** • Praxe v oboru kybernetické bezpečnosti minimálně 5 let	Štefan Porubčan, viz. přiložené CV a certifikáty

	• Zkušenosti s realizací alespoň 2 zakázek obdobného charakteru splňující významné zakázky • Je držitelem certifikátu architekta – TOGAF® Enterprise Architecture Foundation a vyšší, ITIL Foundation a vyšší, Architekt KB dle ZoKB	
2.3.1 E	**POZICE Vedoucí realizačního týmu – Projektový manažer** • Praxe v oboru kybernetické bezpečnosti minimálně 5 let • Zkušenosti s vedením alespoň 3 zakázek obdobného charakteru, jejichž předmětem zahrnoval nebo zahrnuje dodávku, implementaci, podporu a napojení do SOC • Je držitelem certifikátu z oblasti projektového řízení – např. Prince2 Foundation a vyšší, IPMA nebo obdobný	Ján Prostredný, viz. přiložené CV a certifikáty
2.3.1 F	**POZICE Auditor** • Praxe v oboru kybernetické bezpečnosti minimálně 5 let • Zkušenosti s realizací alespoň 1 zakázky obdobného charakteru, jejíž předmět zahrnoval nebo zahrnuje organizační opatření a plán kontinuity	Štefan Porubčan, Juraj Richtárik, viz. přiložená CV a certifikáty
2.3.1 G	**POZICE Technický specialista NetFlow** • Praxe v oboru ICT minimálně 5 let • Zkušenosti s realizací alespoň 1 zakázky obdobného charakteru, jejíž předmět zahrnoval nebo zahrnuje analýzu datových toků v síti na základě monitoringu založeném na analýze NetFlow/IPFIX či obdobné • Je držitelem certifikátu na nabízené technologie, a to minimálně v rozsahu certifikace pro techniky, ne obchodní	Matěj Pilko, Martin Vozár, viz. přiložená CV a certifikáty
2.3.1 H	**POZICE Technický specialista Administrace** • Praxe v oboru ICT minimálně 5 let • Zkušenosti s realizací alespoň 1 zakázky obdobného charakteru, jejíž předmět zahrnoval nebo zahrnuje správu a management zranitelnosti • Je držitelem certifikátu na nabízené technologie, a to minimálně v rozsahu certifikace pro techniky, ne obchodní	Vladimír Ruttkay, Marek Kozel, viz. přiložená CV a certifikáty

2.3.1 I	**POZICE Technický specialista Log management** • Praxe v oboru ICT minimálně 5 let • Zkušenosti s realizací alespoň 1 zakázky obdobného charakteru, jejíž předmět zahrnoval nebo zahrnuje Log Management a SIEM • Je držitelem certifikátu na nabízené technologie, a to minimálně v rozsahu certifikace pro techniky, ne obchodní	Vladimír Ruttkay, Marek Kozel, viz. přiložená CV a certifikáty
2.3.1 J	**POZICE Technický specialista EDR** • Praxe v oboru ICT minimálně 5 let • Zkušenosti s realizací alespoň 1 zakázky obdobného charakteru, jejíž předmět zahrnoval nebo zahrnuje EDR včetně počtu koncových bodů a finanční hodnoty • Je držitelem certifikátu na nabízené technologie, a to minimálně v rozsahu certifikace pro techniky, ne obchodní	Martin Lohnert, viz. přiložené CV a certifikáty

2.3.2 Fáze implementace SOC

Označení	**Požadavek zadavatele**	**Způsob naplnění**
2.3.2 A	Součástí implementace řešení bude zpracování implementační analýzy. Ta bude zpřesňovat technické zajištění a podobu implementace nabízeného řešení v infrastruktuře zadavatele – PNvD.	Ano, řešení obsahuje fázi implementační analýzy popsanou v části 2.1.1 nabídky.
2.3.2 B	Implementační analýza bude popisovat jak počty a účel instalovaných zařízení v infrastruktuře PNvD, tak nastavení procesů s přesahem do SOC na infrastruktuře dodavatele.	Ano, řešení obsahuje fázi implementační analýzy popsanou v části 2.1.1 nabídky.
2.3.2 C	Součástí implementační analýzy budou i odkazy na pracovní postupy (návody, manuály) pro pracovníky PNvD popisující jejich zapojení v řešení SOC.	Ano, řešení obsahuje fázi implementační analýzy popsanou v části 2.1.1 nabídky.
2.3.2 D	Dodavatel se zavazuje spolupracovat v začlenění procesů SOC do businness continuity managementu zadavatele – primárně poskytováním konzultací.	Ano, zavazujeme se spolupracovat v začlenění procesů SOC do business continuity managementu zadavatele – primárně poskytováním konzultací.

2.3.2 E	Implementační analýza podléhá připomínkování a schválení zadavatele. Samotná realizace řešení je možná až po schválení implementační analýzy.	Ano, nabízené řešení počítá se zahájením samotné implementace až schválení implementační analýzy.

2.3.3 Fáze provozu SOC

Označení	Požadavek zadavatele	Způsob naplnění
2.3.3 A	Určení pracovníci zadavatele mají přístup do specializovaného portálu dle bodu 2.5 A až 2.5 D.	Ano, nabízené řešení počítá s přístupem pro autorizované uživatele PNvD
2.3.3 B	Dodavatel se zavazuje spolupracovat v začlenění procesů SOC do business continuity managementu zadavatele – primárně poskytováním konzultací. Kapacity pro tyto konzultace budou zadavateli poskytnuty bezodkladně, zahájení konzultací maximálně do 5 pracovních dní od zadání požadavku.	Ano, zavazujeme se spolupracovat na začlenění procesů SOC do business continuity managementu, primárně prostřednictvím poskytování konzultací. Kapacity pro tyto konzultace vám budou poskytnuty bezodkladně, se zahájením konzultací maximálně do 5 pracovních dní od zadání požadavku.
2.3.3 C	Poskytované konzultace nad rámec smluvených služeb SOC jsou poskytnuty na vyžádání oprávněného zástupce zadavatele a jsou účtovány na základě smluveného rámce hodin pro konzultace. Na vyžádání zadavatele je možné provést dokladování stavu a průběhu řešení požadavku na straně dodavatele – optimálně formou tiketu.	Ano, počítáme s poskytováním konzultací nad rámec smluvených služeb SOC na vyžádání oprávněného zástupce zadavatele, které budou účtovány na základě smluveného rámce hodin pro konzultace. Počítáme také s jejich evidováním a dokladováním v ticketing nástroji.

2.4 Požadavky na dostupnost a úroveň služeb

Označení	Požadavek zadavatele	Způsob naplnění
2.4 A	Aktivní dohled SOC (přítomnost operátorů provádějících L1 triáž a L2 analytika) je zajišťován minimálně v režimu 8x5 dle stanovených SLA parametrů pro řešení bezpečnostních incidentů. Dostupnost automatizovaných detekčních a dohledových nástrojů je zajišťována v režimu 24x7x365.	Ano, aktivní dohled s trvalou přítomností operátorů v SOCu bude zajišťován v režimu 8x5 dle stanovených SLA parametru. Dostupnost automatizovaných detekčních a

		dohledových nástrojů je zajišťována v režimu 24x7x365.
2.4 B	Je požadovaná vysoká dostupnost technologického řešení SOC. V úrovni dostupnosti provozovaného SW (počet instancí, redundance) je designovaná dostupnost 99,9 % (zadavatel nepožaduje pravidelné vyhodnocování reálných úrovní dostupnosti v rámci reportingu). Technologická úroveň datového centra, kde běží technologie SOC, by měla být minimálně v technologickém standardu TIER II (certifikovaný), lépe TIER III (bez certifikátu). Dodavatel v nabídce popíše, jak je technologicky zajištěno splnění výše zmíněných požadavků na dostupnost.	Ano, technologické řešení SOC je designováno s vysokou úrovní dostupnosti na úrovni min. 99,9% Technologická úroveň datového centra, kde běží technologie SOC, je dle standardu Uptime Institute TIER III (bez certifikace) a je také certifikováno NATO na úroveň „Confidential“
2.4 C	V rámci zajištění business continuity managementu zadavatele se zástupci dodavatele podílejí i na práci lokálního CSIRT (Computer Security Incident Response Team). Dodavatel bude službu CSIRT organizačně a technicky zastřešovat a proces spustí na základě požadavku zadavatele. Tyto služby jsou dodávány v rámci poskytovaného měsíčního paušálu.	Ano, v rámci měsíčního paušálu počítáme s participací na práci lokálního CSIRT, dle odsouhlasené strategie procesní integrace jenž je součástí úvodní implementační analýzy.
2.4 D	CSIRT na straně dodavatele je certifikovaný minimálně na stupeň "Accredited" dle mezinárodně uznávané autority Trusted Introducer.	Ano, jsme členy organizace TF-CSIRT Trusted Introducer na úrovni „Accredited“ a zároveň také plnohodnotnými členy organizace FIRST - Forum of Incident Response and Security Teams
2.4 E	**Požadavky na designovanou úroveň poskytovaných služeb** • Log Management: v režimu 24/7 nástroj zpracovává logy ze všech připojených zdrojů, provádí normalizaci a poskytuje zdrojové informace pro SIEM. • Real-time SIEM: v režimu 24/7 nástroj přebírá data z Log Management, vyhodnocuje události ze všech připojených zdrojů a generuje hlášení incidentů. • Non-Real-time SIEM: v režimu 8x5 nástroj přebírá data z Real-time SIEM i Log Management, vyhodnocuje všechny zpracované	Ano, nabízené řešení reflektuje požadované úrovně služeb a počítá s jejich provozovaním v režimu 24/7, s výjimkou Non-Real-time SIEM v režimu 8x5.

	událostí, zaměřuje se primárně na analytiku a vyhodnocování velkých objemů dat s cílem identifikovat trendy a odchylky, provádět behaviorální a forenzní analýzy a následný reporting. • SOAR: v režimu 24/7 provádí orchestraci událostí nad SIEM a dle stanovených pravidel automatizaci procesů spojených s hlášením bezpečnostních událostí a identifikovaných incidentů. • EDR: v režimu 24/7 provdání analýzu a detekci stavu bezpečnosti na koncových stanicích a serverech a předává detekce směrem do SIEM. • NDR: v režimu 24/7 provdání analýzu a detekci stavu bezpečnosti na síti a předává detekce směrem do SIEM. • VM: provdání pravidelné skeny zranitelností a obohacuje těmito informacemi data z výše vypsaných technologií.	

2.4 F	**Smluvní požadavky na úroveň služby (SLA parametry)**
	Níže definované požadavky budou pravidelně ze strany dodavatele vyhodnocovány a data o jejich plnění budou k dispozici (formou reportu nebo v online dashboardu) oprávněným zástupcům zadavatele.
	Nedodržení těchto nastavených parametrů SLA může mít za následek smluvní pokuty.
	Reakce na zjištěnou kybernetickou bezpečnostní událost v režimu aktivního dohledu, dle kategorizace očekávaného kybernetického bezpečnostního incidentu
	• Kategorie I
	  ○ Hlášení o potencionálním incidentu: do 2 hodin
	  ○ Výsledky úvodní analýzy: do 4 hodin
	• Kategorie II
		Ano, naše nabízené řešení reflektuje požadované parametry úrovně služby SLA a počítá s jejich garantováním včetně smluvních pokut.

	○ Hlášení o potencionálním incidentu: do 4 hodin ○ Výsledky úvodní analýzy: do 6 hodin • Kategorie III ○ Výsledky úvodní analýzy: do konce následujícího pracovního dne ***VYSVĚTLIVKY KE KATEGORIZACI POTENCIONÁLNÍCH KYBERNETICKÝCH BEZPEČNOSTNÍCH INCIDENTŮ (v souladu s vyhláškou č.82/2018 Sb.)*** • *Kategorie I: velmi závažné narušení bezpečnosti, které významně a přímo ohrožuje bezpečnost dat nebo poskytovaných služeb a vyžaduje neprodlený zásah odpovědných osob daného systému, pro rozšíření a minimalizaci škod, hlášení NÚKIB.* • *Kategorie II: závažné narušení bezpečnosti poskytovaných služeb nebo dat a vyžadující neprodlený zásah odpovědných osob.* • *Kategorie III: méně závažné narušení bezpečnosti poskytovaných služeb nebo dat, které nevyžaduje okamžitý zásah odpovědných osob.* ***VYSVĚTLIVKY KE SLEDOVANÝM AKTIVITÁM DODAVATELE*** • *Hlášení o potenciálním incidentu – jednoduché oznámení o podezření na incident, základní informace o zasaženém aktivu (monitorovaném zdroji Objednatele)* • *Výsledky úvodní analýzy – aktuální informace o rozsahu incidentu, specifikace zasažených aktiv, potenciálních příčin a dopadů, indikace způsobu řešení, návrh opatření k okamžité ochraně aktiv*	

2.5 Požadavky na reporting

Označení	Požadavek zadavatele	Způsob naplnění
2.5 A	V rámci realizace dodávek budou konány pravidelné schůzky (status meetingy) zpravidla v měsíční periodě.	Ano, V průběhu realizace produkčního provozu SOC služeb budou konány pravidelné schůzky

		(status meetingy), zpravidla s měsíční periodicitou. V průběhu implementace jsou schůzky konány častěji – každý týden.
2.5 B	Součástí SOC je specializovaný portál, kde jsou dostupné potřebné informace na jednom místě v přehledné podobě dashboardu. Tento portál poskytuje dashboardy na míru (možnost konfigurace specialisty dodavatele), kde je možné zobrazit dynamicky aktuální informace ze všech komponent SOC.	Ano, součásti dodávaného řešení je také informační dashboard přístupný pro autorizované uživatele, zobrazující požadované informace. Dashboard je konfigurovatelný správci systému dle požadavek „na míru.“
2.5 C	Dodavatel bude poskytovat zadavateli výstupy (formou reportů nebo dashboardů na portále) poskytující přehled o plnění sledovaných indikátorů nastavených v rámci požadavků na dostupnost a úroveň služeb. Přesná definice sledovaných indikátorů a forma jejich reportingu je definována v implementační analýze.	Ano, nabízené řešení zahrnuje poskytování pravidelně generovaných reportů ve formátu PDF, obsahujících přehled plnění definovaných indikátorů dostupnosti a úrovně služeb.
2.5 D	Řešení je postavené jako otevřené pro zadavatele. Tedy zadavatel má přístup k informacím ve všech částech nebo technologiích minimálně v rozsahu **jen pro čtení**. Přidělení případných vyšších přístupů zástupcům zadavatele může být dohodnuto v rámci fáze implementace a být popsáno v rámci úvodní implementační analýzy.	Ano, pro zadavatelem autorizované uživatele je k dispozici „read-only“ přístup do všech technologických komponent/částí nabízeného řešení. Případné vyšší úrovně přístupů můžou vycházet se schválených výstupů úvodní analýzy.
2.5 E	Součástí dodávaného řešení SOC je tvorba knowledge base a tvorba RUNBOOKS pro efektivní řešeni bezpečnostních událostí.	Ano, součástí dodávaného řešení je tvorba knowledge base a tvorba RUNBOOKS pro efektivní řešeni bezpečnostních událostí.
2.5 F	Nabízené řešení bude podporovat možnosti vícenásobné notifikace jednoho alertu.	Ano, nabízené řešení podporuje nastavení vícenásobné notifikace jednoho alertu.
2.5 G	Nabízené řešení musí podporovat filtraci a agregaci už na úrovni sběru logů v prostředí zadavatele.	Ano, nabízené řešení podporuje filtraci a agregaci událostí přímo v prostředí zadavatele, a to na několika úrovních (v detekčních nástrojech i LM platformě)
2.5 H	Nabízené řešení bude schopné zaznamenávat a vyhodnocovat minimálně následující detaily bezpečnostních událostí: typ nebo akce, datum a čas, ID systému, který událost zaznamenal, ID systému, kde k události došlo a ID uživatele nebo systému, který akci vyvolal.	Ano, nabízené řešení je schopno zaznamenávat a vyhodnocovat širokou škálu detailů bezpečnostních událostí, včetně všech jmenovaných

2.5 I	Nabízené řešení na úrovni Alertingu poskytuje referenci k technikám popsaným v knowledge base MITRE ATT&CK.	Ano, nabízené řešení na úrovni generovaných notifikací poskytuje reference taktik, technik a procedur dle MITRE ATT&CK knowledge base.
2.5 J	Poskytovatel služeb SOC musí nabízet RestAPI (nebo podobné API) rozhraní pro výměnu informací o svých aktivitách, minimálně na úrovni ticketing nástroje.	Ano, nabízené Security Ticketing řešení je dostupné k integraci prostřednictvím popsaného REST/JSON API. Další API integrační rozhraní jsou k dispozici na úrovni jednotlivých komponentů řešení.

2.6 Požadavky na plnění legislativy

Označení	**Požadavek zadavatele**	**Způsob naplnění**
2.6 A	Zadavatel (PNvD) bude dle návrhu nového zákona o kybernetické bezpečnosti a směrnice NIS 2 spadat pod účinnost regulace jako povinný subjekt s vyšším režimem povinností. Nabízené řešení i samotný dodavatel tedy musí podporovat požadavky na zajištění bezpečnosti dodavatelů dle této legislativy, resp. aktuálně platné legislativy.	Ano, nabízené řešení i naše společnost plně podporují požadavky na zajištění bezpečnosti dodavatelů dle platné legislativy a jsme připraveni je plnit také po transpozici NIS2 do nové verzi legislativy.
2.6 B	Dodavatel se podáním nabídky a uzavřením smlouvy zavazuje, že bude spolupracovat na pravidelném hodnocení dodavatelů z pohledu bezpečnosti dodavatelského řetězce dle legislativních požadavků.	Ano, zavazujeme se ke spolupráci na pravidelném hodnocení dodavatelů z pohledu bezpečnosti dodavatelského řetězce dle legislativních požadavků.
2.6 C	Obchodní společnost dodavatele provozuje certifikovaný systém managementu bezpečnosti informací (ISMS) dle mezinárodní normy ISO/IEC 27001. Certifikát bude platný po celou dobu poskytování plnění.	Ano, naše společnost provozuje certifikovaný systém managementu bezpečnosti informací (ISMS) dle mezinárodní normy ISO/IEC 27001 a zavazujeme se jej udržovat platný po celou dobu poskytování plnění.