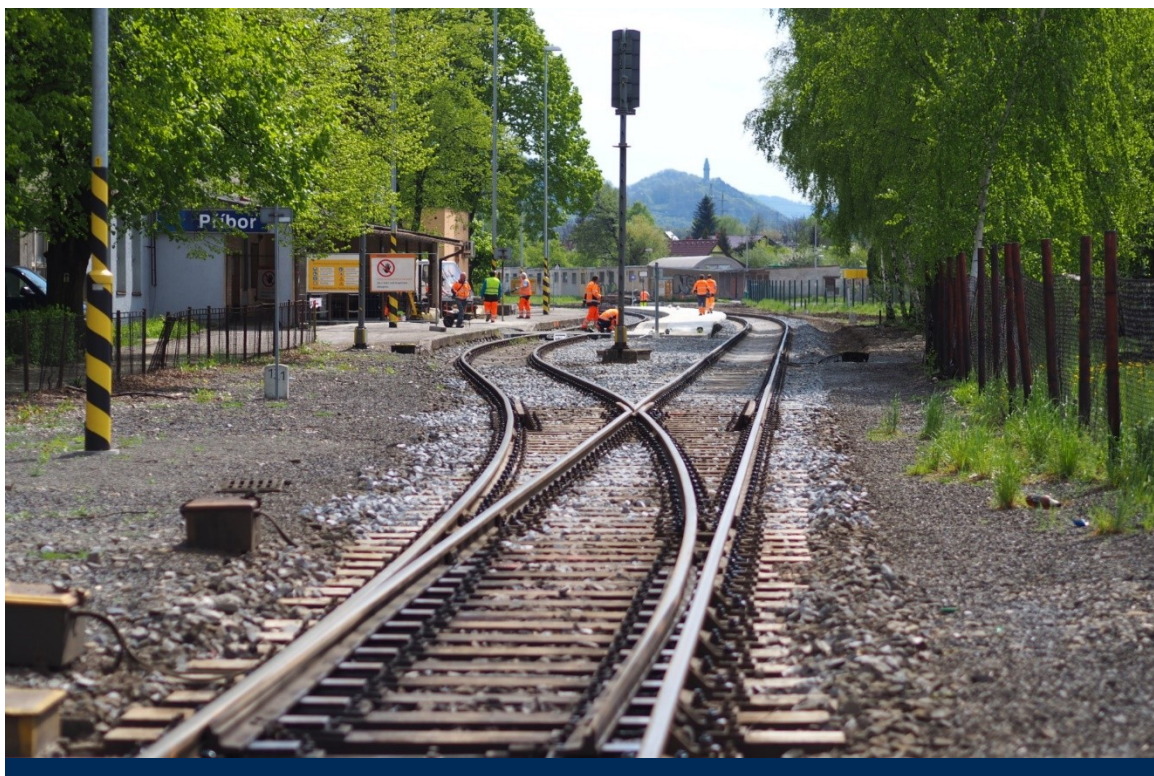




Technická specifikace – OT SIEM

**Příloha č. X Zadávací dokumentace | Otevřené řízení
dle § 56 ZZVZ**

Klasifikace: Pro potřeby VZ

Verze: 1.1 | Datum: [28.05.2026]

Obsah

2	Účel a rozsah dokumentu.....	4
2.1	Předmět plnění	4
3	Popis stávajícího prostředí (As-Is).....	5
3.1	Charakteristika OT prostředí.....	5
3.2	Síťová architektura.....	5
3.3	OT aktiva v prostředí ED	5
3.4	Průmyslové protokoly	5
3.5	Napojení na centrální dohled	6
4	Předmět plnění – detailní specifikace.....	7
4.1	Softwarová appliance OT SIEM	7
4.2	Licence pro síťové senzory	7
4.3	Licence pro OT/ICS endpointy (non-IT aktiva)	7
4.4	Softwarová podpora a maintenance (5 let).....	8
5	Architektonické požadavky	9
5.1	Vícestupňová hierarchická architektura	9
5.2	Ostrovni (air-gapped) provoz.....	9
6	Funkční požadavky	9
6.1	Viditelnost a inventarizace OT aktiv	9
6.2	Pasivní monitoring komunikace.....	10
6.3	Detekční scénáře (Use Cases).....	10
6.4	Správa zranitelností	11
6.5	Integrace s NAC (volitelná)	11
6.6	Integrace s centrálním IT SIEM (dokumentační povinnost)	11
6.7	Správa a auditovatelnost	12
7	Bezpečnostní a legislativní požadavky	13
8	Provozní a rozvojové požadavky	13
9	Licenční podmínky a model dodávky	14
10	Hodnotící a kvalifikační kritéria	15
10.1	Technická kvalifikace dodavatele.....	15
10.2	Hodnotící kritéria (§ 114 ZZVZ)	15
11	Ustanovení k nediskriminaci a otevřenosti soutěže	16
12	Přílohy.....	17
	Příloha D: Cenová tabulka – struktura nabídkové ceny.....	17
	Příloha E: Požadavky na formát exportu do centrálního SIEM.....	17

Zadavatel	Správa železnic, státní organizace
Název VZ	Dodávka licencí a softwarové appliance OT SIEM pro elektrodispečink – kraj Hradec Králové
Druh řízení	Otevřené řízení (§ 56 ZZVZ)
CPV kódy	48000000-8 Software packages and information systems; 72260000-5 Software-related services
Klasifikace dokumentu	Pro potřeby výběrového řízení
Verze / Datum vydání	1.1 / [doplň zadavatel VŘ]
Počet stran	[doplň zadavatel VŘ]
Schválil	[doplň zadavatel VŘ]

2 Účel a rozsah dokumentu

Tento dokument tvoří závaznou technickou specifikaci (dále jen „TS“) a je přílohou zadávací dokumentace výběrového řízení na **dodávku licencí, softwarové appliance a zajištění softwarové podpory systému OT SIEM** pro prostředí elektro dispečinku (ED), provozovaného v rámci technologické datové sítě (TDS) Správy železnic.

2.1 Předmět plnění

Předmětem plnění jsou výhradně:

- Systém OT SIEM ve formě virtuálního serveru nebo fyzického HW dle nabídky uchazeče
- Sensorová architektura a s ní spojené licence a veškeré související produkty spojené s provozem
- Licence pro OT/ICS endpointy (non-IT aktiva) – **250 ks**
- Softwarová podpora (maintenance), aktualizace, technická asistence a záruka dostupnosti produktu na trhu po dobu **5 let**

Předmětem plnění NEJSOU:

- Návrh architektury řešení (byl realizován zadavatelem v rámci Proof of Concept)
- Implementace, instalace, konfigurace a zprovoznění systému (realizuje zadavatel vlastními silami za případné asistence dodavatele)
- Integrace s centrálním SIEM Splunk Enterprise (realizuje zadavatel vlastními silami)
- Jakékoli stavební ani síťové práce v prostředí ED / TDS

Poznámka k Proof of Concept: Zadavatel provedl v předchozí fázi ověřovací nasazení (PoC), jehož výsledkem jsou funkční a výkonnostní požadavky obsažené v tomto dokumentu. Tyto požadavky jsou formulovány **technologicky neutrálně a výkonnostně** – nevylučují žádné řešení, které je schopno prokázat jejich splnění. Technická kvalita a architektura ověřeného nasazení slouží jako referenční base line pro hodnocení nabídek.

3 Popis stávajícího prostředí (As-Is)

3.1 Charakteristika OT prostředí

Elektro dispečink, který je součástí Dispečerské řídicí technologie (DŘT) Správy železnic, zajišťující dohled a řízení elektrické infrastruktury (trakční vedení, trakční napájecí stanice, rozvodny VVN/VN/NN). Prostředí je provozováno v technologické datové síti (TDS) jako **uzavřený ostrovní systém** bez přímého propojení do intranetu / internetu (tj. mimo vnitřní zónu).

3.2 Síťová architektura

- Segmentace na úrovni L2/L3
- Oddělené bezpečnostní zóny, bezpečnostní zóny technologické datové sítě SŽ oddělené na úrovni L3 servisní přístupy (v souladu s modelem Zones & Conduits dle ISA/IEC 62443-3-2)
- Síťová infrastruktura: **přepínače enterprise třídy L2/L3** s podporou s podporou hostování kontejnerových aplikací + průmyslové přepínače (IE řada, Cat9300 apod.) a bezpečnostní prvky (firewall, SPAN/TAP body)
- Virtualizační infrastruktura pro podpůrné systémy (VMware ESXi)

3.3 OT aktiva v prostředí ED

Kategorie	Příklady zařízení
Řídicí a dohledové servery	např. SCADA
Operátorské / inženýrské stanice	HMI, EWS (Engineering Workstations)
Průmyslová řídicí zařízení	PLC, RTU, IED
Síťová infrastruktura	Přepínače L2/L3, průmyslové switche, firewall
Podpůrné systémy	Logovací, diagnostické, integrační servery
Celkový odhadovaný počet non-IT aktiv	cca 250 ks

3.4 Průmyslové protokoly

Prostředí využívá průmyslové komunikační protokoly typické pro řídicí systémy energetické a železniční infrastruktury, zejména: **IEC 60870-5-104** (primární protokol prostředí DŘT), IEC 61850, Modbus TCP/RTU a proprietární protokoly.

3.5 Napojení na centrální dohled

Pro předávání bezpečnostních událostí je uvažováno nepřímé napojení na centrální Log Management / SIEM platformu zadavatele (Splunk Enterprise) prostřednictvím kolektorů v infrastruktuře datové sítě SŽ. Tato integrace **není součástí předmětu plnění** – realizuje ji zadavatel vlastními silami za případné asistence dodavatele. Dodavatel je povinen zadavateli poskytnout dokumentaci API, formátům exportu a dostupným konektorům.

4 Předmět plnění – detailní specifikace

4.1 Softwarová appliance OT SIEM

Dodavatel dodá softwarovou appliance OT SIEM schopnou plnit funkci centrálního analytického uzlu pro dané prostředí. Primární volbou je softwarová appliance provozovatelná jako:

- Virtuální stroj (VMware ESXi bez VMware licencí)
- Fyzická (hardwarová) appliance (x86 server nebo ekvivalent) – v odůvodněném případě

Minimální výkonnostní parametry:

Parametr	Minimální požadavek
Diskový prostor – lokální uzel (Local Center / Edge)	≥ 250 GB SSD nebo HDD
Diskový prostor – centrální / agregační uzel (Global Center)	≥ 1 TB
Podpora virtualizačních platforem	VMware ESXi
Šifrování dat v klidu a při přenosu	FIPS 140-2 nebo FIPS 140-3
Zpětná kompatibilita lokálního a centrálního uzlu	Min. 1 minor verze SW zpětně

4.2 Licence pro síťové senzory

S vazbou na prvky senzorové architektury dodavatel dodá licence aktivující senzorické funkce na **přepínačích enterprise třídy L2/L3** nasazených v OT síti zadavatele případně pak prvky, které budou součástí dodávky, přičemž tyto přepínače jsou schopné provádět **DPI (Deep Packet Inspection) přímo na síťovém prvku** (edge computing přístup).

Klíčový funkční požadavek: Senzor musí provádět analýzu a klasifikaci komunikace lokálně a do centrálního uzlu přenášet **výhradně metadata** (nikoli kompletní zachycený provoz). Tím je dosaženo maximálního zatížení sítě v rozsahu **10 % oproti baseline**, čímž je minimalizován dopad na OT provoz.

Poznámka k nediskriminaci: Výše uvedený požadavek je funkcionální a výkonnostní. Uchazeč může předložit alternativní architekturu senzoru (např. dedikovaný hardwarový probe, softwarový kolektor, distribuovaný agent), pokud prokáže splnění výkonnostního požadavku: přenos pouze metadat, nulový aktivní dopad na OT provoz, žádné zásahy do OT zařízení.

4.3 Licence pro OT/ICS endpointy (non-IT aktiva)

- **Počet licencí:** 250 ks
- **Opce rozšíření:** Zadavatel si vyhrazuje právo doobjednat až 20 % licencí za smluvních podmínek bez nového výběrového řízení

- **Typ pokrytých aktiv:** PLC, RTU, HMI, IED, DCS, SCADA servery, průmyslové přepínače, IoT/IIoT zařízení
- **Model licencování:** Per-asset (pro non-IT aktivum), bez omezení protokolu nebo výrobce aktiva
- **Délka licence: 5 let** od data podpisu smlouvy, **předání licencí** a od podpisu akceptačního protokolu

4.4 Softwarová podpora a maintenance (5 let)

Parametr	Hodnota
Délka podpory	5 let od data podpisu smlouvy
Úroveň SLA	Min. 8x5, NBD (Next Business Day) – pro výměnu HW, 24x7 – softwarová podpora
Aktualizace softwaru (SW)	Zahrnuto – manuální (offline) import (v modelu distribuovaného řešení)
Aktualizace znalostní báze / detekčních signatur	Zahrnuto – offline import bez nutnosti přístupu k internetu
Záruční podmínky	Po celou dobu trvání support smlouvy (5 let)
Způsob poskytování aktualizací	Dodavatel zpřístupní aktualizace ke stažení nebo dodá na fyzickém médiu
Eskalační kontakt	Technický kontakt (TAC nebo ekvivalent)

5 Architektonické požadavky

5.1 Vícetupňová hierarchická architektura

Zadavatel požaduje, aby nasazené řešení podporovalo **vícetupňovou (hierarchickou) architekturu** lokálního a centrálního uzlu:

Vrstva	Funkce	Min. požadavky
Lokální uzel (Local Center / Edge)	Lokální sběr a analýza dat ze senzorů v dané lokalitě; lokální databáze (PostgreSQL nebo ekvivalent); schopnost autonomního provozu bez spojení na centrální uzel	≥ 250 GB disk; VM nebo appliance
Centrální uzel (Global Center / Aggregation)	Agregace metadat ze všech lokálních uzlů; jednotný přehled pro SOC; integrace s externím SIEM	≥ 1 TB disk; dedikovaná VM; vysoký výkon CPU/RAM

Komunikace mezi uzly musí probíhat výhradně prostřednictvím **šifrovaných kanálů** (TLS 1.2 nebo vyšší) a přenášet pouze **metadata a bezpečnostní události** (nikoli surový síťový provoz). Přípustné komunikační protokoly pro inter-node komunikaci: kde standardem jsou AMQP (TCP 5671), Syslog (UDP/TCP 514) nebo funkčně ekvivalentní.

5.2 Ostrovní (air-gapped) provoz

Řešení musí být plně provozovatelné v přísně regulovaném, odpojeném prostředí (air-gapped) bez trvalého přístupu k internetu:

- **Licencování:** Podpora offline správy licencí
- **Aktualizace:** Znalostní báze (threat intelligence), detekční signatury a SW aktualizace musí být importovatelné **manuálně (offline)** bez nutnosti přístupu k internetu
- **Provoz:** Veškeré analytické funkce musí být plně funkční v offline režimu
- **Správa:** Administrační rozhraní musí být dostupné lokálně bez závislosti na cloudové infrastruktuře dodavatele

6 Funkční požadavky

6.1 Viditelnost a inventarizace OT aktiv

- Automatická, **pasivní** (agentless) identifikace a klasifikace OT aktiv bez instalace SW agentů na monitorovaná zařízení
- Evidence – min.: typ, role, výrobce, firmware verze, síťová adresa, komunikační vzorce

- Vizualizace komunikačních vazeb a topologie sítě
- Detekce změn v topologii (nové aktivum, změna firmware, změna role zařízení)
- Schopnost monitorovat komunikaci z OT zařízení za **NATem** bez nutnosti úpravy NAT pravidel

6.2 Pasivní monitoring komunikace

- Výhradně **pasivní** odposlech síťové komunikace – žádné aktivní sondy, žádné zásahy do OT provozu, nulový dopad na řídicí technologii
- Analýza průmyslových protokolů na úrovni L2–L7 (DPI):
 - **IEC 60870-5-104** (povinně – primární protokol prostředí ED)
 - Modbus TCP/RTU, IEC 61850, DNP3, PROFINET, EtherNet/IP a další
- Lokální zpracování komunikace na úrovni senzoru/kolektoru – **přenos pouze metadat** na centrální uzel (bez závislosti výhradně na přenosu kompletního SPAN/TAP zrcadleného provozu k centrálnímu uzlu)
- Identifikace neobvyklých komunikačních vzorců a odchylek od baseline

Poznámka k nediskriminaci: Požadavek „lokálního zpracování“ je funkcionálním výkonnostním požadavkem (minimalizace síťové zátěže, ochrana OT provozu). Dodavatel může prokázat jeho splnění jakoukoliv technickou architekturou – edge aplikace, distribuovaný kolektor, hardwarová sonda s lokální analytickou funkcí apod. Overlay architektura závislá výhradně na přenosu kompletního zrcadleného provozu na centrální uzel je z provozních důvodů TDS nevyhovující.

6.3 Detekční scénáře (Use Cases)

OT SIEM musí podporovat definici, konfiguraci, úpravu a rozšiřování detekčních scénářů zaměřených na bezpečnost OT prostředí, přiřaditelných ke konkrétním aktivům nebo zónám.

a) Anomálie v síťové komunikaci

- Neobvyklé směry komunikace (East-West, North-South)
- Nové nebo neočekávané komunikační vazby mezi aktivy

b) Změny v OT aktivech

- Změna konfigurace zařízení
- Změna firmware nebo SW verze
- Náhlý výskyt nového nebo neznámého aktiva v síti

c) Porušení provozního modelu

- Odchylky od naučeného (baseline) provozního chování
- Neobvyklá kombinace protokolů nebo funkčních příkazů

- Nestandardní sekvence příkazů v průmyslových protokolech (neočekávané write/program příkazy na PLC)
- Výskyt IT protokolů v prostředí OT

d) Bezpečnostní události v kontextu OT

- Indikace neoprávněného přístupu (neznámý zdroj, nový server, neznámý uživatel – podpora komunikace s AD)
- Chování odpovídající známým třídám útoků na ICS/OT – mapování na **MITRE ATT&CK for ICS**
- Hodnocení závažnosti dle **CVSS skóre** s kontextem OT aktiva a podporou Threat Intelligence
- Korelace více slabých signálů do jedné bezpečnostní události

6.4 Správa zranitelností

- Automatizovaná detekce CVE pro OT/ICS komponenty s vazbou na NVD a ICS-CERT databáze
- Podpora importu SBOM (Software Bill of Materials)
- Mapování zranitelností na konkrétní reálná aktiva v inventáři

6.5 Integrace s NAC (volitelná)

Řešení musí technicky umožňovat budoucí integraci s Network Access Control (NAC) systémy prostřednictvím standardizovaného API (např. pxGrid nebo ekvivalentní otevřené rozhraní) za účelem dynamické segmentace a prosazení bezpečnostních politik. Tato integrace **není součástí předmětu plnění**.

6.6 Integrace s centrálním IT SIEM (dokumentační povinnost)

- Výstupy detekčních scénářů a bezpečnostní události musí být exportovatelné do externího SIEM ve standardizovaných formátech: **Syslog / CEF / JSON / REST API**
- Řešení musí disponovat **nativním (out-of-box) konektorem nebo technickým add-on modulem** pro platformu **Splunk** nebo odpovídající otevřenou API dokumentací umožňující integraci realizovanou zadavatelem vlastními silami
- Při exportu musí být zachován **OT kontext** (identifikace aktiva, zóna, typ technologie, závažnost v OT kontextu)
- Výstupy musí být využitelné pro SOC workflow: eskalace, korelace, reporting, tvorba pravidel a jejich alertizace / prioritizace
- Dodavatel předá zadavateli veškerou dokumentaci k integraci jako součást předmětu plnění

6.7 Správa a auditovatelnost

- Webové rozhraní pro správu a vizualizaci (bez závislosti na cloudovém přístupu)
- Podpora RBAC (Role-Based Access Control)
- Auditní log s ochranou integrity: detekční pravidla, konfigurace systému, bezpečnostní události
- Reporting souladu s ISA-99/IEC 62443 a NIS2

7 Bezpečnostní a legislativní požadavky

Standard / Předpis	Relevantní požadavek
ISA/IEC 62443-3-3	Systémové bezpečnostní požadavky; podpora Zones & Conduits segmentace; reporting souladu
ISA/IEC 62443-2-1	Bezpečnostní management a provozní procesy
NIS2 / zákon č. 264/2025 Sb	Soulad s požadavky na hlášení incidentů a opatření pro subjekty kritické infrastruktury
Vyhláška č. 409/2025 Sb. (NÚKIB) ISO/IEC 27001	Technická a organizační opatření kybernetické bezpečnosti Rámec pro ISMS dodavatele i provozovatele; pokrývá dodavatelský řetězec
NIST SP 800-82 Rev. 3	Architektura OT monitoringu, pasivní senzorické funkce
MITRE ATT&CK for ICS	Klasifikace a mapování detekčních scénářů
CISA Secure by Design	Principy bezpečného návrhu OT produktů

8 Provozní a rozvojové požadavky

- Řešení musí být **škálovatelné** pro opakované nasazení v dalších ED a OT lokalitách SŽ bez nutnosti změny základní architektury
- Výpadek OT SIEM ani kolektorů **nesmí mít vliv na řídicí OT provoz** (fail-safe design)
- Dodavatel poskytne kompletní **technickou a provozní dokumentaci, které bude jeden z bodů akceptačního protokolu**, odpovídající prostředí kritické infrastruktury (instalační manuál, administrátorský manuál, API dokumentace, dokumentace k offline licenčnímu modelu, release notes)
- Veškerá dokumentace musí být dodána v českém nebo anglickém jazyce

9 Licenční podmínky a model dodávky

- Typ licence: subscription nebo perpetual (dle nabídky uchazeče – zadavatel neomezuje typ licenčního modelu)
- **Podmínky offline aktivace:** Podpora aktivace licencí v prostředí air-gapped
- **Opce rozšíření:** Zadavatel si vyhrazuje právo doobjednat až 20 % licencí za smluvních podmínek bez nového výběrového řízení
- **Přenositelnost:** Licence musí být přenositelné v rámci organizace zadavatele (přemístění na jiný HW / VM)
- **Ukončení smlouvy:** Podmínky pro export dat a zajištění kontinuity provozu při ukončení smlouvy s dodavatelem (viz.exit strategie – dto. „Bezpečné úložiště“)
- **Podmínky maintenance:** Podpora a aktualizace jsou součástí nabídkové ceny po dobu 5 let; po uplynutí musí být možné prodloužení. Softwarová podpora (maintenance), aktualizace, technická asistence a záruka dostupnosti produktu na trhu po dobu **5 let**

10 Hodnotící a kvalifikační kritéria

10.1 Technická kvalifikace dodavatele

- Reference na dodávku (nikoli implementaci) OT/ICS bezpečnostního monitorovacího řešení nebo jeho licencí (energetika, doprava, průmysl, veřejná správa) – min. **1 referenční zakázka v objemu $\geq 500\,000$ Kč bez DPH** za posledních 5 let
- Doklad o partnerském nebo distribučním oprávnění pro dodávané řešení (OEM certifikace nebo distribuční smlouva s výrobcem)

10.2 Hodnotící kritéria (§ 114 ZZVZ)

Doporučená kombinace ceny a kvality:

Kritérium	Váha
Nabídková cena (celková cena za 5 let vč. všech licencí a maintenance)	100 %

11 Ustanovení k nediskriminaci a otevřenosti soutěže

V souladu s § 36 odst. 1 a § 89 odst. 5 zákona č. 134/2016 Sb. (ZZVZ) a judikaturou ÚOHS platí:

1. **Žádný odkaz na konkrétního výrobce:** Žádný požadavek této specifikace neodkazuje na konkrétního výrobce, obchodní název, patent ani typ produktu.
2. **Ekvivalentní technologie:** Tam, kde je uveden příklad technologie nebo rozhraní (IOx, pxGrid, AMQP, SLR, CSSM, DPI apod.), je vždy přípustný funkčně ekvivalentní přístup jiného výrobce.
3. **Kompatibilita se stávající infrastrukturou:** Požadavek na funkcionalitu v prostředí stávající síťové infrastruktury zadavatele je formulován jako **výkonnostní požadavek** (pasivní monitoring, přenos pouze metadat, žádný dopad na OT provoz) – nikoli jako požadavek konkrétní platformy.
4. **Alternativní architektura senzoru:** Overlay architektura s hardwarovou sondou, softwarovým kolektorem nebo jinou distribuovanou architekturou je přípustná, pokud uchazeč prokáže splnění výkonnostních požadavků v kapitolách 4 a 5.
5. **Zero-hardware footprint:** Tento požadavek je interpretován jako minimalizace dodatečného HW nutného pro nasazení v prostředí zadavatele. Uchazeč může využít existující infrastrukturu nebo dodat vlastní HW komponenty – obě varianty jsou přípustné.
6. **Kompatibilita se Splunk SIEM:** Požadavek na integraci je formulován jako podpora standardizovaných formátů (Syslog/CEF/JSON/REST API) nebo existence nativního konektoru – zadavatel integraci realizuje vlastními silami.

12 Přílohy

Příloha D: Cenová tabulka – struktura nabídkové ceny

Uchazeč vyplní všechny položky v níže uvedené struktuře:

Č.	Položka	Počet / Rozsah	Jedn. cena bez DPH (Kč)	Celkem bez DPH (Kč)
1	Softwarová appliance OT SIEM (VM nebo fyzická)	1 ks		
2	Licence senzor – síťový přepínač L2/L3	4 ks		
3	Licence OT endpoint – non-IT aktivum (PLC, RTU, HMI, IED apod.)	250 ks		
4	Podpora a maintenance (5 let, HW SLA 8x5 NBD, SW SLA 24/7)	1 balíček / 5 let		
5	Technická dokumentace (instalační, administrátorský, API manuál)	1 sada		
Celkem bez DPH				
DPH 21 %				
Celkem vč. DPH				

Příloha E: Požadavky na formát exportu do centrálního SIEM

(k doplnění – Splunk HEC endpoint, formát CEF/JSON, autentizační metoda)

Dokument připraven jako technologicky neutrální, výkonnostně orientovaná technická specifikace pro otevřené výběrové řízení v oblasti státní správy. Veškeré požadavky jsou formulovány v souladu s § 36 odst. 1 a § 89 odst. 5 ZZVZ tak, aby nevytvářely neoprávněné překážky hospodářské soutěže a byly otevřeny i pro třetí strany.

**Správa železnic, státní organizace
Správa železniční telematiky
Millennium Plaza, V Celnici 1028/10
110 00 Praha 1**

© 2026