

Příloha č. 1 – Specifikace předmětu plnění, akceptační kritéria, harmonogram a cena

Specifikace předmětu plnění:

Předmětem plnění smlouvy je implementace systému SIEM a páskových knihoven actiLib Kodiak 6807, dodaných v rámci veřejné zakázky Objednatele č.j.: MV-142306-324/SIK6-2018.

Detailní rozvrh realizovaných činností, pracnost a cena Implementačních služeb jsou uvedeny v následující tabulce:

Nasazení systému SIEM:

Činnost	Pracnost v člověkodnech	Jednotková cena	Cena za příslušnou činnost	Cena za příslušnou činnost /Kč s DPH/
		/Kč bez DPH/	/Kč bez DPH/	
Implementace SIEM	98	x	1 470 000,00 Kč	1 778 700,00 Kč
Zpracování prováděcího projektu	15	15 000,00 Kč	225 000,00 Kč	272 250,00 Kč
Instalace systému a distribuovaných komponent Instalace wincollect	4	15 000,00 Kč	60 000,00 Kč	72 600,00 Kč
Implementace - Konektory na logy a Flow - Parsery - Pravidla	45	15 000,00 Kč	675 000,00 Kč	816 750,00 Kč
Napojení zdrojů součinnost z pohledu nastavení logování, instalace agentů pro sběr logů (wincollect), zaškolení obsluhy	15	15 000,00 Kč	225 000,00 Kč	272 250,00 Kč
Napojení na aplikační logy interpretace stavů	5	15 000,00 Kč	75 000,00 Kč	90 750,00 Kč
Zátěžové testy, Akceptační a bezpečnostní testy	5	15 000,00 Kč	75 000,00 Kč	90 750,00 Kč
Zkušební provoz	5	15 000,00 Kč	75 000,00 Kč	90 750,00 Kč
Vypracování dokumentace	4	15 000,00 Kč	60 000,00 Kč	72 600,00 Kč

Nasazení páskových knihoven actiLib:

Činnost	Pracnost v člověkodnech	Jednotková cena	Cena za příslušnou činnost	Cena za příslušnou činnost /Kč s DPH/
		/Kč bez DPH/	/Kč bez DPH/	
Implementace páskové knihovny actiLib Kodiak 6807 a zálohovacího SW	60,5	x	907 500 Kč	1 098 075 Kč
Instalace HW, propojení na LAN, SAN v souladu s SZR_DOC_20210720_Architektura_a_migrační_plán_0v2.docx	2	15 000 Kč	30 000 Kč	36 300 Kč
Prováděcí projekt	4	15 000 Kč	60 000 Kč	72 600 Kč

Příprava prostředí: POLE: Tvorba LUN na Huawei OceanStore 100 TB. KNIHOVNA: Zapojení drivů knihovny Kodiak do SAN. Naplnění knihovny páskami. SERVER: Osazení serverů do RACK, jejich zapojení do LAN a SAN, nastavení servisního modulu vzdálené správy a RAID. Instalace Windows Server 2022, patchování. Detekci drivů knihovny KODIAK v device managerovi, viditelnost LUN jako připojeného disku. Předání Admin hesel na CIT-TIV. Oba servery vidí navzájem na oba diskové LUN v DC1 a DC2 pro vytváření kopií záloh.	6	15 000 Kč	90 000 Kč	108 900 Kč
Instalace OS na zálohovací servery	1	15 000 Kč	15 000 Kč	18 150 Kč
Instalace IBM Spectrum Protect a napojení na úložiště	4	15 000 Kč	60 000 Kč	72 600 Kč
Instalace zálohovacích klientů, specifické nastavení klientů	4	15 000 Kč	60 000 Kč	72 600 Kč
Příprava prostředí SW: Konfigurace ORACLE RMAN. Schválení úprav v zálohovacích politikách. Konfigurace MSSQL pro účely zálohování (pokud se nebude virtualizovat)	7,5	15 000 Kč	112 500 Kč	136 125 Kč
Konfigurace zálohovacího plánu, podle dokumentu: Návrh_řešení_backup_20210806.docx Konfigurace zálohovacích klientů	20	15 000 Kč	300 000 Kč	363 000 Kč
Finální konfigurace a přepínání zálohovacích úloh, apod	8	15 000 Kč	120 000 Kč	145 200 Kč
Otestování zálohy/obnovy	2	15 000 Kč	30 000 Kč	36 300 Kč
Dokumentace skutečného provedení	2	15 000 Kč	30 000 Kč	36 300 Kč

Akceptační kritéria – pásková knihovna actiLib:

Kontroly proběhnou: zadáním příkazů, screenshotem z IBM SP grafického rozhraní, případně záznamem v logu.

Akceptační kritéria:

- Systém IBM SP je instalován a funkční, do systému je možné přihlášení
- Páskové knihovny jsou zapojené a funkční
- Páskové knihovny jsou fyzicky integrovány do infrastruktury systému ISZR
- Probíhá ukládání zálohování SW Spectrum na disková úložiště
- Probíhá ukládání zálohování SW Spectrum na páskové knihovny
- Zálohovací infrastruktura (páskové knihovny a SW Spectrum) je nastavena a zajišťuje zálohování pro:
 - ORACLE DB
V systému jsou aktivní NODES zálohovacích klientů, úložiště IBM SP je publikované směrem k RMAN
 - Případně ostatní fyzické systémy
V systému jsou aktivní NODES zálohovacích klientů
 - V systému jsou naplánované pravidelné úlohy pro tyto typy záloh (v případě, že jsou napojeny další fyzické systémy)
 - Probíhá záloha interní databáze IBM SP
- Proběhla úspěšná obnova vybrané části databáze z rozhraní RMAN
- Proběhla úspěšná souborová obnova (v případě, že jsou napojeny další fyzické systémy)

Akceptační kritéria SIEM – IBM QRadar SIEM

V případě IBM QRadar SIEM proběhnou kontroly: zadáním příkazů, screenshotem z grafického rozhraní QRadar, případně záznamem v logu. Data o bezpečnostních událostech jsou zpracovávána a vyhodnocována přímo v systému QRadar a z výjimkou notifikací pro administrátory nebudou dále předávána.

- Systém SIEM je instalován a funkční, licence systému je aktivována, do systému je možné přihlášení
- Na SIEM probíhá zaznamenávání bezpečnostních událostí z těchto zdrojů ISZR:
 - Windows Server
 - IIS Web Server
 - UNIX Server (Solaris, RH)
 - DB Oracle Server
 - Cisco IOS zařízení
 - F5 BIG IP zařízení
 - ISZR aplikační log - DB Oracle
- V systému probíhá ukládání událostí z výše uvedených zdrojů, po dobu určenou tzv. retenční politikou
- V systému jsou aktivována korelační pravidla
- Na vznikající kybernetické bezpečnostní události jsou navázány mailové notifikace

Nutné součinnosti SIEM:

- Zajištění odstávek systému
- Zajištění SW QRADAR:
 - 1 x D1RNCLL - IBM QRadar Software Install License
 - 4 x D1S2JLL - IBM QRadar Software Node Install License
 - 1 x D1VRWLL - IBM Security QRadar Data Store Connection License
 - 2 x D1RSOLL - IBM QRadar High Availability Software Install License
 - 1 x D1RP3LL - IBM QRadar Event Capacity 2.5K Events Per Second License
 - 1 x D1RQMLL - IBM QRadar Flows Capacity 50K Flows Per Minute License
- Zajištění HW QRADAR
 - DC1 – QRadar SIEM Console
 - Virtuální server IBM RedHat Appliance
 - 24 VCORE, 64 GB RAM, 10 TB HDD
 - DC1 – QRadar SIEM Processor
 - Virtuální server IBM RedHat Appliance
 - 16 VCORE, 64 GB RAM, 32 TB HDD
 - DC2 – QRadar SIEM Processor
 - Virtuální server IBM RedHat Appliance
 - 16 VCORE, 64 GB RAM, 32 TB HDD

Nutné součinnosti pásková knihovna:

- Zajištění HW:
 - 2x Fyzický SERVER (backup a media server zároveň)
 - Min 1 x 14 CORE CPU GOLD
 - 128 GB RAM
 - 2 x 500 GB SSD nebo SAS 10K rpm na OS
 - 4 x 960 GB SSD na Databázi
 - 2 x FC SAN HBA 8 nebo 16 Gbps – napojení na ActiLib Kodiak 6807 a Diskové pole pro zálohy
 - 1 x Quad-port port 10 GB ETH
- SAN SWITCH – volné porty
 - 8 FC SAN portů per DC (6 pro páskovou knihovnu, 2 backup server) - technicky se bude 8 portů alokovat jako 4 + 4 porty na dvojici SAN switchů v každém DC.

- Úložiště:
 - 100TB na HUAWEI OCEAN STORE v každém DC. LUN s touto kapacitou bude viditelný po SAN z obou zálohovacího serverů.
- Zajištění SW:
 - CIS Standard (MVL 2Lic CoreLic) - (System Center Standard/Windows Server Standard), např.: Windows Server® 2022 Standard,16CORE,FI,No Med,No CAL, Multi Language
 - Licence backup SW s roční podporou výrobce: 100 x D1INFLL - IBM Spectrum Protect Suite Entry Terabyte (1-100) License
- Schválení provozních odstávek
- Zajištění likvidace původní páskové knihovny včetně médií

Harmonogram:

„T“ = datum skutečného zahájení realizace Implementačních služeb, které proběhne nejpozději do 14 dnů od data účinnosti Smlouvy, a to za předpokladu splnění součinnosti Objednatele uvedené v této Příloze č. 1.

Nasazení SIEM:

Činnost	TERMÍN
Zpracování prováděcího projektu	T + 6 týdnů
Instalace systému a distribuovaných komponent Instalace wincollect	T + 8 týdnů
Implementace - Konektory na logy a Flow - Parsery - Pravidla	T + 20 týdnů
Zátěžové testy, akceptační a bezpečnostní testy	T + 21 týdnů
Zkušební provoz	T + 22 týdnů
Vypracování dokumentace	T + 24 týdnů
Celkem	T + 24 týdnů

Nasazení páskových knihoven:

Činnost	TERMÍN
Instalace HW, propojení na LAN, SAN v souladu s SZR_DOC_20210720_Architektura_a_migrační plán_Ov2.docx	T + 1 týden
Prováděcí projekt	T + 8 týdnů
Instalace OS na zálohovací servery	T + 4 týdnů
Instalace IBM Spectrum Protect a napojení na úložiště	T + 4 týdnů
Instalace zálohovacích klientů	T + 10 týdnů

Konfigurace zálohovacího plánu, podle dokumentu: Návrh_řešení_backup_20210806.docx Konfigurace zálohovacích klientů	T + 18 týdnů
Otestování zálohy/obnovy	T + 19 týdnů
Dokumentace skutečného provedení	T + 20 týdnů
Celkem	T + 20 týdnů

