číslo spisu NK ČR: 72/2026
ev. č. N006/26/V00002840/004
číslo smlouvy NK ČR: S0140/2026

# SMLOUVA O DODÁVCE A IMPLEMENTACI SYSTÉMU PRO SBĚR A KORELACI BEZPEČNOSTNÍCH UDÁLOSTÍ (SIEM) A POSKYTOVÁNÍ SLUŽEB PODPORY

Níže uvedeného dne, měsíce a roku smluvní strany:

**Národní knihovna České republiky**
státní příspěvková organizace zřízená Ministerstvem kultury ČR
se sídlem: Mariánské náměstí 190/5, 110 00, Praha 1
zastoupená: Ing. Václav Šubrta, LL.M., náměstek sekce Digitalizace a technologie NK ČR
IČO: 00023221
DIČ: CZ00023221
bankovní spojení: Česká národní banka
číslo účtu: 85535011/0710
(dále jako „**objednatel**“ nebo „**NK ČR**“)

a

**Netlancers s.r.o.**
se sídlem: Revoluční 1836/18, Litoměřice, 412 01
zapsaná v obchodním rejstříku: vedeného Krajským soudem v Ústí n./L., oddíl C, vložka 27938
IČO: 28926269
DIČ: CZ28926269
bankovní spojení: FIO banka, a.s.
číslo účtu: 2900922018 / 2010
jednající: Ing. Martin Macek, jednatel
(dále jako **„dodavatel“**)

(objednatel a dodavatel dále společně též jako „**smluvní strany**“)

uzavřely v souladu s ust. § 1746 odst. 2 ve spojení s ust. § 2586 a násl. zákona č. 89/2012 Sb., občanského zákoníku, ve znění pozdějších předpisů (dále jen „občanský zákoník“), tuto smlouvu na služby (dále jen „smlouva“)

## I. Úvodní ustanovení

1. Podkladem k uzavření této smlouvy je nabídka dodavatele, která byla objednatelem vybrána jako nejvýhodnější nabídka v zadávacím řízení č. N006/26/V00002840/004 na veřejnou zakázku zadanou v otevřeném nadlimitním řízení dle zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „ZZVZ") na služby s názvem **„Dodávka produktu pro sběr a korelaci bezpečnostních událostí - SIEM"** (dále také jen „**veřejná zakázka**").

2. Součástí smluvního ujednání je zadávací dokumentace veřejné zakázky.

3. Dodavatel prohlašuje, že na základě svých podnikatelských a živnostenských oprávnění je oprávněn a schopen poskytnout smluvené plnění řádně a kvalitně dle požadavků této smlouvy. Dodavatel prohlašuje, že není v insolvenci, ani že proti němu není vedeno nalézací, insolvenční či jiné soudní nebo správní řízení, které by bylo způsobilé zpochybnit platnost či účinnost této smlouvy nebo které by se mohlo dotýkat předmětu převodu a práv a povinností z této smlouvy vyplývajících. Dodavatel podle svého nejlepšího vědomí prohlašuje, že k datu uzavření této smlouvy má jako daňový poplatník vyrovnány veškeré své finanční závazky z titulu daňových, odvodových a jiných obdobných finančních povinností vyplývajících z obecně závazných právních předpisů a rozhodnutí příslušného správce daní či poplatků a orgánů vykonávajících správu ve věcech sociálního a zdravotního pojištění.

4. Dodavatel prohlašuje, že měl před podáním své nabídky k dispozici požadavky objednatele na rozsah plnění dle této smlouvy, a to jako součást zadávací dokumentace. Dodavatel tyto požadavky před podáním své nabídky s vynaložením odborné péče přezkoumal a na základě toho prohlašuje, že je schopen předmět plnění této smlouvy splnit. Dodavatel potvrzuje, že měl v případě jakýchkoliv nejasností možnost požádat o vysvětlení zadávací dokumentace.

5. Objednatel prohlašuje, že je oprávněn tuto smlouvu uzavřít a je schopen řádně plnit závazky v ní obsažené.

6. Předmět plnění dle této smlouvy je realizován za finanční podpory EU, název projektu „ Zvýšení kybernetické bezpečnosti Národní knihovny ČR, reg. číslo CZ.31.2.0/0.0/0.0/23_094/0010319.

## II. Předmět smlouvy

1. Předmětem této smlouvy je závazek dodavatele dodat, implementovat a po dobu 5 let provozně podporovat systém pro sběr, normalizaci, korelaci a analýzu bezpečnostních událostí (Security Information and Event Management, dále jen „**SIEM systém**" nebo „**systém**"), a to v rozsahu a kvalitě dle technické specifikace, která tvoří přílohu č. 1 této smlouvy, a závazek objednatele zaplatit za toto plnění sjednanou cenu.

2. Předmět plnění tvoří čtyři vzájemně provázané části: (a) hardwarové komponenty, pokud jsou součástí nabídky dodavatele; (b) softwarové licence; (c) implementace a integrace se stávající infrastrukturou objednatel ho včetně zajištění školení ICT administrátorů objednatele v rozsahu nezbytném pro plné užití funkcí systému, a předání veškeré provozní dokumentace v českém nebo anglickém jazyce; (d) provozní podpora po dobu 5 let od akceptace.

3. Přesná technická konfigurace řešení je součástí nabídky dodavatele a tvoří nedílnou součást přílohy č. 1 této smlouvy. Dodavatel plně odpovídá za to, že zvolená architektura splní výkonnostní a funkční požadavky dle přílohy č. 1 po celou dobu trvání smlouvy.

4. Dodavatel je povinen zabezpečit vlastní dopravu plnění na místo plnění.

5. Dodavatel objednatele ujišťuje, že předmět plnění je bez vad.

6. Dodavatel se zavazuje, že předmět koupě bude bez právních vad. Dodavatel zaručuje objednateli, že ohledně předmětu koupě není veden žádný soudní spor.

7. Dodavatel v rámci implementace SIEM systému provede zejména následující:

- dodávku a instalaci SIEM systému v konfiguraci dle přílohy č. 1, včetně případných hardwarových komponent, jsou-li součástí nabídky dodavatele, na místě plnění dle čl. V odst. 1;Úvodní inicializaci, konfiguraci a integraci SIEM systému se stávající infrastrukturou objednatele v rozsahu dle přílohy č. 1,
- Ověření funkčnosti a splnění výkonnostních parametrů dle akceptačních testů,
- Školení ICT administrátorů objednatele v rozsahu stanoveném v příloze č. 1, zahrnující minimálně: správu a konfiguraci systému, správu uživatelských oprávnění a rolí, práci s korelačními pravidly a dashboardy, postup při hlášení a eskalaci incidentů a správu aktualizací systému;
- Ekologickou likvidaci obalového materiálu, je-li HW součástí dodávky;

10. Nedílnou součástí dodávky je dále:

- Licence k softwarovým částem SIEM systému dle čl. III této smlouvy;
- Provozní dokumentace k systému zahrnující minimálně: architektonickou dokumentaci, instalační a konfigurační příručku, administrátorskou příručku, popis všech integrací a jejich parametrů a postup zálohování a obnovy systému.
- Produktová dokumentace v rozsahu potřebném pro provoz a správu dodaných zařízení.

## III. Licence

1. Dodavatel poskytuje objednateli nevýlučnou, územně a časově neomezenou licenci k užití softwarových částí SIEM systému pro interní provozní potřeby objednatele.

2. Licence zahrnuje oprávnění provozovat systém na infrastruktuře objednatele v neomezeném počtu uživatelských přístupů v rámci jeho organizace, pořizovat záložní kopie pro účely obnovy po havárii a provádět konfigurační úpravy v rozsahu administrátorského rozhraní.

3. Licence neopravňuje objednatele k zpřístupnění systému třetím osobám mimo vlastní zaměstnance a smluvní zpracovatele, k dekompilaci nebo modifikaci zdrojového kódu nad rámec § 66 zákona č. 121/2000 Sb., ani k přeprodeje nebo dalšímu licencování.

4. Licence je nepřevoditelná bez souhlasu dodavatele.

5. Licence trvá nejméně 5 let od podpisu akceptačního protokolu, a to nezávisle na trvání provozní podpory dle čl. IV. Po tuto dobu nevzniká objednateli žádná povinnost platby za samotnou licenci nad rámec dle čl. VII. této smlouvy. Rozhodne-li se objednatel provozní podporu neobnovit nebo ji vypovědět, licence tím nezaniká a dodavatel není oprávněn funkčnost systému jakkoliv omezit.

6. Dodavatel prohlašuje, že je oprávněn licenci poskytnout, že užíváním systému objednatelem v rozsahu dle tohoto článku nejsou porušována práva třetích osob a že systém neobsahuje mechanismy umožňující vzdáleně omezit nebo ukončit jeho provoz bez souhlasu objednatele.

7. Dodavatel při akceptaci předá seznam open source komponent obsažených v SIEM systému včetně příslušných licencí. Dodavatel zajistí, že způsob využití open source komponent nezakládá objednateli žádné povinnosti vůči třetím osobám, zejména povinnost zveřejnit, zpřístupnit nebo distribuovat jakýkoliv vlastní software, data nebo konfigurace objednatele.

## IV. Zajištění podpory

1. Dodavatel se zavazuje zajistit podporu pro dodané zařízení, a to po dobu 5 let od podpisu akceptačního protokolu oběma stranami. Tato podpora musí pokrývat veškeré služby nutné pro zajištění plné funkčnosti dodaných hardware a instalovaných software, jejich aktualizaci a předplatné

pro všechny objednatelem požadované funkce (zejména aktualizace firmware, bezpečnostní záplaty, opravy, resp. výměny HW komponent, změny konfigurace, komunikaci s podporou výrobce). Přesný rozsah, parametry a podmínky podpory jsou stanoveny v příloze č. 2 (SLA), která je nedílnou součástí této smlouvy. Provozní podpora musí zahrnovat:

- Jednotné kontaktní místo (dále jen „JKM"): Dodavatel poskytuje JKM pro hlášení a řešení incidentů dle přílohy č. 2;
- Reaktivní řešení incidentů a vad dle kategorií a lhůt stanovených v příloze č. 2, přičemž smluvní strany se mohou v konkrétních odůvodněných případech dohodnout na lhůtě odlišné, a to prostřednictvím JMK nebo písemnou dohodou oprávněných osob;
- Aktualizaci softwaru, parserů, korelačních pravidel a bezpečnostních záplat po celou dobu podpory;
- Aktualizaci databází hrozeb po celou dobu podpory;
- Výměnu vadných HW komponent, jsou-li součástí dodávky, včetně náhradních dílů a dopravy;
- Centrálně spravované aktualizace bez nutnosti individuálního přístupu k jednotlivým komponentám;
- V případě aktualizace podmínek Podpory výrobce je dodavatel povinen poskytnout objednatel mu tyto aktualizované podmínky Podpory výrobce a nemusí být uzavřen dodatek smlouvy.

2. Dodavatel objednateli garantuje, že dodané zařízení bude od okamžiku akceptace a převzetí do konce doby provozní podpory splňovat výkonnostní a funkční parametry dle přílohy č. 1 a dosahovat garantované dostupnosti dle přílohy č. 2. Tato garance se vztahuje na softwarovou i příp. hardwarovou část systému a nezávisí na tom, zda dodavatel čerpá podporu od výrobce použitých komponent.

3. Dodavatel zajistí, aby po celou dobu podpory byla dostupná podpora výrobce pro klíčové komponenty systému. Ukončí-li výrobce podporu komponenty v průběhu doby podpory, je dodavatel povinen zajistit náhradní řešení zachovávající funkčnost a bezpečnost systému, a to bez navýšení ceny.

4. Podmínky provozní podpory lze měnit pouze písemným dodatkem ke smlouvě.

## V. Dodací lhůta, místo a způsob plnění

1. Místem plnění je sídlo objednatele na adrese Národní knihovna ČR, Mariánské náměstí 190/5, Praha 1 a Centrální depozitář v Hostivaři. Osoba oprávněná k převzetí plnění za objednatele: [redacted] e-mail: [redacted] nebo jím pověřená osoba.

2. Termín dodání předmětu plnění dle čl. II. této smlouvy je stanoven nejpozději do 20. 5. 2026. Podrobný harmonogram realizace jednotlivých kroků bude dohodnut a písemně potvrzen zástupci smluvních stran po nabytí účinnosti této smlouvy. Podpora bude poskytována po dobu uvedenou v této smlouvě.

3. Objednatel si vyhrazuje právo v nezbytném rozsahu prodloužit termín dodání předmětu plnění v případě mimořádných provozních situací, nehod, havárií, stávek, výluk, nepříznivých klimatických podmínek, krizových stavů, nepříznivých zásahů ze strany orgánů veřejné moci či jiných nepříznivých a nepředvídatelných situací, nezávislých na vůli objednatele. V tomto případě nevzniká dodavateli nárok na náhradu případných s tím souvisejících nákladů.

4. Dodavatel je povinen průběžně informovat objednatele o stavu rozpracovanosti a předávat mu informace o plnění předmětu této smlouvy, a to na kontrolních dnech, jejichž termíny určí objednatel, zpravidla s nejméně třídenním předstihem. Objednatel je oprávněn předkládat ke zjištěným

informacím své připomínky a návrhy řešení (dále jen „připomínky“). Dodavatel je povinen vynaložit maximální možné úsilí při zapracování těchto připomínek do řešení, případně objednateli řádně v písemné formě odůvodnit, proč nemohou být připomínky akceptovány.

5. Dodavatel odpovídá za to, že implementace SIEM systému nebude narušovat chod ostatní IT infrastruktury objednatele, mimo v harmonogramu dojednané odstávky. Konfigurace SIEM systému bude probíhat vždy v časech předem dohodnutých s objednatelem.

6. Závazek dodavatele dodat a implementovat SIEM systém bude splněn předáním a převzetím řádně dodaného plnění v odpovídající kvalitě objednatelem, včetně ověření funkčnosti akceptačním testem a prokázání technické kompatibility. Předání a převzetí plnění bude potvrzeno písemně podpisem akceptačního protokolu pověřenými zástupci smluvních stran. Součástí předávaného plnění bude veškerá dokumentace a doklady ke všem částem plnění, výrobkům a zařízením dodaných dodavatelem a dále protokol o proškolení příslušných pracovníků objednatele.

7. Dodavatel vyzve písemně objednatele k předání a převzetí plnění nejméně 3 pracovní dny předem, nebude-li dohodnuto jinak.

## VI. Exit strategie a přechodné období

1. Smluvní strany se zavazují spolupracovat při ukončení provozní podpory tak, aby byl zajištěn hladký přechod na nástupnický systém bez výpadku bezpečnostního monitoringu objednatele. Nejpozději 6 měsíců před uplynutím doby provozní podpory, nebo bezodkladně při předčasném ukončení smlouvy, smluvní strany dohodnou plán přechodu.

2. Dodavatel v rámci přechodu zajistí:
   - export všech logů uložených v systému v otevřeném formátu (JSON, CSV, CEF nebo Syslog) na úložiště objednatele do 30 dnů od výzvy;
   - export veškeré konfigurace systému v čitelné nebo přímo použitelné podobě, zahrnující korelační pravidla, parsery, dashboardy, nastavení RBAC, skupiny zařízení a integrační konektory a dalších konfiguračních prvků systému ve strojově čitelném formátu umožnujícím import do nástupnického systému do 30 dnů od výzvy;
   - technickou součinnost při migraci v rozsahu odpovídajícím potřebám objednatele, zejména konzultace s objednatelem a nástupním dodavatelem a ověření úplnosti exportovaných dat;

## VII. Cena a platební podmínky

1. Celková cena za dodávku a implementaci předmětu plnění včetně zajištění podpory na období 5 let činí 5 757 578,00,-,- Kč bez DPH. DPH bude účtována ve výši určené podle právních předpisů platných ke dni uskutečnění zdanitelného plnění. Cena plnění se skládá:

| Položka | Cena v Kč bez DPH | Jednotka | Cena za požadované jednotky v Kč bez DPH |
|---|---|---|---|
| **Cena za dodávku produktu pro sběr a korelaci bezpečnostních událostí - SIEM systém dle podrobné technické specifikace** | 4 257 578,00 Kč | **1** | 4 257 578,00 Kč |

| | | | |
|---|---|---|---|
| Cena za 1 rok podpory | 300 000,00 Kč | **5** | 1 500 000,00 Kč |
| **Celková cena v Kč bez DPH** | | | 5 757 578,00 Kč |
| **Celková cena v Kč včetně DPH** | | | 6 966 669,38 Kč |

2. Cena dle odst. 1 tohoto článku je konečná, nepřekročitelná, nejvýše přípustná a zahrnuje veškeré náklady a zisk dodavatele spojené s dodáním předmětu koupě.

3. Cenu za pořízení a implementaci SIEM systému dle odst. 1 tohoto článku je objednatel povinen zaplatit dodavateli bankovním převodem na bankovní účet dodavatele na základě řádně vystaveného daňového dokladu, který je dodavatel oprávněn vystavit nejdříve ke dni uskutečnění zdanitelného plnění, který je dnem podepsání předávacího protokolu podle čl. V. odst. 6 této smlouvy.

Cena za každý rok podpory dle odst. 1 tohoto článku bude objednatel hrazena ročně zpětně (na konci příslušného období) na základě řádně vystaveného daňového dokladu, který dodavatel vystaví nejdříve poslední den v měsíci, kterého se fakturace týká, a doručí ho objednateli vždy do 5. dne měsíce následujícího.

Splatnost daňového dokladu je 30 dnů ode dne jeho prokazatelného doručení objednateli na e-mailovou adresu objednatele [redacted] Okamžikem úhrady ceny se rozumí okamžik, v němž je cena odepsána z účtu objednatele ve prospěch účtu dodavatele.

4. Daňový doklad musí obsahovat číslo smlouvy dle číslování objednatele, systémové číslo NEN ve formátu N006/26/V00002840/004 registrační číslo projektu CZ.31.2.0/0.0/0.0/23_094/0010319, uvedení délky záruky, vyčíslení poplatku za následnou ekologickou likvidaci a musí splňovat náležitosti daňového a účetního dokladu podle zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů, zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů (dále jen „zákon o DPH“) a musí mít náležitosti obchodní listiny dle § 435 občanského zákoníku. V případě, že daňový doklad výše uvedené náležitosti nebude splňovat nebo bude obsahovat nesprávné údaje, vrátí objednatel daňový doklad do dne splatnosti daňového dokladu k opravení bez jeho proplacení. Lhůta splatnosti se v takovém případě dnem zpětného odeslání staví a poté počíná běžet znovu ode dne doručení opraveného či nově vyhotoveného daňového dokladu na e-mailovou adresu objednatele uvedenou výše.

5. Platby dle této smlouvy budou probíhat výhradně v Kč a rovněž veškeré cenové údaje budou v této měně.

6. Dodavatel prohlašuje, že na sebe přebírá nebezpečí změny okolností podle § 1765 odst. 2 občanského zákoníku, § 1765 odst. 1 a § 1766 občanského zákoníku se tedy ve vztahu k dodavateli nepoužije.

7. Objednatel neposkytuje zálohové platby.

8. Zveřejní-li správce daně skutečnost, že dodavatel je nespolehlivým plátcem ve smyslu zákona č. 235/2004 Sb., o dani z přidané hodnoty, je objednatel oprávněn z každé fakturované platby zadržet daň z přidané hodnoty a tuto, aniž by k tomu byl vyzván jako ručitel, uhradit za dodavatele příslušnému správci daně. Co do částky takto objednatelem uhrazené není objednatel v prodlení s úhradou ceny dle této smlouvy.

## VIII. Utvrzení a zajištění závazku

1. V případě prodlení dodavatele s odevzdáním kterékoliv části předmětu plnění oproti lhůtě sjednané v čl. V. odst. 2 této smlouvy je objednatel oprávněn požadovat po dodavateli úhradu smluvní pokuty ve výši 0,3 % z celkové ceny za každý i započatý den prodlení.

2. V případě prodlení dodavatele s odstraněním vady kterékoliv části SIEM systému je objednatel oprávněn požadovat po dodavateli úhradu smluvní pokuty ve výši 5.000,- Kč za každý i započatý den prodlení a za každý případ zvlášť.

3. V případě prodlení objednatele s úhradou daňového dokladu (faktury) je objednatel povinen uhradit dodavateli úrok z prodlení ve výši stanovené nařízením vlády č. 351/2013 Sb., ve znění pozdějších předpisů.

4. Sjednáním smluvní pokuty podle tohoto článku není dotčeno právo objednatele na náhradu škody vzniklé z porušení povinnosti utvrzované v odst. 1 tohoto článku, tzn., že smluvní strany se dohodly, že § 2050 občanského zákoníku se nepoužije.

5. Veškeré smluvní pokuty dle této smlouvy jsou splatné do 30 kalendářních dnů ode dne doručení výzvy k jejich zaplacení povinné smluvní straně.

6. Smluvní pokuty je objednatel oprávněn započíst ve smyslu ust. § 1982 a násl. občanského zákoníku proti i nesplatné pohledávce dodavatele na úhradu ceny.

## IX. Záruka (podpora), nároky z vadného plnění

1. Objednatel je oprávněn dle svého uvážení uplatnit vůči dodavateli tato práva z odpovědnosti za vady:

- právo na bezplatné odstranění vad,
- právo na přiměřenou slevu z ceny,
- právo na odstoupení od smlouvy, pokud vady či nedodělky jsou takového charakteru, že podstatně ztěžují či dokonce brání řádnému provozu, správě a užívání předmětu plnění. Za takové vady se považují i vady, které jsou opakovaného charakteru.

## X. Ochrana informací

1. Žádná ze smluvních stran není oprávněna poskytnout třetím osobám jakékoliv informace o plnění této smlouvy a související s touto smlouvou, jejichž obsahem mohou být důvěrné informace. Nedohodnou-li se smluvní strany výslovně písemnou formou jinak, považují se za důvěrné informace implicitně všechny informace, které jsou nebo by mohly být součástí obchodního tajemství, tj. například, ale nejenom osobní a citlivé údaje, technologie, popisy nebo části popisů technologických procesů a vzorců, technických vzorců a technických know-how, informace o provozních metodách, procedurách a strategie nebo jejich části, nabídky, kontrakty, smlouvy, dohody nebo jiná ujednání s třetími stranami, informace o výsledcích hospodaření, o vztazích s obchodními partnery, o pracovněprávních otázkách a všechny další informace, jejichž zveřejnění přijímající smluvní stranou by předávající smluvní straně mohlo způsobit škodu (dále jen „důvěrné informace“).

2. Smluvní strany jsou si vědomy toho, že v rámci plnění závazků z této smlouvy:

a) si mohou vzájemně poskytnout informace, které budou považovat nebo budou označeny za důvěrné informace;

b) mohou jejich zaměstnanci a osoby v obdobném postavení získat vědomou činností druhé smluvní strany nebo i jejich opominutím přístup k důvěrným informacím druhé smluvní strany.

3. Za třetí osoby podle odst. 1. tohoto článku se nepovažují

a) zaměstnanci smluvních stran a osoby v obdobném postavení ve vztahu k objednateli;

b) statutární orgány dodavatele a jejich členové;

c) ve vztahu k dodavateli jeho subdodavatelé; za předpokladu, že se podílejí na plnění této smlouvy. Důvěrné informace jsou jim zpřístupněny výhradně za tímto účelem a zpřístupnění důvěrných informací je učiněno v rozsahu nezbytně nutném pro naplnění jeho účelu a za stejných podmínek, jaké jsou stanoveny smluvním stranám v této smlouvě.

4. Smluvní strany se zavazují v plném rozsahu zachovávat povinnost mlčenlivosti a povinnost chránit důvěrné informace vyplývající z této smlouvy a též z příslušných právních předpisů, zejména osobní údaje dle zákona č. 110/2019 Sb., o zpracování osobních údajů, ve znění pozdějších předpisů (dále jen „ZZOÚ"), Nařízení Evropského parlamentu a rady (EU) 2016/679 (dále jen „GDPR"). Smluvní strany se v této souvislosti zavazují poučit veškeré osoby, které se budou podílet na plnění smlouvy, o výše uvedených povinnostech mlčenlivosti a ochrany důvěrných informací a dále se zavazují vhodným způsobem zajistit dodržování těchto povinností všemi osobami podílejícími se na plnění smlouvy.

5. Budou-li informace poskytnuté objednatelem či třetími stranami, které jsou nezbytné pro plnění dle této smlouvy, obsahovat data podléhající režimu zvláštní ochrany podle ZZOÚ, zavazuje se dodavatel zabezpečit jejich ochranu a splnění všech ohlašovacích povinností, které ZZOÚ vyžaduje, a obstarat předepsané souhlasy subjektů osobních údajů předaných ke zpracování, bude-li jejich obstarání v daném případě nezbytné. Dodavatel je povinen si vyžádat k provedení úkonů dle tohoto odstavce zvláštní plnou moc od objednatele.

6. Veškeré důvěrné informace zůstávají výhradním vlastnictvím předávající smluvní strany a přijímající smluvní strana vyvine pro zachování jejich důvěrností a pro jejich ochranu stejné úsilí, jako by se jednalo o jejich vlastní důvěrné informace. S výjimkou rozsahu, který je nezbytný pro plnění smlouvy, se obě smluvní strany zavazují neduplikovat žádným způsobem důvěrné informace druhé smluvní strany, nepředat je třetí straně ani svým vlastním zaměstnancům a zástupcům s výjimkou těch, kteří s nimi potřebují být seznámeni, aby mohli plnit smlouvu. Obě smluvní strany se zároveň zavazují nepoužít důvěrné informace druhé smluvní strany jinak, než za účelem plnění této smlouvy.

7. Bez ohledu na výše uvedená ustanovení se za důvěrné informace nepovažují informace, které:

a) se staly veřejně známými či dostupnými, aniž by to zavinila záměrně či nedbalostně přijímající smluvní strana;

b) měla přijímající smluvní strana legálně k dispozici před uzavřením smlouvy, pokud takové informace nebyly předmětem jiné, dříve mezi smluvními stranami uzavřené smlouvy o ochraně informací;

c) jsou výsledkem postupu, při kterém k nim přijímající smluvní strana dospěje nezávisle, což je schopna doložit svými záznamy nebo důvěrnými informacemi třetí strany;

d) po podpisu smlouvy poskytne přijímající smluvní straně třetí osoba, jež takové informace přitom nezíská přímo ani nepřímo od smluvní strany, od které tyto informace pocházejí;

e) jejichž zveřejnění je vyžadováno zákonem či pravomocným rozhodnutím orgánu státní správy, obecných či stálých rozhodčích soudů.

8. Povinnost utajovat důvěrné informace uvedená v tomto článku zavazuje smluvní strany po dobu účinnosti této smlouvy a po dobu deset (10) let následujících od jejího ukončení.

## XI. Ukončení smlouvy

1. Tato smlouva může být předčasně ukončena písemnou dohodou smluvních stran

s jednoznačným určením data, ke kterému smlouva zaniká.

2. Obě smluvní strany jsou oprávněny odstoupit od smlouvy v případě podstatného porušení povinností druhou smluvní stranou. V tom případě je smluvní strana odstupující od smlouvy povinna oznámit odstoupení od smlouvy druhé smluvní straně bez zbytečného odkladu poté, co se o jejím podstatném porušení smluvních povinností dozvěděla. Za podstatné porušení smluvních povinností se rozumí zejména:

a) ze strany dodavatele:

- prodlení dodavatele s předáním předmětu plnění delší než 15 dnů,
- prodlení dodavatele s odstraněním vad plnění ve lhůtě dle čl. IV. odst. 2.,
- pokud nabude právní moci rozhodnutí insolvenčního soudu o úpadku dodavatele, v němž tento soud konstatuje, že je dodavatel v úpadku, dále zahájení exekučního řízení na majetek dodavatele a vstoupí-li dodavatel do likvidace,
- jestliže dodavatel objednatele ujistil, že předmět plnění má určité vlastnosti, zejména vlastnosti objednatelem vymíněné, nebo že nemá žádné vady, a toto ujištění se ukáže nepravdivým.

b) ze strany objednatele:

- prodlení s úhradou jakéhokoli oprávněně vystaveného daňového dokladu či dokladů k úhradě dodavateli ve lhůtě delší než 30 dnů.

3. Odstoupením od smlouvy se závazky ze smlouvy zrušují. Plnila-li smluvní strana podstatně porušující smlouvu zčásti, může oprávněná smluvní strana od smlouvy odstoupit jen ohledně nesplněného zbytku plnění. Nemá-li však částečné plnění pro odstupující smluvní stranu význam, může od smlouvy odstoupit ohledně celého plnění. Odstoupení od smlouvy je účinné okamžikem doručení písemného oznámení o odstoupení uvádějícího důvod odstoupení druhé smluvní straně.

4. Odstoupení od smlouvy se nedotýká nároku na zaplacení smluvní pokuty, autorských práv, nároku na náhradu újmy vzniklé porušením smlouvy ani závazku mlčenlivosti dodavatele, ani dalších práv a povinností, z jejichž povahy plyne, že mají trvat i po ukončení smlouvy.

## XII. Závěrečná ujednání

1. Tato smlouva se řídí právním řádem České republiky, a to v otázkách v ní výslovně neupravených zákonem č. 89/2012 Sb., občanským zákoníkem, v aktuálním znění.

2. Tato smlouva nabývá platnosti dnem jejího podpisu oprávněnými osobami obou smluvních stran a účinnosti dnem jejího uveřejnění podle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv, dále jen „ZoRS").

3. Ukáže-li se některé z ustanovení této smlouvy zdánlivým (nicotným), posoudí se vliv takového ustanovení smlouvy obdobně podle § 576 občanského zákoníku.

4. Smluvní strany si výslovně sjednávají zákaz postupování pohledávek z této smlouvy (§ 1881 občanského zákoníku) na třetí osoby a dále zákaz postupování práv a povinností ze smlouvy nebo její části (§ 1895 občanského zákoníku) na třetí osoby.

5. Za adresy pro doručování projevů vůle mezi účastníky se považují adresy uvedené v záhlaví této smlouvy. Za řádné a účinné doručení písemných projevů vůle týkajících se vztahů a nároků vzniklých z této smlouvy se považuje i případ, kdy dojde k tzv. závadám při doručování dodavateli vykazovaným orgánem pověřeným poštovní přepravou (zejm. nevyzvednutí si zásilky adresátem, neznámost nebo nemožnost kontaktovat adresáta na uvedené adrese apod.). V takových případech se za okamžik řádného doručení projevu vůle pro účely této smlouvy považuje 10. den následující po

prvním pokusu orgánu pověřeného poštovní přepravou o doručení projevu vůle adresátovi.

6. Jakékoliv změny závazkového právního vztahu založeného touto smlouvou mohou být činěny toliko písemnými datovanými vzestupně číslovanými dodatky podepsanými oprávněnými osobami obou smluvních stran.

7. Dodavatel se zavazuje zajistit, aby po celou dobu trvání smlouvy zůstalo v platnosti a účinnosti pojištění odpovědnosti za škodu způsobenou jeho podnikatelskou činností objednateli a třetím osobám s minimálním limitem pojistného plnění ve výši 3.000.000,- Kč. Porušení této povinnosti se považuje za hrubé porušení smluvních povinností dodavatele. V případě škodní události se dodavatel zavazuje nahlásit v řádném termínu věc u své pojišťovny tak, aby bylo dosaženo odškodnění objednatele v maximální výši. Dodavatel je povinen nahradit objednateli vzniklou škodu nebo i část škody, která nebude odškodněna pojišťovnou.

8. Dodavatel bere na vědomí, že je osobou povinou spolupůsobit při výkonu finanční kontroly dle § 2 písm. e) zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů, ve znění pozdějších předpisů a zavazuje se, že umožní všem subjektům oprávněným k výkonu kontroly projektu, z jehož prostředků je dodané plnění hrazeno, provést kontrolu dokladů souvisejících s plněním zakázky, a to po dobu danou právními předpisy ČR k jejich archivaci.

9. Objednatel a dodavatel se zavazují řešit veškeré své případné spory vzešlé nebo související s touto smlouvou přednostně mimosoudní cestou, přičemž se za tímto účelem zavazují poskytnout si navzájem potřebnou součinnost.

10. Tato smlouva je vyhotovena a podepsána elektronicky. Každá ze smluvních stran obdrží originál smlouvy v elektronické podobě.

11. Dodavatel bere na vědomí a výslovně souhlasí s tím, že tato smlouva včetně případných dodatků bude objednatelem v souladu s ustanovením ZoRS zveřejněna.

12. Obě strany potvrzují, že tato smlouva byla uzavřena svobodně a vážně, na základě projevené vůle obou smluvních stran, že souhlasí s jejím obsahem, a že tato smlouva nebyla ujednána v tísni ani za jinak jednostranně nevýhodných podmínek.

13. Nedílnou součástí této smlouvy jsou níže uvedené přílohy:

Příloha č. 1 – Technická specifikace předmětu plnění

Příloha č. 2 - Service level Agreement - SLA

V Praze dne *dle elektronického podpisu*

[redacted]
Datum: 2026.05.11 15:47:12 +02'00'

.....

**Národní knihovna České republiky**

Ing. Václav Šubrta, LL.M.
náměstek
sekce Digitalizace a technologie NK ČR

V Litoměřicích dne *dle elektronického podpisu*

[redacted]
Datum: 2026.05.11 15:33:19 +02'00'

.....

**Netlancers s.r.o.**

Ing. Martin Macek
jednatel

| |
|---|
| Součástí zakázky je dodávka, implementace a podpora SIEM systému. Způsob technické realizace (HW appliance, VM nebo jejich kombinace) není předem stanoven – uchazeč navrhuje řešení, které splní níže uvedené funkční a výkonnostní požadavky. Cloud (SaaS/hosted) varianta není přípustná – systém musí být provozován na infrastruktuře kupujícího. |

| **Podrobné technické požadavky na řešení:** | | |
|---|---|---|

| **Požadavky na řešení** | **Závazná hodnota nabízená uchazečem či informace, že daný požadavek splňuje** | **Závaznost** |
|---|---|---|
| 1. Rozsah dodávky SIEM: | | |
| a) Centrální prvek řešení a komponenty pro sběr logů (kolektory) mohou být dodány jako HW appliance, jako VM nebo jako jejich kombinace. Uchazeč v nabídce popíše zvolenou architekturu a zdůvodní ji z hlediska výkonu, dostupnosti a snadnosti správy pro prostředí kupujícího. | ANO | Doložit nabídkou |
| b) Řešení musí být dimenzováno na minimálně 600 zdrojů logů. Licencovaná EPS kapacita musí vycházet z realistického odhadu objemu logů pro navrhované prostředí kupujícího – uchazeč v nabídce doloží výpočet odhadovaného EPS (včetně agentů s FIM monitoringem) a navrhne kapacitu s rezervou min. 30 %. Licencovaná kapacita nesmí být nižší než součet odhadovaných EPS ze všech kategorií zdrojů × 1,3. Řešení musí dále obsahovat licenci pro min. 500 serverových agentů. | ANO | Doložit nabídkou |
| 2. Řešení SIEM musí poskytovat škálovatelnou distribuovanou architekturu s následujícími vlastnostmi: | | |
| a) Komponenty pro sběr logů (kolektory) jsou dodány jako HW appliance, jako VM nebo jako kombinace obou. Uchazeč v nabídce popíše, jak pokryje jednotlivé lokality kupujícího. | ANO | Doložit nabídkou |
| b) Kolektory předávají data událostí do centrálního prvku SIEM architektury pro ukládání a korelaci. | ANO | Podmínka |
| c) Kolektory jsou schopny ukládat data do mezipaměti v případě, že centrální prvek SIEM architektury nebude dostupný. | ANO | Podmínka |
| d) Kolektory komprimují data před odesláním do centrálního prvku SIEM architektury. | ANO | Podmínka |

| | | |
|---|---|---|
| e) Kolektory komunikují s centrálním prvkem prostřednictvím protokolu HTTPS. Směr komunikace je od kolektorů k centrálnímu prvku SIEM architektury. | ANO | Podmínka |
| f) Kolektory se nekonfigurují jednotlivě, ale jsou spravovány centrálně, a pro opětovné nasazení kolektoru by neměla být nutná žádná specifická konfigurace kromě informace o IP adrese. | ANO | Podmínka |
| g) Kolektory musí být schopny zpracovat 10K EPS (událostí za vteřinu). | ANO | Podmínka |
| h) Celková kapacita komponent pro sběr logů musí být minimálně 3× odhadovaný normální EPS load prostředí kupujícího dle výpočtu uchazeče v nabídce. Tím je zajištěna dostatečná rezerva pro zpracování špičkového zatížení při bezpečnostním incidentu bez ztráty dat. | ANO | Podmínka |
| i) Komponenty pro sběr logů musí být schopny provádět aktivní zjišťování zařízení v síti a shromažďovat výkonnostní metriky prostřednictvím standardních protokolů, minimálně SNMP, SSH a WMI/OMI. | ANO | Podmínka |
| j) Komponenty pro sběr logů musí podporovat příjem a zpracování síťových flow dat ve formátech NetFlow, IPFIX nebo sFlow. | ANO | Podmínka |
| 3. Centrální prvek SIEM architektury, úložiště a korelační vrstva SIEM, dále označované jako SIEM, budou mít následující vlastnosti: | | |
| a) Centrální prvek SIEM systému je dostupný jako HW appliance nebo jako VM. Je-li dodán jako VM, musí splňovat podmínky dle bodu b). Je-li dodán jako HW appliance, musí splňovat výkonnostní požadavky dle bodu 1b. | ANO | Podmínka |
| b) Je-li centrální prvek nebo kolektor dodán ve formě VM, musí podporovat všechny tři z následujících on-premise virtualizačních platforem: VMware vSphere, Microsoft Hyper-V, KVM. Podpora cloudových platforem není požadována. | ANO | Podmínka |
| i. VMware vSphere | ANO | Podmínka |
| ii. Microsoft Hyper-V | ANO | Podmínka |
| iii. KVM | ANO | Podmínka |
| c) SIEM lze škálovat přidáním dalších fyzických nebo virtuálních zařízení do clusteru. Tato schopnost škálování musí dále zajistit distribuovanou korelaci pravidel v reálném čase v paměti všech komponent clusteru. | ANO | Podmínka |

| | | |
|---|---|---|
| d) Systém musí podporovat horizontální škálování přidáním dalších komponent (HW nebo VM) bez přerušení provozu a bez nutnosti rekonfigurace stávajících zdrojů logů. Veškerá data uložená napříč komponentami systému musí být dostupná prostřednictvím jednotného GUI. | ANO | Podmínka |
| e) SIEM musí být schopen ukládat jak surové logy, tak i analyzovaný protokol událostí/normalizovaná data. | ANO | Podmínka |
| f) Systém musí být schopen přijmout a zpracovat každou událost předanou komponentami pro sběr logů bez nutnosti samostatného filtrovacího nebo přeposílacího prvku mezi kolektorem a centrálním úložištěm. | ANO | Podmínka |
| g) Data událostí musí být uložena v komprimovaném režimu. Komprese nesmí omezovat dostupnost dat pro analytické vyhledávání v reálném čase. | ANO | Podmínka |
| 4. SIEM musí být schopen shromažďovat další context informací o zařízeních nad rámec logovacích dat ze zařízení, čehož by mělo být dosaženo: | | |
| a) Aktivním zjišťováním zařízení v síti bez nutnosti instalace agenta prostřednictvím standardních protokolů, minimálně: SNMP, WMI, SSH, REST API a rozhraní virtualizačních platforem. | ANO | Podmínka |
| b) Možností sledovat stav a odezvu služeb včetně DNS, FTP/SCP, obecných TCP/UDP, ICMP, JDBC, LDAP, SMTP, IMAP4, POP3, POP3S, SMTP, SSH a webu - HTTP, HTTPS (jedno- a vícekrokové). Výsledky tohoto monitoru dostupnosti lze použít k výpočtu schopnosti služby, například dostupnosti služby, která je dostupná na 99 %. | ANO | Podmínka |
| c) Jakmile je zařízení objeveno, musí být prezentováno v databázi pro správu konfigurace (CMDB) vytvořené v rámci řešení SIEM, dostupné prostřednictvím jednotného GUI. Jedná-li se o samostatnou komponentu, nesmí tato pro provoz vyžadovat samostaný server. | ANO | Podmínka |
| d) Objevená zařízení musí být dynamicky přiřazena skupinám CMDB na základě uživatelem definovaných vlastních vlastností. | ANO | Podmínka |
| e) Každé objevené zařízení musí být automaticky zaznamenáno v databázi pro správu konfigurací (CMDB) integrované v rámci SIEM systému. | ANO | Podmínka |
| f) Objevená zařízení musí být automaticky zařazena do skupin v CMDB na základě jejich typu a vlastností zjištěných při discovery (např. servery Windows, firewally, směrovače). | ANO | Podmínka |

| | | |
|---|---|---|
| g) Aplikace spuštěné na zařízeních musí být automaticky detekovány a zařazena do skupin aplikací v CMDB. Každá skupina aplikací musí automaticky obsahovat seznam zařízení, na kterých daná aplikace běží. | ANO | Podmínka |
| h) Musí být podporován import informací do CMDB prostřednictvím CSV. | ANO | Podmínka |
| i) Po dokončení aktivního zjišťování zařízení musí systém automaticky navrhnout nebo aplikovat šablony definující, jaké výkonnostní metriky se budou pro dané zařízení sbírat a v jakých intervalech. Sběr metrik musí využívat protokoly dle bodu 4a. | ANO | Podmínka |
| j) Výkonnostní metriky sbírané aktivním dotazováním a nespoléhající se na logy generované zařízením musí zahrnovat minimálně: rychlost síťových rozhraní, chyby přenosu, objem odeslaných a přijatých dat; využití CPU, paměti a disku; využití procesů. | ANO | Podmínka |
| 5. Do SIEMu musí být z kolektorů předávána jak surová, tak analyzovaná a obohacená data. Pokud jsou pro surová a obohacená data použity samostatné databáze, musí být vše dostupné jednotně z GUI a vše musí být plně propojené. | ANO | Podmínka |
| 6. Data událostí musí být normalizována a dostupná pro korelaci a vyhledávání bez zbytečného odkladu po přijetí. Uchazeč v nabídce popíše způsob a architekturu zpracování dat a maximální latenci od příjmu události do její dostupnosti pro analytika. | ANO | Doložit nabídkou |
| 7. Správu parserů, atributů, typů zařízení a typů událostí musí být schopen provádět administrátor bez programátorských znalostí. | ANO | Podmínka |
| 8. Parsery musí být upravitelné a rozšiřitelné. Vlastní parsery musí být možné vytvářet a definovat prostřednictvím grafického uživatelského rozhraní bez nutnosti přístupu k CLI nebo zdrojovému kódu. Parsery musí podporovat: definici vzorů a proměnných; funkce pro identifikaci klíčových hodnot; analýzu strukturovaných dat (JSON, XML, CEF); testování parserů přímo v editoru; transformace dat ve fázi parsování. | ANO | Doložit nabídkou |
| 9. Systém musí podporovat monitoring zařízení bez nutnosti instalace agenta prostřednictvím standardních protokolů, minimálně SSH, WMI a PowerShell. | ANO | Podmínka |
| 10. Systém musí podporovat sběr událostí ze systémů Windows prostřednictvím WMI/OMI a prostřednictvím agenta. | ANO | Podmínka |
| 11. Systém musí poskytovat agenta pro systémy Windows se správou centralizovanou z konzole SIEM systému bez nutnosti samostatné správcovské platformy. Agent musí podporovat: | ANO | Podmínka |

| | | |
|---|---|---|
| a) sběr logů z textových souborů a systémových protokolů Windows nad rámec standardních bezpečnostních, systémových a aplikačních logů; | ANO | Podmínka |
| b) sledování integrity souborů (FIM) včetně detekce změn oprávnění a vlastnictví; | ANO | Podmínka |
| c) monitorování registru Windows; | ANO | Podmínka |
| d) sledování použití vyměnitelných médií; | ANO | Podmínka |
| e) šifrovaný přenos dat do SIEM systému (HTTPS/TLS). | ANO | Podmínka |
| 12. Možnosti shromažďovat události systému Linux prostřednictvím syslog i agenta | ANO | Podmínka |
| 13. Systém musí poskytovat přístup založený na rolích, aby bylo možné omezit přístup k datům a také omezit přístup ke grafickému uživatelskému rozhraní. (RBAC) | ANO | Podmínka |
| 14. Systém musí podporovat integraci s Active Directory a LDAP pro obohacení událostí o kontext uživatele, skupin a organizační struktury. | ANO | Podmínka |
| 15. AD strukturu a uživatelský kontext z Active Directory musí být možné použít jako filtrační podmínku v reportech, vyhledávání a korelačních pravidlech. | ANO | Podmínka |
| 16. Systém musí podporovat externí autentizaci prostřednictvím minimálně: Active Directory, LDAP, RADIUS a SAML. | ANO | Podmínka |
| 17. Systém musí podporovat integraci zdrojů Threat Intelligence zahrnující: | ANO | Podmínka |
| a) import TI dat prostřednictvím CSV přes GUI a prostřednictvím REST API | ANO | Podmínka |
| b) podporu formátů STIX/TAXII | ANO | Podmínka |
| c) podporu minimálně těchto typů indikátorů: IP adresy, domény, hash hodnoty souborů, URL adresy, názvy procesů malwaru | ANO | Podmínka |
| d) kapacitu minimálně 200 000 záznamů na jeden TI zdroj | ANO | Podmínka |
| 18. Systém musí poskytovat šablony reportů pro compliance účely bez dalších poplatků, minimálně pro: ISO 27001 a CIS Controls. Uchazeč dále doloží dostupné šablony pro požadavky zákona o kybernetické bezpečnosti a dalších relevantních rámců. | ANO | Doložit nabídkou |
| 19. SIEM musí umožnit export a import nastavení ovládacích panelů, sestav a pravidel. | ANO | Podmínka |
| 20. SIEM musí mít schopnost shromažďovat konfiguraci síťových zařízení, identifikovat změny a poskytovat vzájemné porovnání. | ANO | Podmínka |
| 21. SIEM musí obsahovat přehled, který poskytuje pomocí barev stav reportování z monitorovaných zařízení. | ANO | Podmínka |

| | | |
|---|---|---|
| 22. Vizualizace přehledů musí podporovat různé typy grafů včetně časových řad, geografických map a tabulkových zobrazení. Na grafech musí být možné definovat prahové hodnoty. | ANO | Podmínka |
| 23. Systém musí obsahovat správu incidentů zahrnující: | ANO | Podmínka |
| a) konfigurovatelná pravidla pro oznamování incidentů minimálně e-mailem | ANO | Podmínka |
| b) možnost integrace s externími ticketovacími systémy prostřednictvím API | ANO | Podmínka |
| c) možnost automatické nebo ruční reakce na incident (izolace zařízení, blokace IP, spuštění akce) prostřednictvím integrovaného mechanismu nebo napojení na SOAR | ANO | Doložit nabídkou |
| 24. Systém musí poskytovat analytické funkce zahrnující: | ANO | Podmínka |
| a) vyhledávání událostí v reálném čase bez nutnosti indexování s podporou logických operátorů (AND, OR, NOT), porovnávacích operátorů, testování přítomnosti hodnoty a regulárních výrazů | ANO | Podmínka |
| b) vyhledávání podle klíčových slov i podle parsovaných atributů událostí | ANO | Podmínka |
| c) historické dotazy s boolean filtry, agregacemi, filtry podle času a regulárními výrazy | ANO | Podmínka |
| d) vyhodnocování událostí v reálném čase pomocí korelačního modulu pravidel | ANO | Podmínka |
| e) využití objektů CMDB a kontextu uživatelů a identit ve vyhledávání a pravidlech | ANO | Podmínka |
| f) plánování generování reportů a jejich doručování e-mailem. Export reportů musí být dostupný ve strojově čitelném formátu pro další zpracování a v lidsky čitelném formátu pro sdílení a archivaci | ANO | Podmínka |
| g) vyhledávání událostí v rámci celé organizace nebo až do jednotlivého fyzického či logického prvku | ANO | Podmínka |
| h) systém musí podporovat dynamické seznamy entit (uživatelů, IP adres, zařízení) které se automaticky aktualizují na základě konfigurovatelných podmínek, tyto seznamy musí být použitelné jako vstupní podmínka v korelačních pravidlech i v reportech | ANO | Podmínka |
| i) systém musí umožňovat seskupení zařízení a služeb do logických celků (např. podle business kritičnosti nebo organizační struktury) a prioritizaci hlášení incidentů na základě příslušnosti zařízení k těmto celkům | ANO | Podmínka |

| | | |
|---|---|---|
| j) názvy a popisy incidentů musí podporovat dynamické hodnoty odvozené z dat události, například uživatelské jméno, zdrojová IP adresa nebo název zařízení | ANO | Podmínka |
| k) korelační pravidla musí být mapovatelná na techniky a taktiky MITRE ATT&CK Enterprise Matrix; zobrazení incidentů musí obsahovat přehled pokrytí pravidel vůči matici MITRE ATT&CK | ANO | Podmínka |
| l) systém musí poskytovat mechanismy pro snížení počtu falešných pozitivů, zejména možnost korelace incidentů s kontextovými informacemi o zranitelnostech zařízení a jeho konfigurace: uchazeč popíše způsob implementace a doloží příkladem | ANO | Doložit nabídkou |
| m) možnost automatického přiřazení uživatele k poloze a IP adrese | ANO | Podmínka |
| 25. SIEM musí umožnit předávat veškeré shromážděné informace o událostech prostřednictvím Kafka protokolu. | ANO | Podmínka |
| 26. SIEM musí umožnit přijímat události prostřednictvím protokolu Kafka | ANO | Podmínka |
| 27. Systém musí podporovat archivaci dat na základě konfigurovatelných pravidel na externí úložiště (např. NFS nebo jiné standardní síťové úložiště). Archivovaná data musí být obnovitelná prostřednictvím GUI a po obnovení dostupná pro analytické vyhledávání stejným způsobem jako online data. | ANO | Podmínka |
| 28. Systém musí být integrován s MITRE ATT&CK Enterprise Matrix: | ANO | Podmínka |
| a) systém musí obsahovat minimálně 500 korelačních pravidel z výroby mapovaných na techniky a taktiky MITRE ATT&CK pokrývajících minimálně 10 různých taktik | ANO | Podmínka |
| b) korelační pravidla včetně vlastních musí být přiřaditelná k jedné nebo více technikám ATT&CK | ANO | Podmínka |
| c) systém musí zobrazovat přehled aktuálního pokrytí prostředí vůči matici ATT&CK | ANO | Podmínka |
| d) systém musí umožňovat vyhledávání incidentů podle techniky nebo taktiky ATT&CK | ANO | Podmínka |
| 29. Je-li centrální prvek dodán jako VM, musí umožňovat navyšování kapacity disku v závislosti na přidělených zdrojích hypervizorem bez nutnosti reinstalace systému. Je-li dodán jako HW appliance, uchazeč popíše způsob rozšíření úložné kapacity. | ANO | Podmínka |
| 30. Řešení je licencováno na základě celkového počtu zpracovávaných událostí za vteřinu a případně počtu zařízení, které tyto logy generují | ANO | Doložit nabídkou |

| | | |
|---|---|---|
| 31. Licenční rozšíření kapacity systému (EPS, počet zdrojů nebo obojí) musí být dostupné průběžně bez nutnosti uzavření nové smlouvy. Způsob a granularita navýšení vychází ze zvoleného licenčního modelu uchazeče. Uchazeč doloží ceník rozšiřujících licencí jako součást nabídky. | ANO | Podmínka |
| 32. Systém musí být schopen zpracovávat krátkodobé nárůsty objemu událostí přesahující licencovanou kapacitu (burst handling) bez ztráty dat. Uchazeč v nabídce popíše mechanismus zpracování špičkového zatížení, maximální překročení licencované kapacity které systém udrží a dobu po kterou to vydrží. Chování systému při překročení kapacity musí být viditelné v GUI. | ANO | Doložit nabídkou |
| 33. Systém musí umožňovat aktualizaci funkčních prvků (parserů, korelačních pravidel, reportů, GEO databáze a dalšího obsahu) nezávisle na aktualizaci systému jako celku, bez nutnosti přerušení provozu. | ANO | Podmínka |
| 34. Veškeré historické logy uložené v systému musí být exportovatelné v otevřeném nebo standardizovaném formátu (JSON, CSV, CEF nebo Syslog) na úložiště kupujícího. Veškerá konfigurace systému (korelační pravidla, parsery, dashboardy, nastavení RBAC, skupiny zařízení) musí být exportovatelná ve strojově čitelném formátu umožňujícím import do nástupnického systému. Uchazeč popíše export mechanismus a ukáže formát exportu. | ANO | Podmínka |
| 35. SIEM musí umožnit anonymizaci citlivých údajů jako je zdrojová IP, uživatelské jméno apod. | ANO | Podmínka |
| 36. SIEM musí umožnit vytvořit požadavek na dočasnou de-anonymizaci citlivých údajů pro vyšetřování incidentu. V rámci požadavku je možné nastavit dobu, po kterou budou údaje de-anonymozivány, po jejímž uplynutí budou opětovně anonymní | ANO | Podmínka |

| | |
|---|---|
| **AKCEPTAČNÍ TESTY – ověření při předání systému (testy probíhají na infrastruktuře kupujícího)** | |

| | |
|---|---|
| *Akceptační testy jsou podmínkou předání. Nesplnění kteréhokoli testu znamená odmítnutí akceptace. Testy probíhají výhradně na infrastruktuře objednatele, nikoli v testovacím prostředí dodavatele.* | |
| AT-1 Zátěžový test: Systém zpracuje testovací zátěž odpovídající 130 % licencované EPS kapacity po dobu 30 minut bez ztráty dat a bez degradace výkonu (latence korelace nesmí překročit hodnotu deklarovanou v nabídce). Test provede dodavatel na infrastruktuře objednatele za přítomnosti zástupce objednatele. O průběhu a výsledcích bude vyhotoven protokol. | **Podmínka** |
| AT-2 Detekční test: Systém vygeneruje alert na sadu min. 5 testovacích scénářů simulujících kybernetický útok (pokrývajících různé MITRE ATT&CK taktiky definované objednatelem před akceptací) do 5 minut od první události v sérii. Testovací scénáře připraví objednatel a sdělí je dodavateli nejpozději 5 pracovních dní před akceptací. | **Podmínka** |
| AT-3 Integrační test: Systém prokazatelně přijímá a správně normalizuje logy ze všech kategorií zařízení uvedených v části B (B.3.1). Pro každou kategorii musí být ověřena správnost parsování klíčových polí: zdrojová IP, cílová IP, uživatel, čas, typ události. Test probíhá na reálných zařízeních kupujícího. | **Podmínka** |
| AT-4 Test centrální správy: Veškeré konfigurační změny (nové korelační pravidlo, aktualizace parseru, přidání nového zdroje logů) jsou provedeny výhradně z centrální konzole bez přímého přístupu k jednotlivým komponentám v lokalitách. Demonstrace probíhá za přítomnosti zástupce objednatele. | **Podmínka** |
| AT-5 Test exportu dat: Dodavatel demonstruje export vzorku historických logů v otevřeném formátu (JSON, CSV nebo CEF) a export konfigurace systému (korelační pravidla, dashboardy) ve strojově čitelném formátu. Exportovaná data musí být čitelná bez proprietárního nástroje dodavatele. | **Podmínka** |

**Provozní podpora a smluvní úroveň služeb (Service Level Agreement – SLA)**

## 1. Úvodní ustanovení

**1.1** Tato příloha (dále jen „SLA“) upravuje rozsah a úroveň podpory poskytované dodavatelem k předmětu plnění dle *Smlouvy o dodávce produktu pro sběr a korelaci bezpečnostních událostí - SIEM* (dále jen „Smlouva“).

**1.2** V případě rozporu mezi ustanoveními této SLA a ustanoveními Smlouvy mají přednost ustanovení Smlouvy.

**1.3** Termíny s velkým počátečním písmenem, které nejsou v této SLA výslovně definovány, mají význam stanovený ve Smlouvě.

## 2. Definice pojmů

**2.1 Incident** je každé neplánované přerušení, omezení nebo zhoršení funkčnosti Předmětu plnění, které má za následek, že Předmět plnění není možné užívat způsobem odpovídajícím této Smlouvě a Technické specifikaci (Příloha č. 1 Smlouvy).

**2.2 Vada plnění** je nesoulad Předmětu plnění nebo jeho části se Smlouvou, touto SLA, Technickou specifikací nebo obecně závaznými právními předpisy, bez ohledu na to, zda se jedná o Incident.

**2.3 Havarijní závada (Incident kategorie P1)** je takový Incident, který:

- a) způsobí úplnou nedostupnost Předmětu plnění nebo jeho podstatné části pro většinu uživatelů objednatele, nebo
- b) vede k prokazatelné ztrátě nebo poškození dat, nebo bezprostředně hrozí taková ztráta nebo poškození, nebo
- c) zásadně omezuje plnění zákonných povinností objednatele nebo plnění klíčových procesů stanovených objednatelem.

**2.4 Závažná závada (Incident kategorie P2)** je Incident, který:

- a) významně omezuje funkčnost Předmětu plnění pro část uživatelů objednatele, aniž by došlo k úplné nedostupnosti, nebo
- b) znemožňuje využití některé z klíčových funkcionalit Předmětu plnění, avšak existuje dočasné náhradní řešení umožňující objednateli pokračovat v činnosti.

**2.5 Běžná závada (Incident kategorie P3)** je Incident, který:

- a) omezuje komfort nebo efektivitu užívání Předmětu plnění, avšak nebrání jeho podstatnému užívání, nebo
- b) se týká funkcionalit, které nejsou označeny jako kritické nebo klíčové.

**2.6 Nízkoprioritní závada (Incident kategorie P4)** je drobná závada nebo požadavek, který nemá přímý dopad na běžný provoz Předmětu plnění (např. kosmetické chyby v uživatelském rozhraní, překlepy v textech apod.).

**2.7 Předmět plnění** má význam stanovený ve Smlouvě.

**2.8 Pracovní den** je den, který není sobotou, nedělí ani státem uznaným svátkem v České republice.

**2.9 Pracovní doba podpory** je doba od 8:00 do 16:30 hodin v Pracovní dny, není-li ve Smlouvě nebo této SLA výslovně ujednáno jinak. Pro incidenty kategorie P1 platí nepřetržitá dostupnost 24x7x365 bez ohledu na pracovní dobu.

## 3. Hlášení incidentů

**3.1** Incidenty hlásí objednatel dodavateli prostřednictvím následujících kontaktů:

- a) servisní e-mail: [redacted]
- b) telefonní linka: [redacted], (platná 24x7 pro P1)
- c) případně servisní portál: [doplní se], pokud je zřízen.

**3.2** Objednatel je povinen při hlášení Incidentu uvést alespoň následující údaje: stručný popis Incidentu, předpokládanou kategorii Incidentu (P1–P4), kontaktní osobu a kontaktní údaje pro další komunikaci.

**3.3** Za okamžik řádného nahlášení Incidentu se považuje okamžik, kdy je Incident oznámen některým z výše uvedených způsobů a jsou poskytnuty informace dle bodu 3.2.

**3.4** Zařazení konkrétního Incidentu do kategorie P1–P4 provede objednatel při nahlášení Incidentu; Dodavatel je oprávněn navrhnout změnu kategorie, pokud k tomu existují objektivní důvody. V případě sporu o zařazení Incidentu rozhoduje kategorie určená objednatelem, doku není prokázán opak.

## 4. Reakční a řešící doby (SLA)

**4.1 Doba reakce** je doba od řádného nahlášení Incidentu objednatelem do okamžiku, kdy dodavatel potvrdí přijetí Incidentu, přiřadí Incidentu kategorii a zahájí prokazatelné řešení Incidentu (např. vzdálený přístup, analýza logů, návštěva technika apod.).

**4.2 Doba odstranění** je doba od řádného nahlášení Incidentu objednatelem do okamžiku:

- a) plného odstranění Incidentu, tj. obnovení funkčnosti Předmětu plnění v souladu se Smlouvou, nebo
- b) implementace funkčního dočasného náhradního řešení („workaround"), které umožňuje objednateli pokračovat v užívání Předmětu plnění bez podstatných omezení, přičemž trvalé odstranění Incidentu bude dokončeno v dohodnutém termínu.

**4.3** Není-li dále stanoveno jinak, počítají se doby reakce v rámci Pracovní doby podpory. Doby odstranění Incidentů se počítají v kalendářních hodinách, není-li výslovně uvedeno jinak. Doby P1 se počítají nepřetržitě v kalendářních hodinách 24x7x365.

**4.4** Dodavatel se zavazuje dodržet následující reakční a řešící doby:

**a) Incident P1 – Havarijní závada**

- Doba reakce: nejpozději do 2 hodin od nahlášení Incidentu.
- Doba odstranění: 4 kalendářní hodiny od nahlášení Incidentu.
- Dodavatel je povinen zahájit řešení Incidentu bezodkladně po nahlášení a pokračovat v něm až do odstranění Incidentu, a to i mimo Pracovní dobu podpory, je-li to nutné k dodržení doby odstranění.

**b) Incident P2 – Závažná závada**

- Doba reakce: nejpozději do 2 pracovních hodin v rámci Pracovní doby podpory.
- Doba odstranění: nejpozději do 24 kalendářních hodin od nahlášení Incidentu; doba se počítá v kalendářních hodinách
- Není-li možné Incident odstranit v uvedené době, je dodavatel povinen zajistit funkční dočasné náhradní řešení a dohodnout s objednatelem termín definitivního odstranění.

**c) Incident P3 – Běžná závada**

- Doba reakce: nejpozději do 8 pracovních hodin v rámci Pracovní doby podpory.
- Doba odstranění: nejpozději do 5 Pracovních dnů.

**d) Incident P4 – Nízkoprioritní závada**

- Doba reakce: nejpozději do 5 Pracovních dnů.
- Doba odstranění: v rámci nejbližší plánované údržby nebo releasu, nejpozději do 30 kalendářních dnů od nahlášení Incidentu.

**4.5** V případě, že dodavatel odhadne, že dobu odstranění Incidentu nebude možné dodržet, je povinen tuto skutečnost bezodkladně sdělit objednateli, navrhnout dočasné náhradní řešení (pokud je technicky proveditelné) a dohodnout s objednatelem nový závazný termín odstranění Incidentu.

## 5. Dostupnost systému

**5.1** Dodavatel se zavazuje zajistit, aby dostupnost Předmětu plnění dosahovala minimálně 99,5 % v každém kalendářním měsíci (dále jen „Garantovaná dostupnost“).

**5.2** Do výpočtu Garantované dostupnosti se nezapočítává:

- a) plánovaná odstávka Předmětu plnění předem oznámená objednateli alespoň 3 Pracovní dny předem,
- b) odstávky způsobené výpadky infrastruktury, za které dodavatel neodpovídá (např. dodavatel elektrické energie, poskytovatel konektivity),
- c) odstávky způsobené prokazatelným porušením povinností dodavatele podle Smlouvy.

**5.3** Nedosáhne-li dostupnost v daném kalendářním měsíci garantované hodnoty z důvodů na straně dodavatele, má objednatel nárok na slevu z měsíční ceny podpory: při dostupnosti 99,5 %–99,89 % slevu 10 %; při dostupnosti 99,0 %–99,49 % slevu 20 %; při dostupnosti nižší než 99,0 % slevu 30 % a právo odstoupit od části smlouvy týkající se provozní podpory dle čl. IX. a XI. Sleva se uplatní odečtením z nejbližšího daňového dokladu nebo dodavatel vystaví dobropis do 15 kalendářních dní od oznámení objednatele.

## 6. Sankce a souvislost se Smlouvou

**6.1** Nedodržení dob reakce a odstranění Incidentů podle čl. 4 této SLA se považuje za prodlení dodavatele s odstraněním vady plnění dle Smlouvy. Objednatel je v takovém případě oprávněn uplatnit smluvní pokuty a další nároky z prodlení podle Smlouvy.

**6.2** Opakované nedodržení SLA, zejména nedodržení doby odstranění Incidentů kategorie P1 a P2, se považuje za podstatné porušení Smlouvy a zakládá právo objednatele odstoupit od Smlouvy za podmínek v ní stanovených.

## 7. Závěrečná ustanovení

**7.1** Tato SLA tvoří nedílnou součást Smlouvy.

**7.2** Tuto SLA lze měnit nebo doplňovat pouze formou písemných, očíslovaných dodatků ke Smlouvě, podepsaných oprávněnými zástupci obou smluvních stran.

**7.3** Tato SLA nabývá účinnosti dnem účinnosti Smlouvy.