# Příloha č.3 - Technická specifikace dodávky

* + 1. **Požadavky na monitorovací systém**

Implementované řešení Security Information and Event Management (SIEM) musí být schopno v reálném čase automaticky shromažďovat, analyzovat a porovnávat vybrané informace z požadovaných informačních systémů (IS) a aplikací tak, aby poskytovalo účinnou podporu pro administraci a provozní dohled jednotlivých systémů.

Výstupem řešení musí být pohledy a reporty odpovídající procesu řízení bezpečnosti v MPO. Výstupy musí směřovat k souladu s řadou norem ISO 2700x.

Záznamy musí obsahovat minimálně následující údaje:

* ID původce – informace o tom, kdo činnost realizoval, toto ID musí být jednoznačné v rámci IS,
* datum a čas akce,
* charakteristika akce (popis) – přidání dat, změna dat, odmazání, atd.

Případy, kdy je nezbytné logování, se posuzují individuálně, vždy se však logují následující případy:

* změna záznamu,
* přidání nového záznamu,
* vymazání záznamu,
* změna struktury dat,
* přihlášení a odhlášení uživatele,
* změna oprávnění uživatele,
* přístupy do vymezených oblastí obsahujících údaje nezbytné pro správu systému (např. konfigurační tabulky),
* přístupy do vymezených oblastí obsahujících informace vyžadující zákonnou ochranu, jako např. osobní údaje subjektů kontrol apod.

Doporučená doba pro uchování výše uvedených záznamů je jeden rok od jejich pořízení dle povahy záznamů a možností daného zařízení/aplikace.

Musí být zachován sběr dat a toků ze všech stávajících síťových prvků a sběr logů ze všech stávajících serverů a informačních systémů.

V souvislosti se zavedením systému do produkčního provozu objednatel požaduje od zhotovitele provést školení administrátorů, systémových pracovníků a běžných uživatelů.

Součástí plnění zhotovitele musí být rovněž zajištění průběžné technické podpory, údržby, HotLine dodaného řešení, a to po dobu tří let od uvedení (předání a převzetí) řešení do rutinního provozu.

|  |  |  |
| --- | --- | --- |
| **Sekce** | **Položka** | **Počet** |
| **Upgrade** | **Licence vč. podpory a služeb výrobce 1. rok** |  |
| D1RNCLL | IBM QRadar Software Install License + SW Subscription & Support 12 Months | 1 |
| D1RNXLL | IBM QRadar Event Capacity 1K Events Per Second License + SW Subscription & Support 12 Months | 1 |
| D1RQALL | IBM QRadar Flows Capacity 10K Flows Per Minute License + SW Subscription & Support 12 Months | 1 |
| D1S2JLL | IBM QRadar Software Node Install License + SW Subscription & Support 12 Months | 1 |
| **Podpora výrobce** | **Podpora a služby výrobce 2. rok** | **Počet** |
| E0NBALL | IBM QRadar Software Install Annual SW Subscription & Support Renewal 12 Months | 1 |
| E0NBGLL | IBM QRadar Event Capacity 1K Events Per Second Annual SW Subscription & Support Renewal 12 Months | 1 |
| E0NBXLL | IBM QRadar Flows Capacity 10K Flows Per Minute Annual SW Subscription & Support Renewal 12 Months | 1 |
| E0NEGLL | IBM QRadar Software Node Install Annual SW Subscription & Support Renewal 12 Months | 1 |
| **Podpora výrobce** | **Podpora a služby výrobce 3. rok** | **Počet** |
| E0NBALL | IBM QRadar Software Install Annual SW Subscription & Support Renewal 12 Months | 1 |
| E0NBGLL | IBM QRadar Event Capacity 1K Events Per Second Annual SW Subscription & Support Renewal 12 Months | 1 |
| E0NBXLL | IBM QRadar Flows Capacity 10K Flows Per Minute Annual SW Subscription & Support Renewal 12 Months | 1 |
| E0NEGLL | IBM QRadar Software Node Install Annual SW Subscription & Support Renewal 12 Months | 1 |
| **Služby** | **Rozšířená podpora zákazníka - 3 roky, 1MD/měsíc** | **Počet** |
| Podpora | * Podpora zákazníka na místě realizace * Změny nastavení dle vývoje prostředí zákazníka | 36 |
| **Služby** | **Řízení projektu** | **Počet** |
| Implementace | * Projektové řízení * Řešení nejasností a problémů při modernizaci * Předání řešení do provozu | 1 |
| **Služby** | **Analýza prostředí v místě zákazníka** | **Počet** |
| Implementace | * Analýza prostředí zákazníka - datové, počítačové, aplikační prostředí k provedení modernizace | 1 |
| **Služby** | **Aktualizace technické dokumentace řešení** | **Počet** |
| Implementace | * Vytvoření realizační dokumentace k provedení modernizace * Aktualizace technické dokumentace modernizovaného řešení (provozní, bezpečnostní a uživatelská) | 1 |
| **Služby** | **Upgrade SIEM** | **Počet** |
| Implementace | * Upgrade SW na stávajícím HW (1. etapa) * Migrace SW ze stávajícího HW na VMware MPO (2. etapa) | 1 |
| **Služby** | **Akceptační testy** | **Počet** |
| Implementace | * Akceptační testy prováděné společně dodavatelem a zákazníkem * Dokumentace výsledků akceptačních testů | 1 |
| **Služby** | **Doškolení správců** | **Počet** |
| Školení | * Zaškolení správců ohledně provedené modernizace systému | 1 |

* + 1. **Systémová podpora licencí od výrobce**

Minimální požadavky na podporu po dobu tří let od rutinního provozu jsou:

* technická podpora systému a provozovaného řešení,
* pravidelná údržba systému na místě plnění,
* služba HotLine a servis.