Příloha č. 1

Technická specifikace

Minimální vlastnosti poptávaného SIEM řešení a analyzátoru síťového provozu

Zadavatel požaduje, aby dodavatelem nabízený systém SIEM byl produktem společnosti zařazené dle nezávislého a mezinárodně uznávaného hodnocení jednotlivých bezpečnostních produktů společností Gartner, Inc., Magic Quadrant for Security Information and Event Management do kategorie „Leaders“, minimálně v jednom hodnocení za poslední tři roky hodnocení (tj. za rok 2017, 2018 nebo 2020), a to za účelem získání co nejvyšší kvality dodávaného řešení, minimalizaci možnosti vzniku následných rizik a zaručení stability a udržitelnosti daného řešení..
Řešení musí splňovat minimální technické požadavky (technické podmínky) v níže uvedeném rozsahu.

Požadavky zadavatele jsou uvedeny ve sloupci 1, dodavatel vyplní všechny položky sloupce 2 (např. popisem nabízeného parametru nebo jen slovem „Splňuje“ nebo „Nesplňuje“, pokud by byl popis stejný jako text uvedený ve sloupci 1).

Minimálními technickými požadavky na SIEM HW (sloupec 1)		**Technická specifikace nabízeného zařízení (sloupec 2) Vyplňte: Splňuje/Nesplňuje (pokud je požadováno, doplní dodavatel jak)**
1.	Minimální požadavky na každého z DVOJICE fyzických SIEM serverů Řešení (SIEM) musí být dodáno na HW včetně odpovídajícího rozsahu náležitostí a podpory, musí splňovat požadavky vendora SIEMu, a dále musí splnit tyto minimální požadavky: Server RACK o velikosti max. 2U, min. 2 x 12-ti jádrový procesor, min. 2 GHz, třídy Gold min. 192 GB RAM dostatečná lokální disková kapacita zapojená v RAID6 pro logy a flow pro uchování na min 18 měsíců, požadováno je minimálně 100 TB po odečtení režie RAID. 1 x dual-port síťová karta min 10Gb optický port 1 x quad-port síťová karta min 1Gb ETH RJ-45 Redundantní napájecí zdroj Chlazení stroje zepředu dozadu	Splňuje.

	Servisní management modul pro vzdálenou správu serveru. HW podpora NBD (oprava následující pracovní den v místě objednatele) na 5 let, počítaná od předání dodávky dle smlouvy, se službou ponechání vadného disku v případě jeho výměny.	
2.	Sondy pro lokality {Děčín, Teplice, Most, Chomutov a Litoměřice} Řešení (SIEM) musí být dodáno na HW včetně odpovídajícího rozsahu náležitostí a podpory, musí splňovat požadavky vendora SIEMu, a dále musí splnit tyto minimální požadavky: Zpracování datového toku max 2 Gbps Server RACK o velikosti 1U, min. 1 x 8-mi jádrový procesor, třídy Silver a vyšší min. 32GB RAM min. 2 x 1TB HDD, zapojených v RAID1 Přídavná síťová karta min 2 x 1Gb ETH RJ-45 Redundantní napájecí zdroj HW podpora NBD na 5 let, počítaná od předání dodávky dle smlouvy, se službou ponechání vadného disku v případě jeho výměny.	Splňuje.
3.	Požadavky na 10 SIEM flow sond umístěných ve virtualizaci VMware nebo Hyper-V: Zpracování datového toku min. 1 Gbps Specifikace počtu vCPU Core, RAID a diskového prostoru dodavatele pro každou sondu, uveďte zde.	4vCPU, 16GB RAM a 300 GB diskového prostoru.

Minimálními technickými požadavky na SIEM SW, které zadavatel požaduje **(sloupec 1)**		**Technická specifikace nabízeného zařízení** **(sloupec 2)** **Vyplňte: Splňuje/Nesplňuje (pokud je požadováno, doplní dodavatel jak)**
	Řešení musí být hodnocené v segmentu „leaders“ v Gartner Magic Quadrantu pro SIEM za poslední tři roky hodnocení	Splňuje. IBM QRadar.

	Řešení musí být dodáno ve schématu vysoké dostupnosti, jako fyzické zařízení s SW SIEM v podobě dvouuzlového clusteru a to včetně databáze, operačního systému a jejich případných licencí	Splňuje.
	Každý člen clusteru bude disponovat vlastním úložištěm, které bude nativními prostředky SIEM vzájemné synchronizované.	Splňuje.
	Součástí řešení musí být licence pro patnáct flow sond s funkcí kolektoru. Pět jako fyzické zařízení a deset v podobě virtualizované sondy pro hypervizor VMware nebo Hyper-V. V případě výpadku spojení se SIEMem, musí kolektor pokračovat ve sběru/příjmu událostí/logů, a tyto dočasně lokálně ukládat. Po obnovení spojení musí tyto data dodatečně přeposlat do SIEMu.	Splňuje.
	Management veškerých flow sond musí být přímo součástí jediného rozhraní pro správu SIEM	Splňuje.
	Všechny případné komponenty řešení, např. licence operačního systému, databáze nebo WEB aplikačního serveru a jiné, musí být součástí dodávky SW.	Splňuje.
	Požadujeme podporu a support výrobce na 5 let včetně SW upgrade.	Splňuje.
	Softwarové licence a jejich PN (produktové číselné označení) musí být dostupné v ceníku výrobce	Splňuje.
	Podpora na licence ve všech úrovních, musí být možné zajistit přímo jejich výrobcem, kterého může Zadavatel přímo kontaktovat	Splňuje.
	Požadujeme, aby samostatný formulář pro hlášení kybernetického bezpečnostního incidentu na Národní úřad pro kybernetickou a informační bezpečnost, byl přímo součástí grafického rozhraní produktu	Splňuje.
	Řešení musí být navázáno na národní centrum kybernetické bezpečnosti CSIRT a publikovat v konzoli jím aktuálně uveřejněné hrozby.	Splňuje.

	Podporované protokoly: Syslog, Windows Events Collection (WinRM/ RPC), FTP, S/TP/SCP, SNMP, ODBC/JDBC, CP-LEA, SDEE, log file protokol	Splňuje.
	Bezagentový sběr logů (sběr bez nutnosti instalovat agenta na cílový systém)	Splňuje.
	Licence pro trvalé zpracování 7 500 EPS nebo ekvivalentu 350 GB denně při průměrné velikosti zdrojové události 600 B s možností rozšíření bez nutnosti dodatečného HW, resp. HW upgrade až na dvojnásobek těchto hodnot.	Splňuje.
	Licence pro zpracování 3500 síťových flow za sekundu s možností rozšíření bez nutnosti dodatečného HW, resp. HW upgrade až na dvojnásobek.	Splňuje.
	Součástí bude licence pro rozhraní na skener zranitelností pro minimálně 2000 IP adres.	Splňuje.
	Management scanneru zranitelností musí být přímo součástí jediného rozhraní pro správu SIEM	Splňuje.
	Licence pro neomezený počet zdrojů událostí připojený do SIEM	Splňuje.
	Řešení nebude licenčně omezovat úložnou kapacitou	Splňuje.
	Licence musí umožnit budoucí změnu architektury z All-in-One na distribuovaný systém bez dalších licenčních poplatků.	Splňuje.
	Licence umožňuje dočasné trojnásobné překročení limitu příjmu událostí a síťových flow bez ztráty jejich korelace. Popište, jak řešení splňuje tento požadavek.	Zařízení QRadar SIEM obsahují na svém vstupu buffer o velikosti 5 GB. V případě příjmu velkého množství událostí se tento buffer využije. Takto je možné zpracovat požadované dočasné trojnásobné překročení limitu. https://www.ibm.com/support/pages/qradar-event-and-flow-burst-handling-buffer
	Možnost sběru logů lokálním kolektorem s přeposíláním do SIEM (zejména pro systémy Windows)	Splňuje.

	Centrální management všech komponent a administrativních funkcí ve webovém uživatelském rozhraní. Rozhraní nesmí vyžadovat instalaci dalšího SW na straně uživatelů technologie Java, Flash, apod. a nesmí vyžadovat používání nebo instalaci tlustého klienta.	Splňuje.
	Řešení musí umožňovat definici uživatelských oprávnění pro možnost oddělení přístupu jednotlivých administrátorů k jednotlivým zdrojům logů a toků, jejich skupinám či síťovým segmentům. Přístup je řízen na základě členství ve skupinách Active Directory.	Splňuje.
	Podpora šifrované komunikace mezi zdroji logů a SIEM	Splňuje.
	Integrace s adresářovým systémem (LDAP, Active Directory) pro potřeby autentizace uživatelů. Systém ale musí rovněž umožňovat přihlašování pomocí lokálních účtů (v případě nedostupnosti externích autentizačních mechanismů).	Splňuje.
	Minimální administrace /výběr zařízení ze seznamu od výrobce/pro připojení dalších zdrojů událostí (Windows Active Directory Servers, Windows IIS and Exchange Servers, Windows Standalone Servers, UNIX and Linux Servers, DNS and DHCP Servers, Database Servers, Proxy Servers, Firewalls, IDS, IPS, and DAM, směrovače a přepínače)	Splňuje.
	Log Management s minimální postimplementační administrací (agregace událostí dle typů, analýza, vyhodnocování) pro případy jako je zavedení nového zdroje událostí, nastavení pravidel pro sběr dat a archiv událostí	Splňuje.
	Automatické připojení a samoučící rozpoznání připojených zařízení.	Splňuje.
	Podpora sběru síťových toků a automatická identifikace (NetFlow, JFLow, Sflow) z infrastrukturních prvků (switche, routery, NetFlow sondy)	Splňuje.
	Řešení musí umožňovat automatické aktualizace výrobcem minimálně v rozsahu 1 x měsíčně. Tato funkcionalita je součástí produktové podpory výrobce.	Splňuje.

	Vestavěný reporting podle standardu ISO27000:2013.	Splňuje.
	Vestavěný modul výrobce pro identifikaci a vyhodnocení obsahu spadající pod GDPR	Splňuje.
	Vestavěný modul výrobce pro Analýzu chování uživatelů na základě mechanismů strojového učení.	Splňuje.
	Poskytování automatického backup/recovery procesu	Splňuje.
	Poskytování interní kontroly stavu zařízení (healthcheck) a upozornění uživatele v případě problému	Splňuje.
	Poskytování analytické a korelačních funkcí bez dalších zásahů a činností (out-of-the-box)	Splňuje.
	Možnost rozšíření výběrů o uživatelské položky z obsahu logů	Splňuje.
	Požadujeme funkcionalitu hromadného importu o zdrojích logů	Splňuje.
	Požadujeme zajištění integrity nasbíraných dat.	QRadar SIEM umožňuje pomocí Flow Log Hashing: Yes Event Log Hashing: Yes HMAC Encryption: Yes HMAC Key: Verify HMAC Key: Hashing Algorithm: HMAC-MD5
	Schopnost uchovat nasbíraná data nejméně po dobu 18 měsíců, aniž by to vyžadovalo použití externích paměťových zařízení.	Splňuje.
	Požadujeme možnost nastavit více filtrů retenčních politik pro různé zdroje dat	Splňuje.
	Near-real-time analýza událostí	Splňuje.
	Analýza dlouhodobých trendů událostí	Splňuje.
	Pokročilé "drill-down" dohledávání v případě potřeby	Splňuje.

	Možnost agregace události z logů i podle položek které nejsou standardně zahrnuty v řešení	Splňuje.
	Sběr textových logů ze souborů	Splňuje.
	Sběr logů z databází pomocí JDBC/ODBC	Splňuje.
	Vyhledávací rozhraní systému správy logů musí nabízet možnost rozčlenění vyhledaných dat až na detailní úroveň, IP adresa, typ události, protokol, port atd.	Splňuje.
	Vyhledávací rozhraní systému správy logů musí poskytovat podporu jak pro zadání dotazu s použitím Booleovy logiky, tak pro zadání regulárními výrazy	Splňuje.
	Poskytování alertů na detekované anomálie, změny chování sítě a změny v generování logů a událostí	Splňuje.
	Kombinované hledání v indexovaných i neindexovaných datech v systému správy logů s použitím regulárních výrazů a fulltextového vyhledávání v nestrukturovaném textu současně	Splňuje.
	Korelační modul musí poskytovat již po instalaci (out-of-the-box) metody korelačních pravidel, která automatizují zjišťování incidentů a související workflow procesy	Splňuje.
	Korelace mezi zařízeními již po instalaci (out-of-the-box). Zjišťování chyb autentizace, chování perimetru a výskytu červů bez potřeby specifikovat typy sledovaných zařízení	Splňuje.
	Korelační systém musí využívat i externí on-line reputační databázi výrobce pro vyhodnocování bezpečnostních rizik.	Splňuje.
	Požadujeme automatické vytváření souhrnných informací o bezpečnostních hrozbách na základě korelace dílčích událostí	Splňuje.
	Systém musí být schopen využít detekované anomálie a informace ze sítě pro korelaci s logy do jednotných incidentů, pro zpřesnění kontextu a snížení false-positives	Splňuje.

	Řešení musí poskytnout alerting vycházející z detekovaných bezpečnostních hrozeb od monitorovaných zařízení	Splňuje.
	Požadujeme zpracování a vyhodnocení identifikovaných hrozeb formou jednoduchého workflow	Splňuje.
	Alerting založený na vypozorovaných anomáliích a změnách chování sítě (analýza síťových toků). Řešení musí poskytovat NBAD (Network Behavior Anomaly Detection) funkcionalitu	Splňuje.
	Požadujeme schopnost samostatného "učení" normálního stavu. Podle nastavené bezpečnostní politiky pak reagovat na vznik skupinových nebo kontextuálních anomálií.	Splňuje.
	Řešení musí poskytnout alerting porušení bezpečnostních pravidel, založený na stanovené bezpečnostní politice.	Splňuje.
	Vykonávání akci v závislosti na přijatém logu jako např. zaslat email, notifikaci nebo spustit předem definovaný skript	Splňuje.
	Schopnost pracovat s IP geolokacemi (botnet kanály atp.)	Splňuje.
	Generování alertu při výpadku logů z konkrétního zařízení	Splňuje.
	Vestavěný mechanismus na klasifikaci systémů podle typu (např. mail server vs. databázový server)	Splňuje.
	Vyhodnocení chybějících sekvencí (např. služba přestala běžet)	Splňuje.
	Schopnost korelovat události DHCP, VPN a Active Directory a sledovat průběh uživatelské relace (session) v rámci celé instituce (přesná identifikace uživatele)	Splňuje.
	Schopnost korelovat data o událostech se statickými a dynamickými seznamy označujícími položky, které mají či nemají být v síti povoleny	Splňuje.

	Poskytování rozhraní pro reporting, pomocí kterého lze vytvářet nové sestavy bez nutnosti sestavovat SQL dotazy	Splňuje.
	Požadujeme pravidelnou, plánovanou tvorbu takových reportů minimálně ve formátech PDF a CSV.	Splňuje.
	Nezměněná funkcionalita reportingu i při změně nebo náhradě některé technologie jako např. firewallu nebo IDS	Splňuje.
	Řešení musí obsahovat nativní podporu vysoké dostupnosti (HA) bez rozšiřujících komponent/software třetích stran.	Splňuje.
	Nabízené řešení musí poskytovat automatické aktualizace řešení, bez pomoci profesionálních služeb výrobce. Tato funkcionalita je součástí produktové podpory výrobce.	Splňuje.
	Nabízené řešení musí zaznamenávat činnost uživatele, udržovat informaci o jeho reputaci v čase a to i v případě, že tato informace není bezprostředně obsažena ve všech událostech.	Splňuje.
	Řešení musí nabízet přístup k datům skrze otevřené REST API pro integraci s dalšími systémy.	Splňuje.
	Řešení musí být navrženo tak, aby bylo schopno pracovat s interními překrývajícími se rozsahy adres spolu se síťovými toky, událostmi a zařízeními v síti	Splňuje.
	Řešení musí uchovávat logy i flows jak v normalizovaném formátu, tak i „raw“ formátu.	Splňuje.
	Řešení nebude licenčně omezeno počtem používaných korelačních pravidel.	Splňuje.
	Řešení nebude licenčně omezeno počtem generovaných reportů	Splňuje.
	Řešení nebude licenčně omezeno počtem současně připojených administrátorů či operátorů.	Splňuje.
	Řešení musí být schopno konsolidovat výsledky z několika řešení, jako jsou vulnerability scannery, risk management nástroje a externí vstupy bezpečnostních informací z různých zdrojů.	Splňuje.

	Nabízené řešení musí umět zvyšovat/snižovat riziko na základě kontextu (klasifikace zařízení, subnetu, parametru…)	K úpravě rizikovosti s využitím kontextu se používá referenčních množin. Do těch se ukládají zde zmíněné klasifikace, které se promítají do hodnotících pravidel.
	Řešení musí obsahovat funkcionalitu pro výměnu standardizovaných informací informačně bezpečnostního charakteru, jako jsou STIX nebo TAXII.	Splňuje.
	Řešení musí nabízet bezpečnostní informace jako je IP Reputation feed, botnety, zdroje malwaru apod., které jsou pravidelně aktualizované a jsou korelované v reálném čase se všemi událostmi. Popište, jaké zdroje nabízené řešení využívá a jak je implementováno v korelačních pravidlech.	Splňuje.

Systém pro analýzu síťového provozu, který okamžitě identifikuje bezpečnostní události a který splňuje Klíčové minimální požadavky uvedené níže.

Nabízená technologie musí být určená pro český trh. HW a SW licence a jejich PN (produktové číselné označení) musí být dostupné přímo v oficiálním ceníku výrobce pro český trh. Podpora na licence ve všech úrovních musí umožnit, aby Zadavatel přímo kontaktoval výrobce.

Při definici technických požadavků jsou všechny uvedené požadavky závazné. Je-li definice požadavku „umožňuje, lze, je možné, možnost, …“ je uvedený parametr závazný a požadovaná funkcionalita musí být v rámci Systému dodána/naimplementována a případně licencována.

Řešení musí splňovat VŠECHNY níže uvedené požadavky:

Minimálními technickými požadavky na zařízení pro monitoring a analýzu síťového provozu, které zadavatel požaduje (sloupec 1)		**Technická specifikace nabízeného zařízení (sloupec 2) Vyplňte: Splňuje/Nesplňuje (pokud je požadováno, doplní dodavatel jak)**
1.	Řešení odděluje komponenty sondy a kolektoru pro budoucí distribuovaného zapojení více sond.	Splňuje.
	Systém pro analýzu síťového provozu Systém složený z hardwarových zařízení musí monitorovat síťovou aktivitu v reálném čase a identifikovat potenciální kybernetické hrozby,	Splňuje.

	bezpečnostní rizika a anomální chování a musí o nich v reálném čase vytvářet upozornění. Systém zajišťuje detailní viditelnost do síťové komunikace s drill down prokliky na veškerá uložená data. Všechny komponenty systému musí být instalované v interním prostředí zadavatele („on premise“) a **použití externích komponent nebo cloudových služeb se nepřipouští**.	
	Analýza plného síťového provozu Dodaný systém musí analyzovat síť na základě zrcadleného síťového provozu a zároveň bez potřeby nasazovat agenty na koncové stanice nebo další zařízení v síti. Systém musí být schopen získávat data zrcadlené komunikace ze SPAN portů a síťových TAPů. Systém je zcela pasivní vzhledem k monitorovanému provozu, monitorovaný provoz přes něj neprochází.	Splňuje.
	Rozhraní Přehledný dashboard s okamžitou indikací problémů a top statistik.	Splňuje.
	Analýza protokolů typu NetFlow Dodaný systém musí analyzovat síť na základě zpracování statistických protokolů typu NetFlow v5, NetFlow v9, IPFIX, NetStream a případně dalších.	Splňuje.
	Zaznamenávání provozu Je požadováno zaznamenávání síťového provozu minimálně na základě parametrů: cílová a zdrojová IP/MAC adresa, podsíť, využitý protokol, IPv4 nebo IPv6.	Splňuje.
	Integrace se SIEM Je požadován simultánní export NetFlow protokolu do řešení SIEM. Dále je požadována integrace prostřednictvím minimálně syslog.	Splňuje.
	Kontextuální informace Systém musí být schopen pro každé zařízení získávat, vizualizovat a integrovat v jednotném grafickém rozhraní kontextuální informace: • Hostname zařízení a jeho historie na základě zpracování relevantních dat z DNS provozu a Active Directory	Splňuje.

	• IP geolokace	
	Požadavky pro pokrytí sítě Je požadován HW datový kolektor a sensor (sonda, proba) pro zpracování síťové komunikace o celkovém objemu do 10.000 hostů v síti. Požadované rozhraní pro sběr dat je min. 2x 10GE, optické porty. Dále je vyžadován alespoň 1x 1GE pro management port. Připouští se maximálně dvojice Rack mount zařízení, každé o výšce maximálně 2U. HOT SWAP disky, HW RAID včetně smart detekce.	Splňuje.
	Ukládání dat Vestavěný kolektor pro dočasné ukládání flow statistik po dobu 18 měsíců (zajištění redundance).	Splňuje.
	Správa Zabezpečená vzdálená správa, dohled a konfigurace – SSH, HTTPS	Splňuje.
	Monitorování zařízení, segmentů sítě a využívaných síťových služeb Dodaný systém musí přibližně identifikovat všechna zařízení připojená do sítě včetně koncových zařízení, serverů, IoT zařízení apod. Zároveň musí být systém schopen identifikovat změny v síti. Systém musí umožnit zaslat alert při výskytu nového zařízení (obecně assetu).	Splňuje.
	Monitorování komunikace Požadován je modul pro analýzu sítě: vytváření dlouhodobých grafů a přehledů o komunikaci na síti s různými typy pohledů rozdělených do kategorií podle objemu (počet přenesených bytů, toků, paketů), IP provozu (TCP, UDP, ICMP, ostatní) nebo protokolu (http, IMAP, SSH), SSL a DNS provozu, VoIP statistik, SMB/CIFS, DHCP a e-mail provozu.	Splňuje.
	Vyhledávání, filtrování a vizualizace všech dat Zobrazení provozu a jeho adekvátní hloubková analýza. Systém musí být schopen okamžitého vyhledávání a vizualizace pro forenzní analýzu a podporu threat hunting bez zvláštního dotazovacího jazyka a bez	Splňuje.

	hlubokých znalostí konkrétních komunikačních protokolů.	
	Monitorování http komunikace Podpora pro příjem a analýzu HTTP provozu – včetně položek typu URL a hostname.	Splňuje.
	Samostatné učení a detekce anomálií NBA Systém musí používat matematické metody samostatného učení (např. strojové učení) pro analýzu síťové aktivity, musí vytvářet a v čase automaticky modifikovat modely chování na základě běžného chování jednotlivých zařízení a na nich provozovaných služeb. Systém musí mít schopnost na základě modelu daného zařízení a jeho služeb identifikovat nestandardní síťové chování.	Splňuje.
	Identifikace neznámých hrozeb, podezřelých chování na síti a porušení politik Systém musí být schopen detekovat neznámé hrozby, které nelze identifikovat prostřednictvím detekčních signatur, jako jsou trojské koně, botnety apod. Zejména musí být identifikovány tyto příznaky potenciálně škodlivého chování: • průzkumné aktivity v síti, • potenciální úniky dat, • detekce podezřelého strojového chování, které nevytvářejí lidští uživatelé sítě, • detekce příznaků těžení kryptoměn, • útoky hrubou silou a enumerace dat.	Splňuje.
	Behaviorální analýza Detekce nežádoucích vzorů chování na síti (útoky, anomálie datového provozu, nežádoucí aplikace, detekce virů a botnetů ve vnitřní síti, detekce odchozího spamu, provozních problémů). Detekce anomálií vzhledem k dlouhodobému profilu chování zařízení na síti.	Splňuje.
	Události a false-positives Systém generuje události s možností identifikace neplatných událostí pomocí mechanismu false-positives. Taková událost se při příštím výskytu potlačí.	Splňuje.

	Ověřování Podpora autentizace vůči LDAP, včetně podpory RBAC (přiřazení úrovně oprávnění na základě členství uživatele v konkrétní LDAP skupině).	Splňuje.
	Reporting Vytváření dlouhodobých grafů a přehledů s různými typy pohledů do kategorií podle objemu (počet přenesených bytů, toků, paketů), IP provozu (TCP, UDC, ICMP, ostatní) nebo protokolu (http, IMAP, SSH). Generování statistik a podobných výpisů nad volitelnými časovými intervaly.	Splňuje.
	Reporting Výpis tzv. top N statistiky podle různých kritérií (počet přenesených bytů, paketů, toků atd.) umožňující vypsat nejaktivnější či anomální počítače podílející se na síťovém provozu.	Splňuje.
	Možnost automatizovaného reportingu Možnost vytváření automatizovaných manažerských reportů včetně možnosti exportu do PDF a CSV formátu. Automatické zasílání reportů emailem (reporty v českém a anglickém jazyce).	Splňuje.
	Automatické bezpečnostní hlášení (alerty) Notifikace na základě překročení prahových hodnot definovaných při implementaci či v průběhu provozu. Systém musí být schopen upozorňovat uživatele prostřednictvím minimálně emailu a logu o: • všech identifikovaných událostech, • událostech filtrovaných minimálně dle IP a MAC adresy, podsítě, závažnosti události, kategorie události, země, uživatele, síťové služby, čísla portu, provozu do/z internetu.	Splňuje.

Součástí dodávky budou dále tyto služby:

Zpracování detailní analýzy a prováděcího projektu nejpozději do 6 týdnů ode dne účinnosti smlouvy:

- Detailní analýza a prováděcí projekt, budou zpracovány do jednoho dokumentu
- Prováděcí projekt bude obsahovat podrobný popis architektury a specifikace rozsahu realizace všech částí předmětu plnění. Konkrétně:
    - Doporučení pro logování
        - Doporučený obsah logovacích událostí a síťových toků
        - Způsob záznamu a doručení logovacích událostí a flow
        - Síťové toky
        - Požadavky na součinnost Zadavatele a třetích stran
    - Architektura SIEM v prostředí Zadavatele
    - SIEM software
        - Nasazení a adresace
        - Popis hardware
        - Popis software

Požadavky na komunikaci systému SIEM do Internetu

- Behaviorální analýza uživatelů
- Konfigurace systému SIEM
- Behaviorální analýza uživatelů
- Konfigurace systému SIEM
    - Klasifikace zdrojů
    - Síťové rozsahy
    - Korelační pravidla
    - Návrh Use-Cases
    - Politika hesel
    - Profily a role
    - Autentizace a autorizace uživatelů
    - Uživatelské a servisní účty
    - Notifikace
    - Retenční politiky
    - Integrita uložených logovacích událostí a flow
    - Pohledy v konzoli
    - Nastavení modulu a formuláře pro hlášení kybernetického bezpečnostního incidentu NÚKIB
    - Nastavení modulu načítání hrozeb z českého CSIRT
    - Reporting, minimálně dle ISO27000:2013
    - SIEM Assety a jejich naplnění
    - Napojení na SOC Uchazeče
    - Monitoring
    - Zálohování
- Popis Integrace jednotlivých připojených systémů do SIEM

  - Návrh akceptačních kritérií a testů, včetně akceptačního protokolu pro všechny dodávané části předmětu plnění. Zadavatel na základě návrhů akceptačních kritérií a testů jednotlivých dodavatelů, vypracuje jednotné akceptační kritéria a testy.
  - Návrh monitoringu, zálohování a obnovy všech částí předmětu plnění.
  - Časový harmonogram realizace.
  - Návrh osnovy školení.
- Dokument analýzy a prováděcího projektu bude vypracován v písemné i elektronické editovatelné podobě, ve formátu MS Word/Excel.

Implementace na základě prováděcího projektu

- kompletní dodávku implementačních služeb SIEM, jeho instalaci a konfiguraci v systémovém prostředí zadavatele pro informační systémy definované v prováděcím projektu a související infrastrukturu. Zejména se jedná o:
  - Instalace SIEM a jeho komponent do prostředí
  - Nastavení LogManagementu, včetně vývoje parserů.

    Pozn.: Vlastní schopnost aplikace logovat zajišťuje Zadavatel.
  - Nastavení Flow
  - Nastavení retence dat
  - Nastavení korelačních pravidel s využitím framework MITRE ATT&CK
  - Nastavení modulu napojení na český CSIRT
  - FNastavení modulu pro hlášení kybernetického bezpečnostního incidentu NÚKIB
  - Nastavení modulu User Behavior Analytics
  - Nastavení importu aktiv z Active Directory do databáze Assetů
  - Nastavení use-cases
  - Nastavení všech principů a zásad uvedených v analýze a prováděcím projektu
  - Ladění False-positives Alarms
- Nastavení autorizace a oprávnění
- Vytvoření Dasboard profilů
- Nastavení reportingu

Zátěžové testy, Akceptační a bezpečnostní testy

Zkušební provoz 1 měsíc zakončení zátěžovými testy, akceptačními a bezpečnostními testy.

Školení v rozsahu:

- 3 dny x 8 hodin, pro všechny osoby nominované Zadavatelem
- školí se v místě Zadavatele, který zajistí i prostory a prezentační techniku
- struktura a rozsah školení bude součástí prováděcího projektu
- dodavatel musí po absolvování školení připojit standardní zdroj a vytvořit či upravit pravidlo

Vypracování dokumentace v rozsahu:

- Administrátorská příručka SIEM v češtině
- Uživatelská příručka SIEM v češtině
- Dokumentace konečného provedení v prostředí Zadavatele v češtině
- Provozní a bezpečnostní dokumentace zahrnující doporučení pro údržbu a zálohování, postupy obnovy v případě havárie apod. (může být součástí administrátorské příručky)
- Školící dokumentace v češtině
- Veškerá dokumentace bude vypracována v písemné i elektronické editovatelné podobě, ve formátu MS Word/Excel
- Součástí dokumentace je i dokumentace výrobce dodávaných produktů, která musí být minimálně dostupná na webových stránkách

Součástí ročního paušálu je následující objem služeb

Roční cena služby servisní podpory:

Linka zákaznické podpory (hotline) pro předmět plnění bude dosažitelná prostřednictvím internetového portálu, e-mailu a telefonu. Požadavek o podporu bude realizován pracovníky Zadavatele, kteří v případě výskytu problému kontaktují linku zákaznické podpory a následně pracují dle instrukcí.

Linka zákaznické podpory (Helpdesk):

[redacted]

Dodavatel zajistí služby zajišťující rutinní provoz systému:

Provoz služby zákaznické podpory (helpdesk) pro zadávání požadavků a provozních závad předmětu plnění s garantovanou dostupností služby v pracovní dny od 8:00 do 17:00 hod.

Reakční doby pro řešení požadavků jsou uvedeny v následující tabulce.

	A: Kritická závada (nefunkční systém) **Kybernetický bezpečnostní incident**	**B: Méně závažná vada**	**C: Závada neohrožující funkčnost, návrh na změnu**
Zahájení řešení požadavku	Do 4 pracovních hodin, v pracovní dny od nahlášení požadavku.	Do 8 pracovních hodin, v pracovní dny od nahlášení požadavku.	Do 5 pracovních dnů, v pracovní dny od nahlášení požadavku.
Zprovoznění systému, nebo informace o postupu řešení	Do 24 pracovních hodin, v pracovní dny od nahlášení požadavku.	Do 5 pracovních dnů, v pracovní dny od nahlášení požadavku.	Do 10 pracovních dnů, v pracovní dny od zapsání nahlášení požadavku.

Úplné vyřešení požadavku	Do 3 pracovních dnů, v pracovní dny od nahlášení požadavku.	Do 10 pracovních dnů, v pracovní dny od nahlášení požadavku.	Do 30 pracovních dnů, v pracovní dny od nahlášení požadavku.

Roční cena služby bezpečnostního dohledu:

- Poskytování služeb bezpečnostního dohledu, v rozsahu 4 ČD měsíčně, který bude zajišťovat níže uvedené činnosti týkající se všech lokalit:
  - Obsluha kontaktního místa a sledování kontinuity SIEM
  - Proaktivní ověření a analýza detekovaných kybernetických bezpečnostních událostí
  - Průběžné doplňování znalostní báze o monitorovaných zařízeních
  - Ověření a analýza detekovaných bezpečnostních událostí
  - Označování falešně pozitivních událostí a jejich eliminace
  - Reportování identifikovaných bezpečnostních incidentů a jejich interpretace
  - Proaktivní reportování závažných a kritických incidentů
  - Doporučení vzhledem k interpretaci incidentů
  - Asistence při realizaci doporučení
  - Tvorba měsíčního reportu o poskytované službě

Roční cena služby aplikační podpory:

- Poskytování HotLine a pravidelných upgrade a provádění pravidelných profylaktických prohlídek (vyřizování požadavků specialistou na základě požadavků objednatele) bude minimálně v rozsahu 12 hodin měsíčně.

Pozn.: Jeden ČD je 8 člověkohodin, 1 člověkohodina je jedna hodina práce

Preferuje se bez-agentový sběr logů, ale připouští se i nasazení agenta pro Windows systém. Bez-agentový sběr logů (sběr bez nutnosti instalovat agenta na cílový systém).

- Podporované protokoly: Syslog, Windows Events Collection (WinRM/ RPC), FTP, S/TP/SCP, SNMP, ODBC/JDBC, CP-LEA, SDEE, log file protokol

- Možnost sběru logů lokálním kolektorem s přeposíláním do SIEM (zejména pro systémy Windows)

Minimální administrace /výběr zařízení ze seznamu od výrobce/pro připojení dalších zdrojů událostí: (Windows Active Directory Servers, Windows IIS and Exchange Servers, Windows Standalone Servers, UNIX and Linux Servers, DNS and DHCP Servers, Database Servers, Proxy Servers, Firewalls, IDS, IPS, and DAM, směrovače a přepínače).

Požadavky na předmět plnění uvedené v tomto dokumentu jsou závazné, jejich nedodržení bude považováno za nesplnění zadávacích podmínek s následkem vyloučení dodavatele z účasti v zadávacím řízení.

Dodavatel prohlašuje, že jím nabízené plnění splňuje všechny požadavky uvedené v této Příloze č. 3 Technická specifikace:

V Praze,

Za společnost AUTOCONT a.s.

[redacted]

[redacted]

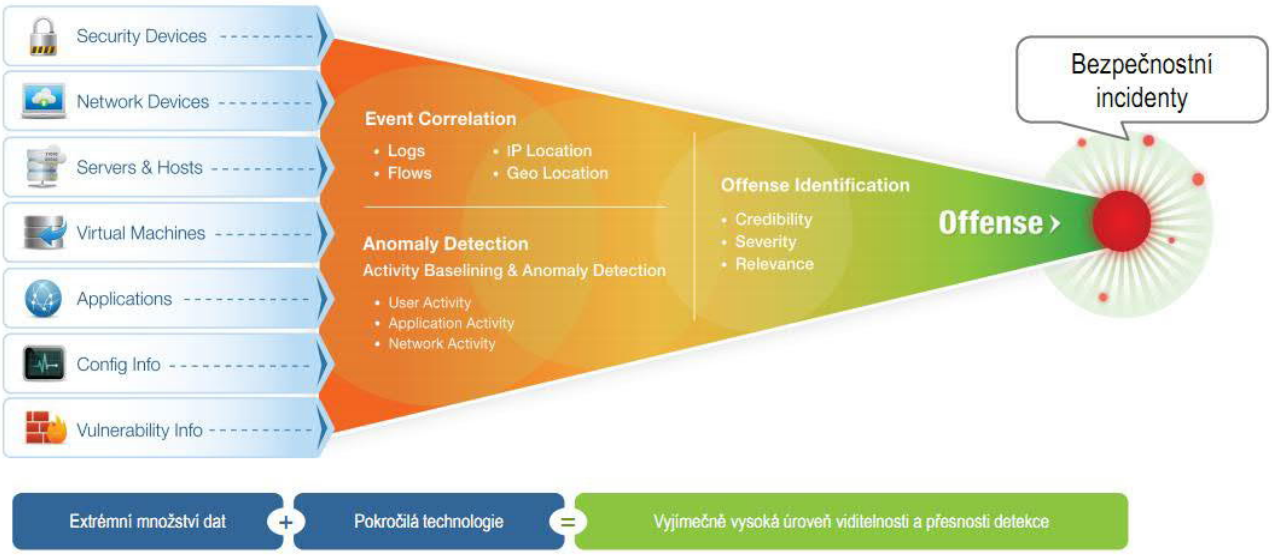
Osoba oprávněná jednat jménem či za dodavatele (pozice, titul, jméno, příjmení)

[redacted]

Příloha č. 2

Popis řešení a licenční podmínky

[redacted]



Zařízení QRadar SIEM tvoří škálovatelná řešení, která jsou již po instalaci předkonfigurována a určena k co nejrychlejšímu nasazení v prostředí zákazníka. Dodávají se v podobě licence, kterou je možné nasadit na appliance (HW společně s OS a QRadar SW – výrobce Lenovo a DELL), jakýkoliv serverový fyzický nebo virtualizovaný HW splňující minimální parametry. Zařízení jsou buď typu All-in-One, kdy nevyžadují žádné další QRadar licence nebo jako jednotlivé komponenty pro stavbu distribuovaných QRadar infrastruktur (Console, Processor, Collector). Systém disponuje všemi charakteristickými komponentami dnešních SIEM (Security Information and Event Management) systémů. Jedná se o sběr, normalizaci, uložení, indexaci, korelaci, identifikaci hrozeb, alerting, reporting a onLine prezentaci bezpečnostních událostí. Vše v prostředí jednotné management konzole.

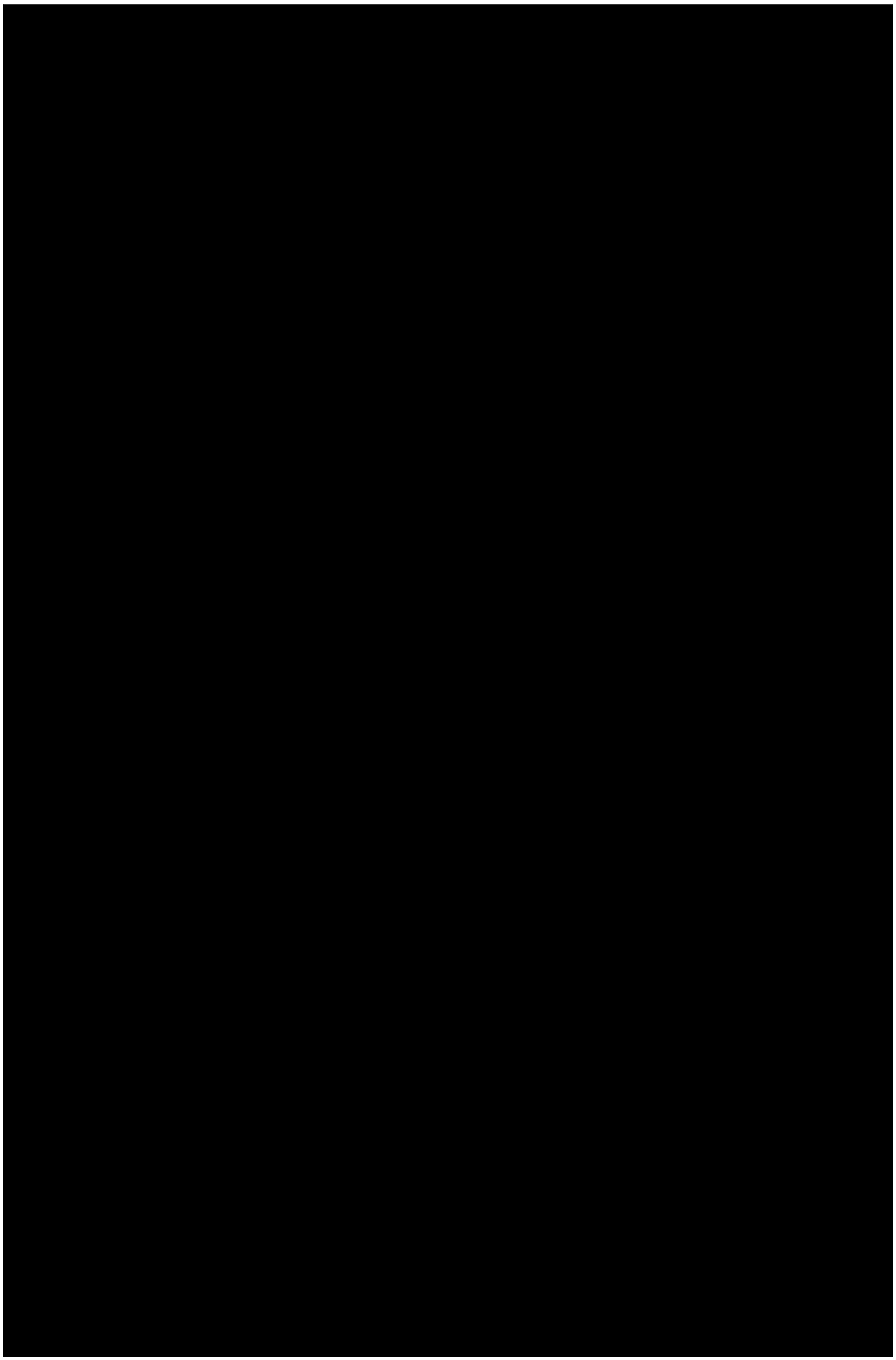
[redacted]

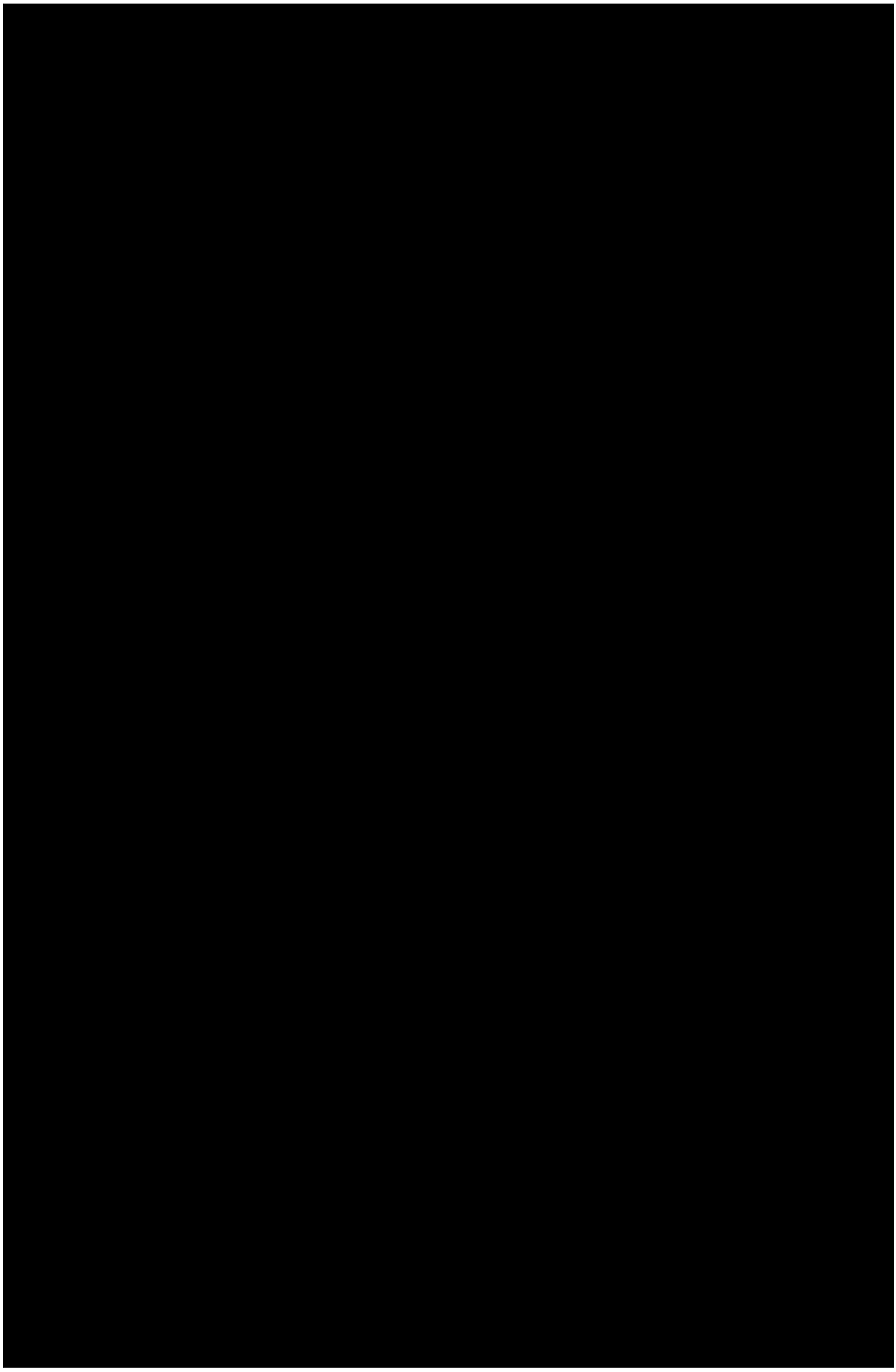
Bližší technická specifikace nabízeného řešení

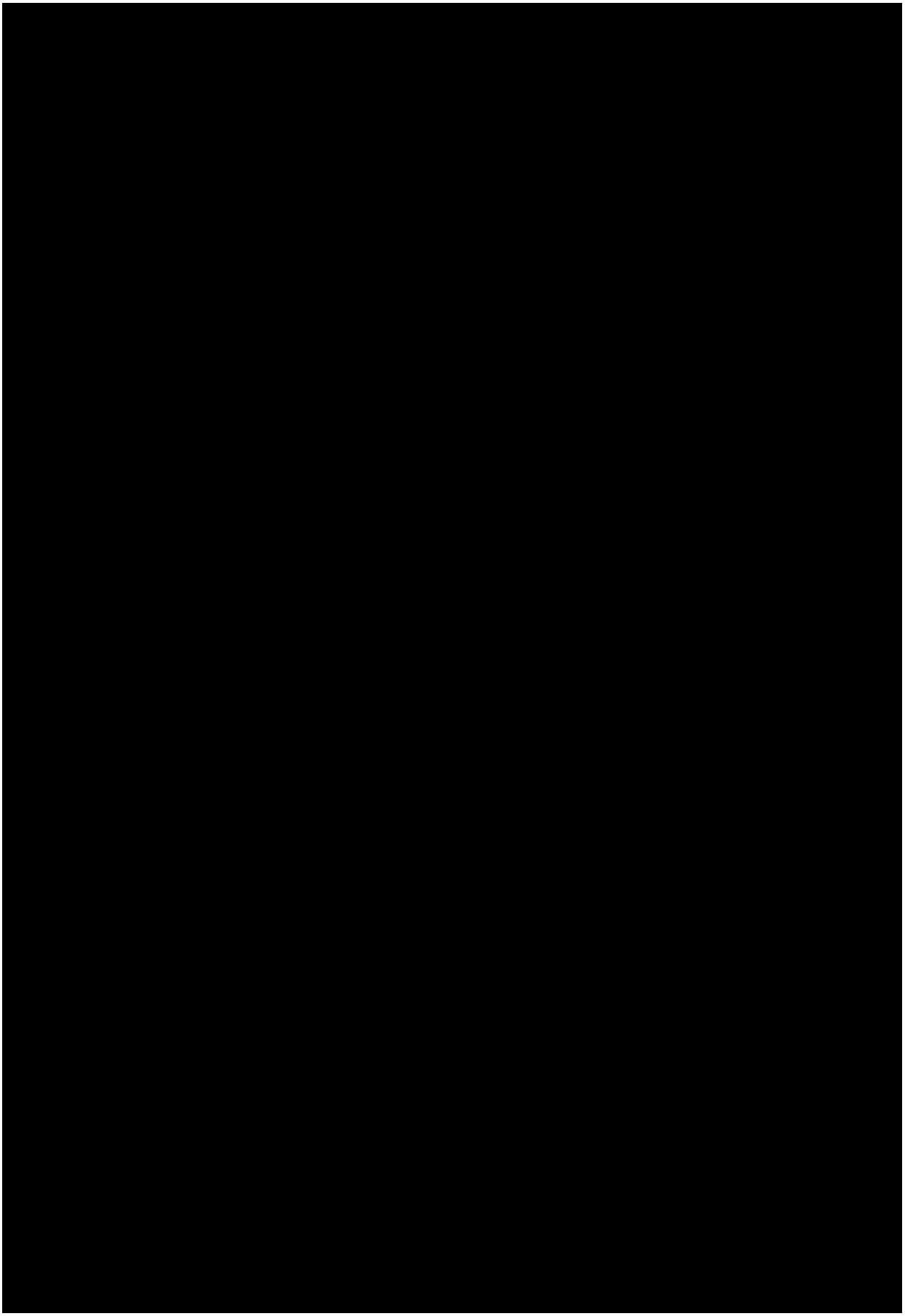
[redacted]

Navržené SIEM řešení splňuje všechny TECHNICKÉ požadavky Zadávací Dokumentace

HW a SW Licence







Příloha č. 3

Realizační tým Poskytovatele

Členové realitačního týmu splňují požadavky uvedené v Zadávací dokumentace

Člen realizačního týmu	Kontaktní údaje
Projektový manažer	[redacted]
Architekt kybernetické bezpečnosti	
Specialista na implementaci SIEM č. 1	
Specialista na implementaci SIEM č. 2	
Specialista kybernetické bezpečnosti	
Specialista na implementaci Vulnerability Managementu	

Příloha č. 4

Oprávněné osoby

Za Objednatele:

ve věcech obchodních:

Jméno a příjmení	[redacted]
Adresa	
E-mail	
Telefon	

ve věcech technických:

Jméno a příjmení	[redacted]
Adresa	
E-mail	
Telefon	

Za Poskytovatele:

ve věcech smluvních:

Jméno a příjmení	[redacted]
Adresa	
E-mail	
Telefon	

ve věcech obchodních:

Jméno a příjmení	[redacted]
Adresa	
E-mail	
Telefon	

ve věcech technických:

Jméno a příjmení	[redacted]
Adresa	
E-mail	
Telefon	

Příloha č. 5

Seznam poddodavatelů

1)

Název:	x
Sídlo:	x
Právní forma:	x
Identifikační číslo:	x
Rozsah plnění Smlouvy:	x

Příloha č. 6

Zadávací dokumentace

Krajská zdravotní, a.s.
Sociální péče 3316/12A
401 13 Ústí nad Labem
Tel.: +420 477 111 111
Fax: +420 477 114 900
e-mail: sekretariat@kzcr.eu

Krajská zdravotní, a.s.

ZADÁVACÍ DOKUMENTACE

pro nadlimitní veřejnou zakázku na dodávky zadávanou v otevřeném řízení
dle § 56 a násl. zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů.

Název veřejné zakázky

„Dodávka SIEM systému včetně systému pro analýzu síťového provozu“

Zadavatel veřejné zakázky:

Krajská zdravotní, a.s.
se sídlem Sociální péče 3316/12A
400 11 Ústí nad Labem, IČO: 25488627, zapsaná v obchodním rejstříku vedeném Krajským soudem v Ústí nad Labem pod spisovou značkou B 1550

Zastoupená: MUDr. Petrem Malým, MBA, generálním ředitelem

Tato zadávací dokumentace je vypracována jako podklad pro otevřené zadávací řízení nadlimitní veřejné zakázky dle § 56 a násl. zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „ZZVZ“).

Pokud dojde k rozporu mezi údaji uvedenými v textové části zadávací dokumentace a údaji uvedenými v oznámení o zahájení zadávacího řízení, platí údaje uvedené v oznámení o zahájení zadávacího řízení.

1 Identifikační údaje zadavatele

Název zadavatele:	Krajská zdravotní, a.s.
Zadavatel ve smyslu ZZVZ:	jiná právnická osoba, dle § 4 odst. 1 písm. e)
Právní forma:	akciová společnost
IČO:	25488627
DIČ:	CZ25488627
Sídlo zadavatele:	Sociální péče 3316/12A, 400 11 Ústí nad Labem
Osoba oprávněná zastupovat:	[redacted]
Kontaktní osoba zadavatele:	
Elektronický profil zadavatele:	E-ZAK na adrese https://zakazky.kzcr.eu/

Komunikace mezi zadavatelem a dodavatelem se řídí § 211 ZZVZ.

Krajská zdravotní, a.s.

Krajská zdravotní, a.s.
Sociální péče 3316/12A
401 13 Ústí nad Labem
Tel.: +420 477 111 111
Fax: +420 477 114 900
e-mail: sekretariat@kzcr.eu

2 Identifikační údaje dodavatele

Dodavatel je povinen uvést v nabídce v souladu s ustanovením § 103 odst. 1 ZZVZ a v návaznosti na ustanovení § 28 odst. 1 písm. g) ZZVZ své identifikační údaje takto:

Obchodní firma nebo název:
Právní forma:
IČO a DIČ:
Sídlo:

Dodavatel v nabídce dále uvede:
Kontaktní osoba dodavatele:
Telefon, e-mail:

3 Vymezení plnění veřejné zakázky

Účel veřejné zakázky

Účelem této nadlimitní veřejné zakázky zadávané v otevřeném řízení dle § 56 a násl. ZZVZ je pořízení systému pro sběr, identifikaci a řešení kybernetických bezpečnostních incidentů.

Předmět veřejné zakázky

Předmětem této veřejné zakázky je dodávka systému SIEM (Security Information and Event Management - bezpečnostní informace a správa událostí), tj. dodávka systému pro detekci a vyhodnocování kybernetických bezpečnostních incidentů a analýzu síťového provozu zadavatele.

Předmětem plnění je dále dodávka hardware, zejména 2 „fyzických" SIEM serverů, sond pro lokality Děčín, Teplice, Most, Chomutov a Litoměřice, a 10 SIEM flow sond.

Zadavatel požaduje poskytnutí veškerých nezbytných licencí k řádnému užívání dodaného systému SIEM, tj. k řádnému užívání předmětu plnění veřejné zakázky.

Dodavatel v nabídce specifikuje název, počet a licenční podmínky ke všem nutným licencím, dále pak uvede licenční politiku, pravidla pro přidělení a případně změny v počtu licencí, typy a verze licencí. Veškeré dodávané licence budou převedeny do vlastnictví zadavatele.

Minimální požadavky zadavatele na předmět plnění jsou uvedeny v příloze č. 3 – Technické specifikace této zadávací dokumentace.

Dodavatel doloží v nabídce popis nabízeného řešení obsahující uvedení kompletních technických parametrů minimálně v rozsahu dle přílohy č. 3 – Technická specifikace této zadávací dokumentace.

Zadavatel požaduje doložit v nabídce doplněnou přílohu č. 3, včetně prohlášení dodavatele, že jím nabízené řešení splňuje všechny minimální požadavky zadavatele na předmět plnění. Prohlášení je součástí přílohy č. 3.

Krajská zdravotní, a.s.
Sociální péče 3316/12A
401 13 Ústí nad Labem
Tel.: +420 477 111 111
Fax: +420 477 114 900
e-mail: sekretariat@kzcr.eu

Zadavatel požaduje doložit v nabídce oprávnění od výrobce produktu, nebo subjektu pověřeného výrobcem, ve formě prosté kopie, že dodavatel je autorizovaným partnerem oprávněným k prodeji a instalaci nabízeného řešení.

Zadavatel dále požaduje doložit v nabídce platnou certifikaci ISO 27001 – Systémy řízení bezpečnosti informací a ISO 20000 – Systém managementu kvality IT služeb, a to v prosté kopii.

Zadavatel tímto informuje dodavatele, že je ve smyslu zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále jen „ZKB"), povinnou osobou (tj. podle § 3 písm. f) a g) ZKB je zadavatel správcem a provozovatelem informačního systému základní služby), a zároveň upozorňuje, že je ve smyslu § 4 odst. 2 ZKB, povinen zavést a provádět bezpečnostní opatření v rozsahu nezbytném pro zajištění kybernetické bezpečnosti provozovaných systémů. V souladu s § 4 odst. 4 ZKB je zadavatel povinen zohlednit požadavky vyplývající z bezpečnostních opatření při výběru dodavatele. Zohlednění požadavků vyplývajících z bezpečnostních opatření tedy nelze považovat za nezákonné omezení hospodářské soutěže nebo neodůvodněnou překážku hospodářské soutěži.

Zadavatel tímto upozorňuje dodavatele, že je povinen vyhodnotit rizika spojená s předmětem plnění ve smyslu § 37 ZZVZ, a povinností vyplývajících ze ZKB a stanovit bezpečnostní požadavky na dodavatele podle § 5 odst. 2 písm. e) ZKB.

Zadavatel na základě jím provedené analýzy rizik a plnění svých povinností vyplývajících ze ZKB a vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), ve znění pozdějších předpisů, ve smyslu § 37 odst. 1 písmeno b) a § 89 ZZVZ, požaduje aby dodavatelé nenabízeli předmět plnění výrobců, vůči kterým bylo vydáno varování Národního Úřadu pro Kybernetickou a Informační Bezpečnost dne 17. 12. 2018, a to konkrétně společností Huawei Technologies Co., Ltd., Šen-čen, Čínská lidová republika, a ZTE Corporation, Šen-Čen, Čínská lidová republika. **Dodavatel, který nabídne v rámci předmětu plnění zařízení výše uvedených výrobců, bude ze zadávacího řízení vyloučen.**

Dodavatel se zavazuje nabídnout zadavateli předmět plnění, který je v souladu s právními předpisy ČR a EU.

Pokud se na plnění předmětu veřejné zakázky bude podílet poddodavatel nebo poddodavatelé, požaduje zadavatel, aby účastník v souladu s § 105 ZZVZ v nabídce:
1) určil části veřejné zakázky, které hodlá plnit prostřednictvím poddodavatelů, nebo
2) předložil seznam poddodavatelů, pokud jsou účastníkovi známi a uvedl, kterou část/části veřejné zakázky bude každý z poddodavatelů plnit.

Veškeré platné doklady musí být předloženy v **českém jazyce** a musí být v souladu s právním řádem ČR opravňujícím dodavatele k vykonávání požadovaných služeb.

IČ: 25488627, DIČ: CZ25488627, Krajská zdravotní a.s. je vedená Krajským soudem v Ústí n. L., oddíl B vložka 1550.

Krajská zdravotní, a.s.
Sociální péče 3316/12A
401 13 Ústí nad Labem
Tel.: +420 477 111 111
Fax: +420 477 114 900
e-mail: sekretariat@kzcr.eu

Krajská zdravotní, a.s.

Klasifikace předmětu veřejné zakázky

Název	CPV
Balík programů pro zabezpečení	48730000-4

Předpokládaná hodnota veřejné zakázky

Název	Částka v Kč bez DPH
Systém SIEM	12 000 000 Kč
Servisní podpora na 5 let	8 000 000 Kč
Částka celkem	**20 000 000 Kč**

4 Doba plnění veřejné zakázky

Zadavatel předpokládá zahájení plnění předmětu veřejné zakázky bez zbytečného odkladu po ukončení zadávacího řízení této veřejné zakázky. **Nejzazší termín předání předmětu plnění (včetně zkušebního provozu) je 8 měsíců ode dne účinnosti smlouvy.**

Zadavatel požaduje uzavření smlouvy na dobu 60 měsíců.

5 Místa plnění veřejné zakázky

Místem plnění veřejné zakázky je:
Krajská zdravotní, a.s.
Sociální péče 3316/12
401 13 Ústí nad Labem
a veškeré místa, které jsou součástí síťového provozu zadavatele (nacházející se v Děčíně, Teplicích, Mostu, Zahražanech, Chomutově, Litoměřicích a Ryjicích)

V případě servisních nebo dohledových činností, které mohou být prováděny formou vzdáleného přístupu, je místem plnění sídlo vybraného dodavatele.

6 Požadavky na prokázání kvalifikace

Zadavatel požaduje, aby dodavatel prokázal kvalifikaci v dále uvedeném rozsahu.

Neprokáže-li účastník kvalifikaci v plném rozsahu, může být dle § 48 odst. 2 ZZVZ vyloučen z účasti v zadávacím řízení.

Krajská zdravotní, a.s.

Krajská zdravotní, a.s.
Sociální péče 3316/12A
401 13 Ústí nad Labem
Tel.: +420 477 111 111
Fax: +420 477 114 900
e-mail: sekretariat@kzcr.eu

Základní způsobilost dle § 74 ZZVZ

Dodavatel prokáže základní způsobilost dle § 74 ZZVZ předložením dokladů uvedených v § 75 ZZVZ, nebo jiným způsobem v souladu se ZZVZ.

Dodavatel je oprávněn pro prokázání splnění základní způsobilosti **předložit čestné prohlášení**, jehož vzor je součástí přílohy č. 4a této zadávací dokumentace.

Pravost a stáří dokladů se řídí § 45 a § 86 ZZVZ.

Profesní způsobilost dle § 77 ZZVZ

Dodavatel prokáže profesní způsobilost dle § 77 odst. 1 ZZVZ předložením výpisu z obchodního rejstříku, pokud je v něm zapsán, či výpisu z jiné obdobné evidence, pokud je v ní zapsán, nebo jiným způsobem v souladu se ZZVZ.

Dodavatel dále prokáže profesní způsobilost dle § 77 odst. 2 písm. a) ZZVZ předložení oprávnění k podnikání v rozsahu odpovídajícímu předmětu veřejné zakázky, tj. živnostenské oprávnění „Poskytování software, poradenství v oblasti informačních technologií, zpracování dat, hostingové a související činnosti a webové portály".

Dodavatel je oprávněn pro prokázání splnění profesní způsobilosti **předložit čestné prohlášení**, jehož vzor je součástí přílohy č. 4b této zadávací dokumentace.

Pravost a stáří dokladů se řídí § 45 a § 86 ZZVZ.

Technická kvalifikace dle § 79 ZZVZ

Dodavatel prokáže technickou kvalifikaci dle § 79 odst. 2 písm. b) ZZVZ předložením seznamu minimálně 3 (tří) významných zakázek v níže uvedeném rozsahu a předmětem plnění, realizovaných v posledních 3 letech před zahájením zadávacího řízení, k čemuž je oprávněn využít přílohu č. 5a - Seznam významných dodávek této zadávací dokumentace.

V souladu s § 79 odst. 3 ZZVZ může dodavatel pro účely prokázání splnění technické kvalifikace předložit i významné dodávky, které realizoval v době po zahájení tohoto zadávacího řízení.

Typy a rozsah významných dodávek:

Typ A – **minimálně jednu** významnou zakázku na analýzu systému SIEM v minimálním finančním objemu **1 mil. Kč bez DPH**.

Typ B – **minimálně jednu** významnou zakázku na dodávku a implementaci systému SIEM v minimálním finančním objemu více než **10 mil. Kč bez DPH** na nabízenou technologii SIEM.

Typ C – **minimálně jednu** významnou zakázku na dodávku a implementaci systému SIEM v minimálním finančním objemu více než **5 mil. Kč bez DPH** na nabízenou technologii SIEM.

Krajská zdravotní, a.s.
Sociální péče 3316/12A
401 13 Ústí nad Labem
Tel.: +420 477 111 111
Fax: +420 477 114 900
e-mail: sekretariat@kzcr.eu

Významná zakázka typu B nebo typu C na dodávku a implementaci SIEM musí zahrnovat informační systém klasifikovaný dle ZKB, jako kritický nebo významný informační systém nebo obsahující prvky kritické infrastruktury.

Seznam významných zakázek bude předložen v následující struktuře:

- název objednatele,
- předmět významné zakázky, vč. počtu zdrojů logů, je-li níže požadován,
- finanční hodnota významné zakázky, je-li níže požadována,
- doba realizace (dokončení) významné zakázky (měsíc/rok),
- kontaktní osoba objednatele, u které bude možné realizaci významné zakázky ověřit, vč. kontaktního e-mailu a telefonu.

Dodavatel může předložit významné dodávky v jiné než české měně, v tom případě bude hodnota těchto plnění přepočítána dle kurzu ČNB ke dni podání nabídek.

Dodavatel prokáže technickou kvalifikaci dle § 79 odst. 2 písm. c) a d) ZZVZ předložením seznamu členů realizačního týmu, kteří se budou podílet na plnění této veřejné zakázky (viz příloha č. 5b této zadávací dokumentace), bez ohledu na to, zda jde o zaměstnance nebo osobu v jiném vztahu k dodavateli. Realizační tým určený dodavatelem musí být složen minimálně z níže uvedených členů, kteří musí splňovat vymezené minimální kvalifikační podmínky. Dodavatel prokáže splnění kvalifikačních podmínek předložením strukturovaných profesních životopisů, včetně čestného prohlášení dodavatele o pravdivosti údajů obsažených v životopisech, ze kterých bude vyplývat, že členové realizačního týmu splňují níže uvedené požadavky zadavatele.

Zadavatelem požadovaní členové realizačního týmu:

- 1 projektový manažer
  - středoškolské nebo vyšší vzdělání ekonomického nebo technického zaměření,
  - min. 5 let praxe v oblasti projektového managementu,
  - min. 3 roky praxe v oblasti vedení projektů na SIEM řešení,
  - v posledních 3 letech před zahájením zadávacího řízení byl v pozici vedoucího/manažera minimálně dvou zakázek, které splňují požadavky dle bodu 6 této zadávací dokumentace,
  - je držitelem certifikátu z oblasti projektového řízení – např. PMP (Project Management Professional) nebo PRINCE2:PRACTITIONER nebo IPMA:C anebo ekvivalentu uvedených certifikátů, a který doloží předložením prosté kopie certifikátu k životopisu;

- 1 architekt kybernetické bezpečnost a informací
  - středoškolské vzdělání nebo vyšší,
  - min. 5 let praxe v oblasti informačních a komunikačních technologií,
  - min. 5 let praxe v oblasti bezpečnosti informací,

Krajská zdravotní, a.s.

Krajská zdravotní, a.s.
Sociální péče 3316/12A
401 13 Ústí nad Labem
Tel.: +420 477 111 111
Fax: +420 477 114 900
e-mail: sekretariat@kzcr.eu

- v posledních 3 letech před zahájením zadávacího řízení se podílel na minimálně dvou zakázkách, které splňují požadavky dle bodu 6 této zadávací dokumentace,
- je držitelem certifikace Certified Information Security Manager (CISM) nebo Certified in the Risk and IS Control (CRISC) a který doloží předložením prosté kopie certifikátu k životopisu;

- 1 specialista kybernetické bezpečnosti
  - středoškolské nebo vyšší vzdělání,
  - min. 3 roky praxe v oblasti informačních technologií,
  - min. 3 roky praxe v oblasti implementace SIEM řešení.
  - v posledních 3 letech před zahájením zadávacího řízení se podílel na minimálně dvou zakázkách, které splňují požadavky dle bodu 6 této zadávací dokumentace,
  - je držitelem některého z relevantních certifikátů pro architekta kybernetické bezpečnosti Certified Ethical Hacker (CEH), CompTIA Security+, Certified Information Security Manager (CISM), a který doloží předložením prosté kopie certifikátu k životopisu,
  - je držitelem technické certifikace na administraci nebo implementaci nabízeného SIEM řešení, a který doloží předložením prosté kopie certifikátu k životopisu;

- 2 specialisté na implementaci SIEM
  - středoškolské nebo vyšší vzdělání,
  - min. 3 roky praxe v oblasti informačních technologií,
  - min. 3 roky praxe v oblasti implementace nabízeného SIEM řešení, a které doloží formou technického certifikátu výrobce na nabízenou technologii;

- 1 specialista na implementaci Vulnerability Managementu
  - středoškolské nebo vyšší vzdělání,
  - min. 3 roky praxe v oblasti informačních technologií,
  - min. 3 roky praxe v oblasti implementace Vulnerability Management řešení, a které doloží formou technického certifikátu výrobce.

Prokázání kvalifikace prostřednictvím jiné osoby

Pokud není dodavatel schopen prokázat splnění určité části kvalifikace v plném rozsahu, je oprávněn splnění kvalifikace v chybějícím rozsahu prokázat prostřednictvím jiné osoby.

Dodavatel je v takovém případě povinen zadavateli předložit:

a) doklady prokazující splnění profesní způsobilosti podle ustanovení § 77 odst. 1 ZZVZ (touto) jinou osobou,
b) doklady prokazující splnění chybějící části kvalifikace prostřednictvím jiné osoby,

Krajská zdravotní, a.s.
Krajská zdravotní, a.s.
Sociální péče 3316/12A
401 13 Ústí nad Labem
Tel.: +420 477 111 111
Fax: +420 477 114 900
e-mail: sekretariat@kzcr.eu

c) doklady prokazující splnění základní způsobilosti podle ustanovení § 74 ZZVZ (touto) jinou osobou,
d) písemný závazek jiné osoby k poskytnutí plnění určeného k plnění veřejné zakázky nebo k poskytnutí věcí nebo práv, s nimiž bude dodavatel oprávněn disponovat v rámci plnění veřejné zakázky, a to alespoň v rozsahu, v jakém jiná osoba prokázala kvalifikaci za dodavatele.

Požadavek podle výše uvedeného odstavce písm. d) je splněn, pokud obsahem písemného závazku jiné osoby je společná a nerozdílná odpovědnost této osoby za plnění veřejné zakázky společně s dodavatelem. Prokazuje-li však dodavatel prostřednictvím jiné osoby kvalifikaci a předkládá doklady podle § 79 odst. 2 písm. b) nebo d) ZZVZ vztahující se k takové osobě, musí dokument podle výše uvedeného odstavce písm. d) obsahovat závazek, že jiná osoba bude provádět části plnění, ke kterým se prokazované kritérium kvalifikace vztahuje.

Změny v kvalifikaci

Dojde-li v průběhu zadávacího řízení po předložení dokladů nebo prohlášení o kvalifikaci ke změně kvalifikace účastníka zadávacího řízení, je účastník zadávacího řízení povinen do 5 pracovních dnů tuto změnu zadavateli oznámit a do 10 pracovních dnů od oznámení této změny zadavateli předložit nové doklady nebo prohlášení ke kvalifikaci. Tuto povinnost účastník zadávacího řízení nemá, pokud je kvalifikace změněna takovým způsobem, že

a) podmínky kvalifikace jsou nadále splněny,
b) nedošlo k ovlivnění kritérií pro snížení počtu účastníků zadávacího řízení nebo nabídek a
c) nedošlo k ovlivnění kritérií hodnocení nabídek.

Nesplnění této povinnosti je dle § 88 odst. 2 ZZVZ důvodem pro bezodkladné vyloučení účastníka zadávacího řízení.

7 Obchodní a platební podmínky

Obchodní a platební podmínky jsou stanoveny obligatorním návrhem smlouvy, jehož závazný text je uveden v příloze č. 2 této zadávací dokumentace (dále jen „Obligatorní návrh smlouvy").

Dodavatel **nepředkládá do nabídky** Obligatorní návrh smlouvy. Obligatorní návrh smlouvy bude vyplněn až před uzavřením smlouvy s vybraným dodavatelem, kdy budou doplněny veškeré chybějící údaje (zejména identifikace dodavatele, nabídková cena, jméno kontaktní osoby apod.).
Dodavatel je však povinen v rámci své nabídky učinit **čestné prohlášení** (příloha č. 4c této zadávací dokumentace) o tom, že Obligatorní návrh smlouvy plně a bezvýhradně akceptuje.

Požadavky na pojištění

Zadavatel vyžaduje od dodavatele **pojištění odpovědnosti** za škodu způsobenou dodavatelem zadavateli, příp. třetí osobě, včetně škody na zdraví a životě, které vzniknou v souvislosti s plněním závazku pro celé období plnění veřejné zakázky, a to s požadovanou minimální hranicí pojistného plnění ve výši **50 000 000,- Kč**. Pojistná smlouva musí být udržována v platnosti po celou dobu trvání smluvního vztahu.

IČ: 25488627, DIČ: CZ25488627, Krajská zdravotní a.s. je vedená Krajským soudem v Ústí n. L., oddíl B vložka 1550.

Krajská zdravotní, a.s.
Sociální péče 3316/12A
401 13 Ústí nad Labem
Tel.: +420 477 111 111
Fax: +420 477 114 900
e-mail: sekretariat@kzcr.eu

Krajská zdravotní, a.s.

Dodavatel **nepředkládá** do nabídky pojistnou smlouvu, její návrh ani jiný pojistný dokument. Zadavatel však požaduje, aby dodavatel předložil v nabídce **čestné prohlášení** o splnění povinnosti sjednání pojištění odpovědnosti v požadované výši (příloha č. 4d zadávací dokumentace).

8 Požadavky na způsob zpracování elektronické nabídky

- Celá nabídka bude předložena v elektronické podobě ve formátu *.pdf a pokud možno v jednom souboru. Dokumenty mohou být předloženy v archivu formátu zip, rar, 7z.
- Nabídka bude zpracována v českém jazyce.
- Zadavatel připouští katalogy, prospekty a jiný podpůrný materiál technické povahy v anglickém jazyce.

Struktura nabídky

Zadavatel doporučuje řazení řádně očíslovaných listů nabídky v tomto pořadí:

1) Krycí list (příloha č. 1 této zadávací dokumentace) **podepsaný osobou oprávněnou** zastupovat dodavatele;
2) Doklady prokazující kvalifikační způsobilost dle této zadávací dokumentace;
3) Čestné prohlášení dodavatele;
4) Cenová nabídka se započtením veškerých nákladů, rizik, zisku a finančních vlivů platná po celou dobu realizace zakázky, včetně vyplnění přílohy č. 6 této zadávací dokumentace (cenová nabídka obsahuje rozpis cen jednotlivého HW a SW);
5) Ostatní doklady a dokumenty požadované zadavatelem.

Informace a údaje uvedené v jednotlivých částech této zadávací dokumentace a v přílohách zadávací dokumentace vymezují **závazné požadavky** zadavatele na plnění veřejné zakázky. Tyto požadavky je dodavatel povinen plně a bezvýhradně respektovat při zpracování své nabídky. Neakceptování požadavků zadavatele uvedených v této zadávací dokumentaci či změny obchodních podmínek budou považovány za nesplnění zadávacích podmínek s následkem vyloučení dodavatele z účasti v zadávacím řízení.

9 Vysvětlení, změna, doplnění zadávací dokumentace

Vysvětlení zadávací dokumentace se řídí ustanovením § 98 ZZVZ. **Zadavatel vždy uveřejní vysvětlení zadávací dokumentace včetně přesného znění žádosti na profilu zadavatele.**

Změna nebo doplnění zadávací dokumentace se řídí ustanovením § 99 ZZVZ. **Zadavatel vždy uveřejní informaci o změně nebo doplnění zadávací dokumentace na profilu zadavatele.**

10 Podmínky pro podání nabídky

Dodavatel podá nabídku v elektronické podobě prostřednictvím elektronického nástroje E-ZAK Krajské zdravotní, a.s., na adrese: https://zakazky.kzcr.eu/. Více informací o elektronickém nástroji E-ZAK naleznete na adrese http://www.ezak.cz.

IČ: 25488627, DIČ: CZ25488627, Krajská zdravotní a.s. je vedená Krajským soudem v Ústí n. L., oddíl B vložka 1550.

Krajská zdravotní, a.s.
Sociální péče 3316/12A
401 13 Ústí nad Labem
Tel.: +420 477 111 111
Fax: +420 477 114 900
e-mail: sekretariat@kzcr.eu

Krajská zdravotní, a.s.

Zadavatel doporučuje dodavatelům, **seznámit se v dostatečném předstihu** před podáním elektronické nabídky, s podmínkami podání elektronické nabídky a provést test podání nabídky na: https://zakazky.kzcr.eu/test_index.html.

Dodavatel je za účelem podání nabídky **povinen se registrovat** v elektronickém nástroji.

Systémové požadavky na PC pro podání nabídek jsou k dispozici na internetové adrese: https://www.ezak.cz/faq/pozadavky-na-system.

Test nastavení prohlížeče a systému je možno provést na internetové adrese: https://zakazky.kzcr.eu/test_index.html.

Podrobné instrukce elektronického nástroje se nacházejí v „uživatelské příručce" na internetové adrese: https://zakazky.kzcr.eu/manual.html.

Při technických problémech s elektronickým podáním nabídky je kontakt na technickou podporu dodavatele systému: tel.: +420 538 702 719 podpora@ezak.cz (pracovní dny 9.00 – 17.00 hod.).

Lhůta k podání nabídky

Lhůta pro podání nabídek je uvedena na profilu zadavatele https://zakazky.kzcr.eu/ a v oznámení o zahájení zadávacího řízení ve Věstníku veřejných zakázek.

Zadavatel upozorňuje, že na otevírání nabídek v elektronické podobě nemají právo být přítomni zástupci dodavatelů.

11 Způsob a kritérium hodnocení nabídek

V souladu s ustanovením § 114 odst. 1 ZZVZ budou nabídky této veřejné zakázky hodnoceny podle jejich ekonomické výhodnosti. Ekonomická výhodnost bude hodnocena v souladu s ustanovením § 114 odst. 2 ZZVZ pouze podle nejnižší nabídkové ceny bez DPH.

Zadavatel provede hodnocení tak, že seřadí nabídky podle výše nabídkové ceny v Kč bez DPH stanovené dle této zadávací dokumentace. Nabídka s nejnižší nabídkovou cenou v Kč bez DPH bude vybrána jako ekonomicky nejvýhodnější.

Způsob zpracování nabídkové ceny

Dodavatel stanoví celkovou nabídkovou cenu jako celkovou cenu za plnění předmětu veřejné zakázky za celé období 5 let v souladu s touto zadávací dokumentací, a to absolutní částkou v české měně.

Celkovou nabídkovou cenu dodavatel doloží vyplněnou přílohou č. 6 – Rozklad nabídkové ceny této zadávací dokumentace, kterou přiloží k nabídce. Celková nabídková cena bude výsledným součtem cen jednotlivých položek uvedených v příloze č. 6 - Rozklad nabídkové ceny této zadávací dokumentace.

Krajská zdravotní, a.s.
Sociální péče 3316/12A
401 13 Ústí nad Labem
Tel.: +420 477 111 111
Fax: +420 477 114 900
e-mail: sekretariat@kzcr.eu

12 Podmínky pro uzavření smlouvy

Zadavatel požaduje, aby smlouva na plnění veřejné zakázky byla uzavřena elektronicky. K uzavření smlouvy je vyžadován zaručený elektronický podpis.

Vybraný dodavatel je v souladu s § 122 odst. 3 písm. a) ZZVZ povinen na výzvu zadavatele předložit originály nebo ověřené kopie dokladů o jeho kvalifikaci, pokud je již nemá zadavatel k dispozici. Tyto doklady mohou být již součástí nabídky účastníků.

Vybraný dodavatel před podpisem smlouvy na plnění veřejné zakázky na výzvu zadavatele předloží prostou kopii pojistné smlouvy, nebo jiný pojistný dokument, ze kterého bude patrné plnění požadavku zadavatele stanoveného v bodě 7 této zadávací dokumentace.

13 Práva a výhrady zadavatele

- Zadavatel si vyhrazuje, aby veškerá komunikace mezi zadavatelem a dodavatelem probíhala výhradně prostřednictvím profilu zadavatele na adrese https://zakazky.kzcr.eu/.
- Dodavatel může podat pouze jednu nabídku.
- Zadavatel nepřipouští variantní řešení nabídky.
- Dodavateli podáním nabídky nevznikají žádná práva na uzavření smlouvy na veřejnou zakázku se zadavatelem.
- Zadavatel je oprávněn před rozhodnutím o výběru nejvhodnější nabídky si ověřit, popřípadě upřesnit informace uvedené účastníkem v nabídce.
- Zadavatel nehradí případné náklady dodavatele spojené s podáním nabídky, ani žádné náklady spojené s účastí v zadávacím řízení.
- Zadavatel nevrací podané nabídky, které zůstávají u zadavatele jako doklad o průběhu zadávacího řízení, s obsahem nabídek bude zacházeno důvěrně.
- Zadavatel si vyhrazuje právo zakázku zrušit dle § 127 ZZVZ.

14 Přílohy zadávací dokumentace

Příloha č. 1: Krycí list nabídky
Příloha č. 2: Obligatorní návrh smlouvy
Příloha č. 3: Technická specifikace
Příloha č. 4a: Vzor čestného prohlášení dodavatele o splnění základní způsobilosti
Příloha č. 4b: Vzor čestného prohlášení dodavatele o splnění profesní způsobilosti
Příloha č. 4c: Vzor čestného prohlášení dodavatele o akceptaci Obligatorního návrhu smlouvy
Příloha č. 4d: Vzor čestného prohlášení dodavatele o splnění povinnosti sjednání pojištění
Příloha č. 5a: Seznam významných dodávek
Příloha č. 5b: Seznam členů realizačního týmu vč. čestné
Příloha č. 6: Rozklad nabídkové ceny

Ústí nad Labem dne: 18 -03- 2021

[redacted]

IČ: 25488627, DIČ: CZ25488627, Krajská zdravotní a.s. je vedená Krajským soudem v Ústí n. L., oddíl B vložka 1550.

Příloha č. 7

Cena

Název dodavatele	AUTOCONT a.s.
IČO dodavatele	IČ: 04308697

Cena za jednorázovou implementaci

A	B	C	D
Č.	**Product Number**	**Název položky**	**CELKOVÁ nabídková cena bez DPH [v Kč] za rok**
1		Cena dodaného HW s 5 letou podporou výrobce	[redacted]
2		Cena dodaného SW s 1 letou podporou výrobce	
3		Vypracování projektu nasazení (analýzy)	
4		Implementace systému	
5		Školení a dokumentace	
CELKEM			11 789 377

Cena maintenance a služeb na 5 let

A	B	C	D
Č.	**Product Number**	**Název položky**	**CELKOVÁ nabídková cena bez DPH [v Kč] za rok**
1		Roční cena služby servisní podpory dodavatele (1. až 5. rok)	[redacted]
2		Roční cena služby bezpečnostního dohledu dodavatele (1. až 5. rok)	
3		Roční cena služby aplikační podpory dodavatele (2. až 5. rok)	
CELKEM za 5 let			7 855 984

CELKEM za Implementaci a služby za 5 let	19 645 361

Ceník víceprací

A	B	C	D
Č.	**Product Number**	**Název položky**	**CELKOVÁ nabídková cena bez DPH [v Kč]**
1		Cena za 1 hodinu poskytování servisních služeb	[redacted]

CELKOVÁ NABÍDKOVÁ CENA	
A	**B**
Celková nabídková cena bez DPH [v Kč]	19 645 361
Sazba DPH, která se vztahuje k nabídkové ceně [v %]	21%
Výše DPH [v Kč]	4 125 526
Celková nabídková cena s DPH [v Kč]	23 770 887

Datum a podpis osoby oprávněné jednat jménem či za dodavatele	[redacted]

* Dodavatel je povinen vyplnit žlutě podbarvená pole kladnou nenulovou hodnotou

** Zadavatel si vyhrazuje právo neodebrat uvedené předpokládané množství zboží, a to bez jakékoliv sankce vůči němu uplatněné.