**Příloha č. 1**

**Technická specifikace**

Předmětem plnění veřejné zakázky jsou zařízení a systémy uvedené v následující tabulce, včetně služeb (komodity):

| **Komodita** | **Zajišťovaná oblast** | **Stručný popis položky** | **Jednotka** | **Počet jednotek** |
| --- | --- | --- | --- | --- |
| K.2 | Zavedení nástrojů pro zaznamenávání činnosti informačního nebo komunikačního systému, jeho uživatelů a administrátorů | 1. Zaznamenávání činností (logů) IS DPMUL a souvisejících systémů do externích systémů. 2. Nástroje pro kompletní správu životního cyklu (pořízení, zpracování, zobrazení, prohledávání, ochrana, uchování a archivace) logů chráněných IS a souvisejících a podpůrných systémů a technologií. 3. Pokročilé notifikační nástroje bezpečnostních a nestandardních událostí IS.Součástí je pořízení software pro komplexní správu logů (log management), hardware nebo hardwarové appliance pro běh software a implementace a související služby. | soubor | 1 |

1. **Požadované parametry technického řešení**

### Obecné požadavky

* + - 1. Zadavatel při výstavbě, správě a provozu technologií striktně dodržuje hledisko technologické neutrálnosti, tj. využití technologií takovým způsobem, který neomezuje implementaci technologií různých výrobců – tuto strategii musí splňovat i řešení dodané v rámci této veřejné zakázky.
			2. Pokud uchazeč vyžaduje využití konkrétních softwarových produktů a jím zvolený přístup k řešení zadání je na takových konkrétních řešeních závislý, musí jejich pořízení zahrnout ve své nabídce v potřebném rozsahu a v rámci nabídnuté ceny.
			3. Za předpokladu, že uchazečem navržené řešení vyžaduje fyzickou infrastrukturu (např. servery, úložiště, komunikační prvky atd.) neobsaženou v popisu předmětu plnění, zahrne uchazeč do své ceny všechny náklady na její pořízení, instalaci, konfiguraci a další služby potřebné pro uvedení do provozu.
			4. Pro každý softwarový produkt, který uchazeč nabídne v rámci svého řešení, budou v nabídce výslovně uvedeny všechny licenční nebo výkonové požadavky spojené s instalací a provozem řešení, včetně uvedení konkrétní infrastruktury, na které bude řešení provozováno.
			5. Pokud jsou v nabízeném řešení zahrnuty jakékoliv licence, jejich legální používání nesmí být časově omezeno. Nabízené řešení tedy musí být plně funkční i po uplynutí doby placené podpory.
			6. Zadavatel z důvodů co nejjednodušší a jednotné správy a minimalizace provozních nákladů vyžaduje využití stávajících prostředků a používaných technologií. V případě, že uchazeč vyžaduje ve svém řešení stejné nebo podobné funkce, jaké poskytují stávající prostředky a technologie, je povinen využít nebo vhodným způsobem rozšířit stávající prostředky – není přípustné implementovat např. další serverovou virtualizační platformu, adresářovou službu apod.
			7. Uchazeč prokáže, že všechny dodávky, které dodá Zadavateli:
				1. jsou nové, byly oprávněně uvedeny na trh v EU nebo pochází z autorizovaného prodejního kanálu výrobce,
				2. mají plnou záruku od výrobce,
				3. mohou být podporovány výrobcem a mohou být součástí servisního a podpůrného programu výrobce,
				4. obsahuji licenci na používání příslušného softwaru,
				5. jsou určeny pro provoz v České republice,
				6. z databází výrobce, distributora či prodejce bude možné výše uvedené skutečnosti doložit.

Tyto skutečnosti uchazeč doloží čestným prohlášením distributora, popř. uchazečem samotným, nelze-li prohlášení distributora získat. Zadavatel si vyhrazuje právo na zjištění původu výrobku při jejich převzetí, a to dle příslušných sériových čísel a právo podpisu akceptačního protokolu, osvědčujícího převzetí dodávky, až po ověření původu výrobku.

### Specifické požadavky – K1 – Zavedení nástrojů pro zaznamenávání činnosti informačního nebo komunikačního systému, jeho uživatelů a administrátorů

* + - 1. V současné době nevlastní DPMUL žádný nástroj pro (centrální) zaznamenávání činnosti (logů) a navazujících systémů. Činnosti jsou v některých systémech zaznamenávány lokálně, ale bez jednotné politiky, dlouhodobého ukládání a ochrany logů před změnou, přetečením apod. Chybí tak nástroj pro podporu řešení případných kybernetických událostí a incidentů, poskytování konsolidovaných informací před vznikem a v průběhu události/incidentu. Absence nástroje také neumožňuje efektivně analyzovat chování IS a souvisejících systémů z pohledu kybernetické bezpečnosti, ale i z pohledu běžného provozu pro účely zavádění preventivních opatření předcházejících výskytu nestandardního provozního stavu a/nebo opatření k zamezení jeho opakování.

* + - 1. Zvýšení úrovně zabezpečení v oblasti řízení přístupových oprávnění interních i externích správců bude dosaženo:
				1. Implementací nástroje pro správu logů (tzv. log management) - zavedením komplexního systému pro správu logů dojde k centralizovanému sjednocení různých bází bezpečnostních a provozních záznamů, které jsou poskytovány různými typy hardwarových zařízení, dále různými provozovanými operačními systémy a aplikacemi, včetně všech nástrojů implementovaných v rámci tohoto projektu. Zaznamenané činnosti budou k dispozici na jednom místě ve sjednoceném formátu při zachování jejich dostupnosti, důvěrnosti a integrity. Systém zajistí uložení dat k okamžitému prohlížení a prohledávání minimálně po dobu 18 měsíců a bude umožňovat archivaci starších záznamů s možností rychlé obnovy archivu v případě potřeby. Systém musí zajistit integritu archivu.
				2. Pořízením vyhrazeného serveru nebo hardwarové appliance pro provoz nástroje pro správu logů, aby byla zajištěna nezávislost nástroje na infrastruktuře DPMUL a tím schopnost zaznamenávání její činnosti i v nestandardních provozních stavech (přetížení, start, nestabilita apod.). Server nebo hardwarová appliance musí být napojena do systému pro správu HW komponent Dell OpenManage, který zadavatel využívá.
			2. Požadované řešení je standardní Log/Event Management, který musí umožnit být v budoucí rozšíření o další systémy (např. systém SIEM) nebo napojení na služby SOC (Security operations center).
			3. Řešení umožní sofistikovanou, transparentní a opakovatelnou pokročilou analýzu, spojenou s řešením běžných provozních i bezpečnostních událostí/incidentů a upozorňováním na ně, a to z kritických i nekritických a podpůrných systémů a aplikací. Řešení musí být schopné generovat reporty o aktivitách systémů i uživatelů, včetně auditních reportů na vyžádání, nebo se stanovenou periodicitou s definovatelným obsahem, primárně v českém jazyce a dále variantně v jazyce anglickém, bez nutnosti používat SQL (či obdobnou „programátorskou“) syntaxi pro definici či úpravu reportů.
			4. Nabízené řešení musí zachovávat originál logů za účelem bezpečnostního auditu, a to v souladu s požadavky ISO/ČSN 27001:2013 pro pořizování auditních záznamů.
			5. Řešení musí umožnit snadné a rychlé multikriteriální vyhledávání pro účely analýz, auditů, a podporu běžného provozu komplexního řešení ICT infrastruktury DPMUL.
			6. Pro zajištění požadavků bezpečnosti musí řešení Log/Event Management disponovat konfigurovatelným uživatelským oddělením rolí a ochranou centralizovaných logů před neoprávněným přístupem k citlivým datům.
			7. Reporty systému budou sloužit pro přehlednou kontrolu stavu a chování informačních systémů a uživatelů za určité období (typicky 1 měsíc) a ke kontrole dodržování compliance („jednání v souladu s pravidly") organizace.
			8. Data uložená v systému a systémem archivovaná budou zajištěna a zabezpečena před neoprávněnou změnou i pro účely vyšetřování případného bezpečnostního incidentu.
			9. Bude implementováno řešení, které umožní příjem a vyhodnocení všech požadovaných informací – může se jednat o jediné zařízení, softwarový nástroj či appliance nebo o řešení složené z více samostatných a vzájemně kompatibilních komponent. Zařízení umožní správu z jedné grafické konzole, přístupné nativně skrze https bez nutnosti instalace klienta. Ukládání všech informací do bude prováděno jedné databáze (nebo více integrovaných databází) tak, aby bylo možno realizovat multikriteriální vyhledávání napříč informacemi z různých.
			10. Mandatorní informace, která bude v systému vždy obsažena a uchována, je vazba IP-uživatel-čas. Tuto informaci bude systém čerpat ze security event-logu adresářové služby, dále z informací o probíhajících komunikacích na straně firewallu za pomoci jeho SSO agentů či logů a dalších přístupových a autentifikačních systémů (např. RADIUS logy). Dále budou získávány informace o překladu zdrojových, vnitřních IPv4 adres na externím výstupním rozhraní firewallu, kde bude prováděn NAT. Bude se tedy jednat o informace obsažené v NAT tabulce. Spolu s tím bude po stanovenou dobu možné zpětně dohledat i vnější provoz k vnitřnímu zařízení.
			11. Bude umožňovat uchování každého záznamu v jeho nezměněné podobě, ale zároveň bude schopný dávat jednotlivé události ihned do souvislostí a vyhodnocovat riziko a případné bezpečnostní události aktivně notifikovat, resp. reportovat.
			12. Implementace systému bude v provedena v souladu s § 23 Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí Vyhlášky č.316/2014 Sb. k Zákonu č. 181/2014 Sb., o kybernetické bezpečnosti.
			13. Součástí dodávky musí být úplná a podrobná dokumentace systému v češtině
			14. Zadavatel bude vyžadovat poskytnutí funkčního vzorku (v identické konfiguraci s nabízeným systémem) pro účely testování a ověření požadovaných funkčních vlastností, uchazeč je povinen doručit testovací vzorky na Místo plnění do pěti (5) pracovních dnů od doručení výzvy k jejich poskytnutí. Vybraný uchazeč poskytne testovací vzorky bezplatně a na dobu minimálně následujících 10 pracovních dnů poskytne i součinnost s testováním.

Zadavatel v rámci testovacího provozu na dodaném testovacím vzorku, **vycházeje z dodané dokumentace k nabízenému systému**, provede tyto práce a vytvoří záznam o jednotlivých činnostech a jejich výsledcích. Jedná se zejména tyto testy:

* + - * 1. Základní nastavení systému a jeho konfigurace tak, aby mohl pracovat v prostředí zadavatele, včetně vytvoření uživatelů s rozdílným systémovým i databázovým oprávněním, a to v jednotném webovém rozhraní nabízeného systému
				2. Zapojení pěti vybraných zdrojových systémů logů odesílajících logy prostřednictvím Syslog protokolu přes UDP/TCP/TLS z prostředí zadavatele a otestování následujících vlastností:

nastavení klasifikace zdrojů

nastavení značek (tagů) pro vybrané zdrojové systémy

filtrování událostí

úprava normalizace existujícího zdroje v grafickém rozhraní nástroje

vytvoření reportů a exportu logů a vybraných údajů z logů

* + - * 1. Konfiguraci pěti vybraných systémů Microsoft Windows tak, aby posílaly EVTx a textové logy do testovaného systému, s konfigurací pouze v jednotném grafickém rozhraní nabízeného systému
				2. Ověření funkčních a výkonových parametrů Windows agenta a jeho centralizované správy v nabízeném systému – viz Technická specifikace, všechny body z odstavce „Sběr událostí z Microsoft prostředí“ včetně centrální instalace a centrální konfigurace Microsoft Sysmon služby pro rozšíření hodnoty logů vytvářených zdrojovými systémy dle doporučené auditní politiky.
				3. Konfigurace kolektoru logů z jedné databáze z prostředí zadavatele v jednotném webovém rozhraní nabízeného systému bez nutnosti instalovat na databázový server další produkty třetích stran
				4. Oprava ze záloh po simulovaném úplném selhání nabízeného systému v následujících krocích:

Provedení zálohy konfigurace a dat na externí systém

Vytažení dvou libovolných disků za běhu systému

Nastavení systému do továrního nastavení

Obnovení konfigurace a všech dat z vytvořených záloh

Kontrola úplnosti obnovené konfigurace a dat ze záloh

* + - * 1. Navýšení a ponížení software nabízeného systému v grafickém rozhraní a provedení kontroly, že v případě ponížení nedojde ke ztrátě dříve shromážděných dat
				2. **Kontrola výkonu systému v běžné zátěži** – generátorem logů se odešle vzorek originálních dat sesbíraných během předchozích testů. A to rychlostí odpovídající nabízenému systému, po dobu minimálně 30 minut. Sledované hodnoty budou: přijetí všech logů a jejich správné zařazení do databáze s časovým razítkem odpovídajícím skutečné době přijetí logu. Dále bude provedena kontrola, zda nedošlo během zpracování logů k jejich poškození nebo ztrátě. Logy musejí být kompletně zpracovány bez ztráty dat, se správným časovým razítkem uloženy v databázi, normalizovány a doplněny o rozšiřující informace typu metadata, DNS-PTR a geolokace
				3. Kontrola kompletnosti dokumentace pro nabízený systém v českém jazyce
				4. Součástí ověření funkčních vlastností může být i ověření požadované funkcionality a parametrů dodaného funkčního vzorku systému dle Technické specifikace tohoto zadání.

## Implementační služby

### Obecné požadavky

* + - 1. Zadavatel požaduje provést minimálně následující implementační práce na dodaných komponentech a případně dalších zařízeních. Uchazeč je dále povinen zahrnout do nabídky veškeré další činnosti a prostředky, které jsou nezbytné pro provedení díla v rozsahu doporučeném výrobci a dle tzv. nejlepších praktik, i v případě, pokud nejsou explicitně uvedeny, ale jsou pro realizaci předmětu plnění podstatné. Implementační služby budou minimálně v následujícím rozsahu:
				1. Zajištění projektového vedení realizace předmětu plnění.
				2. Zpracování prováděcí dokumentace, která představuje projektovou dokumentaci, podle které se projekt bude realizovat. Součástí zpracování prováděcí dokumentace je mj. provedení předimplementační analýzy a zpracování finálního návrhu cílového stavu. Prováděcí dokumentace musí respektovat a využívat osvědčené praktiky (tzv. Best Practice) a doporučení výrobců nabízených technologií.
				3. Dodávku nabízených prvků a kompletní implementaci řešení provedenou podle prováděcí dokumentace a splňující povinné parametry technického řešení,
				4. Provedení školení,
				5. Zajištění zkušebního provozu,
				6. Provedení akceptačních testů,
				7. Zpracování provozní dokumentace v rozsahu detailního popisu skutečného provedení a popisu činností běžné údržby a administrace systémů a činností pro spolehlivé zajištění provozu.
				8. Předání do ostrého provozu,
			2. Náklady na provedení implementačních služeb musí být zahrnuty v nabídkové ceně k položce, ke které se vztahují a nelze je vyčíslit zvlášť.
			3. Uchazeč je dále povinen zahrnout do nabídky i další související služby minimálně v dále uvedeném rozsahu. Pro každou uvedenou službu uvede uchazeč podrobný popis způsobu provedení služby při realizaci předmětu plnění zohledňující požadavky zadavatele na technické řešení.

|  |
| --- |
| K.1 - Zavedení nástrojů pro zaznamenávání činnosti informačního nebo komunikačního systému, jeho uživatelů a administrátorů |
| * 1. Analýza a detailní identifikace zdrojů dat, jejichž provozně bezpečnostní informace bude nutné, popř. vhodné sbírat, korelovat a analyzovat. Bude obsahovat i návrh způsobu zpracování získaných informací a vhodných proaktivních i reaktivních akcí
	2. Vybudování systému centrálního logování pro zaznamenávání činnosti informačního nebo komunikačního systému, jeho uživatelů a administrátorů
	3. Návrh a provedení akceptačních testů, musí zahrnovat i testy archivace a obnovy logů a ověření detekce jejich neoprávněně modifikace.
	4. Předání technické dokumentace skutečného provedení
	5. Zaškolení
 |

* + - 1. Uchazeč dle svého uvážení může doplnit v nabídce další služby, které jsou dle jeho názoru potřebné pro úspěšnou realizaci zakázky.
			2. Veškerá dokumentace musí být zhotovena výhradně v českém jazyce, bude dodána v elektronické formě ve standartních formátech (MS Office) používaných zadavatelem.

| **Komodita K.1 - Zavedení nástrojů pro zaznamenávání činnosti informačního nebo komunikačního systému, jeho uživatelů a administrátorů**  |
| --- |
| **Část** | **Parametr** | **Popis povinného parametru** | **Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek** | **Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru** |
| **Systém pro správu logů** | Základní funkce | Integrovaný systém zpracování logů a událostí z definovaných zdrojů napříč výrobci aplikací, operačních systémů a síťového hardware |   |   |
| Architektura | Integrovaná appliance (hw se specializovaným firmware/software) nebo server se specializovaným software včetně operačního a podpůrných systémů (databáze apod.), samostatně funkční nezávisle na infrastruktuře zadavatele  |   |   |
| Provedení | Určené pro montáž do stávajícího serverového datového rozvaděče 19", hloubka max 900 mm, včetně výsuvných kolejnic a ramene pro vedení kabelů.  |   |   |
| Ovládání | Grafická webová konzole pro administrátory I operátory, umožňuje kompletní správu systému včetně úvodního nastavení. |   |   |
| Autentizace | Autentizace uživatelů vůči Active Directory nebo LDAP serveru. V případě výpadku AD/LDAP musí systém umožnit autentizaci z lokální databáze. |   |   |
| Uživatelské role | Podpora uživatelských rolí obsahujících přístupová práva k uloženým událostem a jednotlivým ovládacím částem systému. |   |   |
| Sběr dat (logů) | Bezagentový sběr logů s výjimkou systémů Windows |   |   |
| Windows agent | Kompletní správa a aktualizace z administrátorské konzole, sběr dat z textových i Event logů (včetně rozšířených) , šifrovaná komunikace, buffer pro případ ztráty komunikace, překlad kódů na text (např. Logon type 2 => "Interactive" apod.) a textový popis události shodný s Windows Event Viewerem |   |   |
| Protokoly  | Příjem a zpracování logy, událostí a další strojově generovaných data minimálně protokoly UDP/TCP 514 (SYSLOG), TCP 20514 (RELP, nešifrovaně) a TCP 20515 (RELP, šifrovaně). |   |   |
| Formáty logů | Mini. RAW, Syslog, CEF, LEEF, JSON RFC7159, Windows EventLog |   |   |
| Třídění logů | Podpora příjmu logů na rozsahu alespoň 50 UDP a TCP portů pro zjednodušené třídění vstupních zpráv.  |   |   |
| Zpracování logů | Integrované parsování a normalizace přijatých událostí/logů bez nutnosti instalovat externí aplikace nebo systémy |   |   |
| Ochrana logů | Zamezení mazání nebo modifikování již uložených logů. Každý log musí mít unikátní identifikátor pro jeho jednoznačnou identifikaci.  |   |   |
| Vizualizace logů | Grafická vizualizace logů, událostí a strojových dat (grafy událostí). Dynamická vizualizace - změnou volby (např. filtru) v jednom grafu se ostatní svázané grafy upraví automaticky dle požadované volby. Integrované podpora zobrazení TOP X událostí za zvolené časové období.  |   |   |
| Pracovní plochy | Předpřipravené pohledy (dashboardy) na uložená data dle jednotlivých kategorií zdrojových zařízení i dle logického členění, průběžná aktualizace pohledů výrobcem. Integrovaná podpora tvorby uživatelských dashboardů včetně ukládání  |   |   |
| Zajištění logů | Ochrana proti ztrátě logů při přetížení systému. Ukládání nezpracovaných logů/událostí do vyrovnávací paměti o kapacitě min 25 GB, notifikace správce systému při riziku zaplnění vyrovnávací paměti |   |   |
| Doplňování logů | Integrovaná podpora doplňování logů dalšími údaji - např. umístění zařízení, typ zařízení, kritičnost zařízení apod. - k jednotlivým zdrojům dat, aplikacím, zařízením, IP rozsahů apod.  |   |   |
| Archivace | Integrovaná archivace logů včetně zajištění integrity archivů, obnova  |   |   |
| Rozpoznávání IP, MAC | Automatické doplňování reverzních DNS záznamům k IP adresám a výrobce podle MAC adresy |   |   |
| Časová razítka | Podpora doplňkové značky (razítka) navíc k časovému údaji zaznamenané události/logu, slouží jako výchozí časový údaj pro systém |   |   |
| Vyhledávání | Snadné multikriteriální vyhledávání událostí bez nutnosti speciálních znalosti (např. SQL dotazů apod.) napříč všemi typy data a zařízení. |   |   |
| Rychlé vyhledávání | Rychlé vyhledávání i v aktuálně uložených položkách (průběžné indexování) |   |   |
| Geolokace | Automatické doplňování geolokačních informací k událostem a jejich grafické znázornění na mapě bez služeb třetích stran |   |   |
| Reporty | Integrovaný reportovací nástroj s přednastavenými obvyklými reporty a možností vlastních úprav a vytvoření nových pohledů bez potřeby speciálních znalostí (např. SQL dotazů apod.). Průběžná aktualizace přednastavených reportů výrobcem. |   |   |
| Integrace | Integrované REST API rozhraní pro napojené systémy, musí umožnit autorizovaný přístup ke strukturované databázi logů. |   |   |
| Parsery | Integrovaný grafický (vizuální) nástroj pro tvorbu vlastních parserů logů včetně testování a ladění - okamžitého zobrazení rozparsovaných testovacích dat včetně případných chyb  |   |   |
| Konektory | Konektory (specifické parsery) pro stávající technologie - min. Active Directory, Hyper-V, Windows (vč. DNS, DHCP), Icewarp, MS SQL, Sophos, HPE/Aruba, Dell servery, Synology, Linux, Apache. |   |   |
| Alerty, notifikace | Předpřipravené alerty a integrovaný grafický (vizuální) nástroj pro vytváření automatických notifikací/alertů generovaných při splnění definovaných podmínek v přijatých datech. Odesílání alertů min SMTP, Syslog, TCP. |   |   |
| Výkon | Min. 6000 EPS (events per second), krátkodobá (min. 10 min) přetižitelnost systému 200% |   |   |
| Kapacita | Využitelná diskové kapacita pro ukládání data min. 40 TB, disky musí být chráněny min. RAID 5 |   |   |
| Řízení diskového systému | Hardwarový řadič RAID se zálohovanou vyrovnávací pamětí (zápis I čtení) o kapacitě min 8 GB |   |   |
| Úložiště logů | Logy musí být ukládány do databáze (příslušná licence musí být součástí dodávky) s podporou komprese ukládaných dat. |   |   |
| Napájení | Systém musí mít redundantní napájení (min. 2 nezávislé zdroje) |   |   |
| LAN konektivita | Min. 2x LAN 1 Gb + 1x 1Gb nezávislý port pro správu hardware prostřednictvím KVM konzole s grafickým rozhraním, zabezpečeným přístupem a detailním přehledem o stavu hardware včetně okamžité a dlouhodobé spotřeby elektrické energie a stavu dílčích komponent. |   |   |
| Aktualizace  | Integrovaná aktualizace systému prostřednictvím administrátorské konzole včetně podpory downgrade  |   |   |
| Zálohování | Integrované zálohování a obnova konfigurace  |   |   |
| Škálovatelnost | Systém lze propojit s dalšími systémy stejného výrobce. Spojením systémů dojde ke zvýšení kapacity, výkonu (včetně vyhledávání) a dostupnosti. Navenek se propojené systémy chovají jako jeden. |   |   |
| Dokumentace  | Plnohodnotná (tj. shodná s originální) dokumentace v českém jazyce |   |   |
| Záruka | Min. 36 měsíců s opravou hardware do druhého pracovního dne v místě instalace, včetně nároku na nové verze firmware/software a aktualizace  |   |   |

**Technická kvalifikace**

Zadavatel požaduje prokázání splnění technické kvalifikace dodavatele: § 79 odst. 2 písm. b) zákona předložením seznamu významných dodávek poskytnutých za poslední 3 roky před zahájením zadávacího řízení včetně uvedení ceny, doby jejich poskytnutí a identifikace objednatele: - Dodavatel do seznamu uvede minimálně 3 (tři) významné dodávky týkajících Log managementu včetně implementace.