Technická specifikace

1 Úvod

Zadavatel předkládá v rámci výběrového řízení požadavky na doplnění/rozšíření již provozovaných aktiv pořízených zadávacími postupy dle ZZVZ, a plánuje realizovat pořízení systémů doplňujících technologickou úroveň IT infrastruktury, tj. v souladu s § 89 odst. 5 písm.a) ZZVZ.

Lokality, ve kterých budou systémy a technologie aplikovány a provozovány:

Klatovská nemocnice, a.s., Plzeňská 929, 33901 Klatovy
Domažlická nemocnice, a.s., Kozinova 292, 34422 Domažlice
Stodská nemocnice, a.s., Hradecká 600, 33301 Stod
Rokycanská nemocnice, a.s., Voldušská 750, 33701 Rokycany
Nemocnice následné péče Horažďovice, s.r.o., Blatenská 314, 34101 Horažďovice
Nemocnice následné péče Svatá Anna, s.r.o., Kyjovská 607, 34815 Planá

2 Kapacitní rozšíření blokových diskových polí

Bloková disková pole

Doplnění diskových kapacit do stávajících blokových diskových polí.

Stávající předmětná bloková disková pole:

- 2 x Flash Array //X20 R4
- 2 x Flash Array //X20 R3

Zadavatel požaduje:

- Rozšíření kapacity blokových diskových polí Flash Array //X20 o 27TB hrubé kapacity.
- Podpora výrobce 24x7 non stop s 15ti minutovou reakční dobou výrobce vzdáleně a doručením náhradního dílu následujícího pracovního dne v místě instalace na 5 let.

3 VDI Technologie

Zadavatel požaduje dodání 200 licencí pro aktivní uživatele (CCU) Omnissa Horizon Enteprise (dříve VMware) a implementaci do již provozované VDI farmy, která je postavena na technologii Omnissa Horizon Enterprise a disponuje počtem licencí pro cca 450 aktivních uživatelů (CCU).

4 Licence Microsoft RDS CAL

Zadavatel požaduje dodat softwarové licencí typu Microsoft Remote Desktop Services Client Access License (RDS CAL), určené pro přístup zařízení k prostředí Microsoft Windows Server.

Technická specifikace požadovaných licencí:

- Microsoft Remote Desktop Services CAL

- Device CAL (licence přiřazená konkrétnímu zařízení)
- Verze: určeno pro Windows Server 2022, s možností zpětné kompatibility (downgrade) pro starší verze systému Windows Server
- trvalá (perpetual) licence, bez časového omezení
- Jazyková verze - multilanguage (včetně CZ/EN)
- Způsob dodání elektronicky – prostřednictvím Microsoft 365 Admin Center
- Počet licencí požadovaných zadavatelem je uveden v příloze č. 1 – Krycí list

Požadavky na plnění:

- originální licence pocházející z oficiální distribuční sítě Microsoft a umožňující jejich evidenci a správu v licenčním portálu Microsoft.
- Licence nesmí být typu OEM, second-hand nebo jinak omezené.

5 Systém pro vyhodnocování bezpečnostních událostí

Parametry systému

Níže uvedené minimální požadavky na systém jsou mandatorní, pokud systém nabídnutý v rámci zadávacího řízení těmito funkcemi nedisponuje, bude z hodnocení vyřazen.

Požadavek na funkce pro detekce událostí:

- Detekce událostí je možná v reálném čase, případně nad historickými daty.
- Je k dispozici knihovna předdefinovaných korelačních pravidel pokrývajících základní scénáře útoků (např. MITRE ATT&CK, Cyber Kill Chain), v minimálním počtu 400 korelací.
- Detekce anomálií je podporována na základě metrik (zejména EPS, frekvence událostí, chování uživatelů, síťové vzory).
- Detekce a výsledky korelace jsou zobrazovány v centrální konzoli s možností filtrování, třídění a přiřazování priorit.
- Systém umožňuje korelaci událostí z více logovacích zdrojů a systémů současně.
- Je podporována tvorba, editace a nasazení vlastních korelačních pravidel pomocí grafického editoru nebo textového rozhraní.
- Upozornění na detekované události je distribuováno prostřednictvím e-mailu, SMS nebo integračních rozhraní (např. MS Teams, Slack, SIEM/SOAR API).

Požadavek na integraci a sdílení

- Systém je schopen integrovat informace z globálních i lokálních threat intelligence feedů (TI).
- Podporuje použití standardních formátů a protokolů (STIX, TAXII, JSON).
- Možnost rozšiřování logů o indikátory kompromitace (IoC) získané z TI zdrojů – IP adresy, URL, hashe souborů, domény.
- Umožňuje import a správu vlastních seznamů IoC vytvářených zadavatelem.
- Aktualizace TI probíhá automaticky a v pravidelných intervalech, s možností manuální aktualizace.
- Systém umožňuje napojení na komerční i komunitní informační služby o hrozbách a incidentech.

- Zadavatel požaduje, ab import bezpečnostních seznamů a indikátorů probíhal v reálném čase, aby bylo možné okamžitě detekovat události odpovídající známým hrozbám.

Funkce pro reakce na incidenty

• Systém umožní automatické případně poloautomatické reakce na definované události.

• Systém podporuje workflow pro řízení bezpečnostních incidentů (incident management), včetně logování kroků a změn stavů.

• Opatření a reakce na incidenty je možné v systému navázat na korelační pravidla nebo detekce hrozeb.

• Je požadována podpora těchto akcí/aktivit:

- blokace IP,
- deaktivace uživatelského účtu v AD,
- izolace zařízení,
- generování ticketu v helpdesk systému,
- odeslání notifikací.

• Zadavatel požaduje možnost definice vlastních reakčních scénářů (playbooks) a tyto scénáře je možné sdílet.

• Systém podporuje integraci se SOAR nástroji pro rozšířené automatizace reakcí.

• Aktivity jsou auditovány a současně je k dispozici historie zásahů a provedených kroků.

Licenční pokrytí

Zadavatel požaduje, aby řešení je schopno vyhodnocování logů v rozsahu min. 5000 událostí/sec, a v rámci licenční politiky nevznikla limitace na velikost uložení dat případně počet uložených souborů.

Implementace systému

• Způsob sběru a zpracování dat z jednotlivých zdrojů bude detailně popsán v předimplementační analýze a v dokumentu Solution Design.

• Dodavatel zajistí podporu integrace i pro zdroje dat, které nejsou v systému nativně podporovány, a to formou tvorby vlastních zásuvných modulů nebo konektorů. Pokud zadavateli vznikne potřeba integrace takového systému, dodavatel zajistí implementaci bez dodatečných nákladů.

• Dodavatel připraví a nakonfiguruje všechny nezbytné konektory, korelační pravidla a základní reakční scénáře potřebné pro provozní použití.

• Součástí implementace je příprava a předání až 20 reportů a dashboardů, pokrývajících klíčové požadavky zadavatele (např. provozní, bezpečnostní a compliance reporty).

• Dodavatel zajistí napojení systému na infrastrukturu zadavatele (např. MS Active Directory, tiketovací systém Alvao, síťová zařízení Aruba, servery).

• Před předáním do produkčního prostředí proběhne testování sběru dat, korelačních pravidel, reakčních scénářů a výstupních reportů.

• Dodavatel poskytne dokumentaci k implementovaným modulům, konektorům a vytvořeným scénářům.

• V rámci implementace provede dodavatel školení administrátorů a bezpečnostního týmu zadavatele.

• Dodavatel zajistí, že řešení bude po implementaci připraveno k produkčnímu nasazení, včetně zálohovacích mechanismů. Zadavatel využívá pro zálohování systém Veeam.

6 Systém pro centrální správu koncových zařízení

Zadavatel požaduje moderní, rozšířitelný, modulární Systém, založený na běžně používaných technologiích a vývojových standardech, který zajistí efektivní správu koncových stanic (desktopy, notebooky), serverů (fyzických i virtuálních) a bude splňovat bezpečnostní standardy v souladu s připravovanou novelou ZKB.

Systém musí být homogenní z hlediska aplikačního software (jeden výrobce) i databázového prostředí. Dodavatel zajistí příslušnou licenci pro DB server. Musí být použit pouze jeden typ databáze (např. MS SQL, Oracle, aj.) pro celé řešení. Licence pro databázi musí být součástí dodávky.

Zadavatel akceptuje nabídku na Systém provozovaný v cloudovém prostředí. V takovém případě zadavatel požaduje, aby veškeré náklady spojené s touto formou provozu systému byly součástí předložené nabídky.

Rozsah požadované zakázky je dodávka Systému, instalace, implementace a školení administrátorů.

Základní informace o IT prostředí zadavatele

Zadavatel:

- aktuálně nedisponuje softwarovým řešením pro centrální správu koncových zařízení a serverů.
- provozuje virtuální prostředí na platformě VMware.
- provozuje serverovou platformu primárně na OS MS Windows server (verze 2019 nebo 2022).
- jako základní prohlížeč používá MS Edge.

Zaměstnanci zadavatele, kteří budou využívat přístup do Systému, mají přidělený adresný jmenný účet v AD.

6.1. Požadavky na bezpečnost, zálohování a správu

Systém bude provozován v režimu 24×7, servisní výpadky provozu pro provedení aktualizací bude prováděno dle oboustranně odsouhlaseného harmonogramu a v předem stanovených časových termínech.

Systém musí umožnit aplikovat režim řízení a nastavení více úrovní přístupových oprávnění pro uživatele systému. Jednomu uživateli může být přiřazeno více rolí.

Systém musí umožnit nastavení různých úrovní přístupů pro jednotlivé role uživatelů. Nastavit jednotlivým uživatelům povolenou funkcionalitu a rozsah dat, ke kterým mohou přistupovat.

Systém musí obsahovat nástroje na administraci těchto procesů s musí umožnovat synchronizaci uživatelů dle skupin v MS AD, ke kterým budou v SW přiřazovány příslušné role.

Systém musí umožnit hromadnou úpravu práv uživatelů změnou práv pro konkrétní roli.

Systém musí umožnit opravu klíčových dat pouze uživateli s příslušnými právy.

Systém zajistí identifikaci a autentizaci každého uživatele při přístupu, a to v návaznosti na parametry uživatelského účtu v AD.

Systém musí umožnit zaznamenání aktivity uživatele a změn dat.

Zadavatel provádí zálohování pomocí stávajícího systému Veeam, ať už aplikační nebo databázové části. Dodavatel v podané nabídce předloží a popíše způsob zálohování a archivace dat a Systému s přihlédnutím k zálohovacímu systému zadavatele.

Dodavatel předloží jako součást dokumentace k Systému zpracovaný návrh dokumentace pro případ havárie celého nebo některé části systému – Disaster Recovery plán, s popisem nezbytných postupů a činností pro úplné obnovení jeho běhu. S každou novou verzí, případně významnou změnou prostředí, musí proběhnout jeho revize a případně aktualizace.

Přístupy z aplikační části do databáze musí být realizován pomocí účtů s nezbytnými oprávněními pro danou činnost, zadavatel neakceptuje požadavek na provoz privilegovaný účet s právy „administrátorského“ typu, ani jiný s neomezenými oprávněními pro dané databázové prostředí.

Využívané webové služby musí umožnit zabezpečení pomocí SSL certifikátu zadavatele.

Veškeré nastavení všech součástí Systému je nutné provádět v souladu se zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (ZKB) a Vyhlášky č. 82/2018 Sb. (Vyhláška o kybernetické bezpečnosti).

Čas pro Systém je synchronizován z domény nebo z lokálních NTP (network time protocol) serverů.

6.2. Implementace

Zadavatel požaduje před zahájením samotné implementace předložení implementačního plánu. Plán vypracuje dodavatel a bude v souladu s požadavky zadavatele, které jsou uvedené v této technické specifikaci a s výsledky analýzy prostředí, kterou si provede dodavatel před začátkem implementace projektu.

Bude vytvořen implementační tým, jehož součástí budou pracovníci Dodavatele a Zadavatele.

Minimální požadavky, které budou zohledněny v plánu:

- Časový harmonogram prací tak, aby byly dodrženy požadavky definované touto zadávací dokumentací.
- Návrh konfigurace systémové infrastruktury pro provoz Systému v IT prostředí zadavatele obsahující grafický a textový popis architektury systému a specifikaci prvků.

Akceptační kritéria nasazení Systému:

- Nainstalovaná aplikační část SW
- Školení pro role:
  - Systém Owner
  - Systém Administrátor
- Nasazení klientského SW na 10% koncových stanic
- Úspěšná demonstrace Remote control v každé lokalitě
- Patching: >90% zařízení přidaných do Systému splňuje compliance do 7 dnů od nasazení
- Bezpečnostní baseline: >90% zařízení přidaných do Systému splňuje compliance do 7 dnů od nasazení

Po akceptaci kritérií zadavatel dokončí nasazení Systému do své IT infrastruktury vlastními silami.

6.3. Obecné funkce systému

Níže uvedené požadavky jsou mandatorní, pokud systém nabídnutý v rámci zadávacího řízení těmito funkcemi nedisponuje, bude z hodnocení vyřazen.

ID	Požadavek	Ano/Ne
OB-1	Modularita a Škálovatelnost Možnost rozšíření o další moduly, rozšíření množství spravovaných koncových bodů, uživatelů a rolí.	
OB-2	Varianta nasazení: OnPremise nebo Cloud nasazení. Součástí nabídky je specifikace požadavků na HW a připojení.	
OB-3	Integrace s objekty z AD.	
OB-4	Webové rozhraní: Pokud řešení obsahuje webové konzole, musí být zajištěna kompatibilita s aktuálně podporovaných verzích MS Edge.	
OB-5	Možnosti nasazení proxy/relay/gateway v lokalitách	
OB-6	Správa prostředí z jedné konzole	
OB-7	Dodávka projektové dokumentace a provozních manuálů.	
OB-8	Možnost spravovat koncová zařízení s OS Windows, Windows Server	
OB-9	Možnost spravovat fyzická zařízení i virtuální zařízení	
OB-10	Lokalizace prostředí v českém nebo anglickém jazyce	
OB-12	Možnost správy koncových bodů po LAN i WAN a možnosti optimalizace provozu po WAN (proxy/relay/gateway…)	
OB-13	Možnost zasílání e-mailů přes Office365	
OB-14	Možnost definovat role v tomto rozsahu (včetně předpokládaných počtů osob jednotlivých rolí): **UEM System Owner** – kompletní správa systému - 2 osoby **UEM Administrator** – tvorba/úprava instalačních balíčků a instalací OS - 2 osoby	

	Endpoint Technician – Spouštění instalací OS a SW balíčků na koncové stanice, připojování na vzdálenou plochu koncových stanic - 7 **Server Technician** – Spouštění instalací OS a SW balíčků na servery, připojování na vzdálenou plochu koncových stanic a serverů - 5 **Remote Support Technician** – připojování na vzdálenou plochu koncových stanic: 7	

6.4. Funkce Systému – Správa SW balíčků a distribuce aplikací

ID	Požadavek	Ano/Ne
SW-1	Repozitář SW balíčků: Centrální úložiště pro MSI/EXE/Skripty, verzování balíčků.	
SW-2	Směrování instalací: Dynamické přiřazení podle umístění koncového zařízení v OU v AD, skupin v AD, lokality, HW parametrů, názvového vzoru apod.	
SW-3	Tiché instalace a rollback: Plná podpora unattended instalací vč. odinstalace/rollback na předchozí verzi.	
SW-4	Plánování a vlny: Nasazování v oknech údržby (např. mimo pracovní dobu), pilotní okruhy, Rozfázování instalací v případě více koncových bodů.	
SW-5	Závislosti: Deklarace závislostí mezi jednotlivými SW balíčky.	
SW-6	User experience: Notifikace uživateli o plánované instalaci, odklad instalace, řízené restartování s UX okny.	
SW-7	Distribuce obsahu: Peer-to-peer/branch caching, řízení šířky pásma a throttling.	
SW-8	Skriptování a opravy: Pre/post install skripty, remediation (opravné skripty při selhání).	
SW-9	Telemetrie a audit: Přehled úspěšnosti/chyb, detailní logy.	
SW-10	Možnost instalace OS přes PXE	

6.5. Funkce systému – Vzdálená správa a ovládání klientů

ID	Požadavek	Ano/Ne
RE-1	Remote control: Bezobslužné připojení (i na přihlašovací obrazovce) a převzetí ovládání (myš a klávesnice) koncového zařízení.	
RE-2	Souhlas uživatele – Možnost nastavení schvalování připojení ze strany uživatele	
RE-3	Šifrované relace	

RE-4	Auditní stopa využití Remote control	
RE-5	Specifikace skupin uživatelů a jejich povolení přístupu na konkrétní stroje (např. server tým může využít Remote control na servery, ale Endpoint tým může pouze na stanice)	
RE-6	Nástroje podpory: • Chat • Přenos souborů • Vzdálené spouštění sktiptů/PowerShellu • Inventář HW/SW v relaci • Správa služeb/procesů	
RE-7	Vícenásobné připojení na koncovou stanici v jeden okamžik (poskytování podpory více techniky najednou	
RE-8	Podpora zobrazení více monitorů u připojovaných koncových zařízení	

6.6. Funkce systému – Patch management

ID	Požadavek	Ano/Ne
PA-1	Možnost vytvořit a nastavit workflows pro nasazení patchů a updatů. Např. AD Testovací skupina 1 → AD Testovací skupina 2 → Schválení nasazení do produkce → produkce. Pro různé typy patchů (např. priorita nízká/střední/kritická) různá workflow	
PA-2	Přístup a správa Windows Update – Jakožto náhrada za WSUS	
PA-3	Katalog updatů pro produkty třetích stran (např. Adobe/Java/prohlížeče/ZIP nástroje apod)	
PA-4	Možnost tvorby vlastních balíčků (které nebudou v katalogu)	
PA-5	Mimo VPN: Aktualizace i mimo firemní síť (externí ordinace, home office…) bez nutnosti VPN.	
PA-6	Reporting o úspěšnosti/neúspěšnosti aplikace patchů	
PA-7	Možnost automatického nasazení nových patchů (včetně předpřipravených workflows)	
PA-8	Plánování a vlny: Nasazování patchů v oknech údržby (např. mimo pracovní dobu), pilotní okruhy, Rozfázování instalací v případě více koncových bodů.	
PA-9	Možnost aktualizace driverů	

6.7. Funkce systému – Řízení rizik, zranitelností a compliance

ID	Požadavek	Ano/Ne
CO-1	Sken zranitelností (CVE): Korelace nainstalovaných verzí s databází CVE, označení severity a prioritizace. Pro MS i 3rd party aplikace	
CO-2	Konfigurační compliance: kontrola konfiguračních zranitelností (např. kontroly BitLocker/Firewall/AV definic/heslových politik/služeb, detekce odchylek a návrhy nápravy).	
CO-3	Remediace: Automatizovatelné remediation steps (instalace chybějící záplaty, korekce registru/politiky atp). Opravné kroky předpřipravené od výrobce/dodavatele.	
CO-4	Aplikace: Whitelist/blacklist aplikací	
CO-5	Reporty a audity: Předpřipravené šablony reportů (trendy, stav souladu, export pro audit/ISO/NIS2).	

6.8. Funkce systému – Reporting a přehledové dashboardy

ID	Požadavek	Ano/Ne
RP-1	Centrální dashboard: Přizpůsobitelný, v reálném čase: online/offline, stav distribucí, patch compliance, neplnění politik	
RP-2	Předdefinované reporty: Chybějící kritické záplaty/zranitelnosti, instalovaný SW, nevyhovující zařízení, top-N rizik	
RP-3	Plánované rozesílání reportů: Automatická tvorba a e-mail distribuce (týden/měsíc) na cílové skupiny	
RP-4	Vlastní reporty/dotazy: Tvorba custom výstupů, filtry, dotazy, export pro ad-hoc analýzy	
RP-5	Možnost automatizovaného e-mailového posílání předefinovaných reportů	