

Příloha č. 2 Zadávací dokumentace – Formulář technických požadavků

VZ Zvýšení kybernetické bezpečnosti Zlínského kraje

Dodávka a implementace řešení pro zaznamenávání činnosti VIP účtů a zajištění následné podpory

Číslo	Minimální požadované vlastnosti a funkce (požadavky)	Splňuje dodavatel požadavky (Ano/Ne)	Popis naplnění požadavků dodavatelem
1.	Zavedení zaznamenávání činností VIP účtů administrátorů a uživatelů třetích stran		
1.0	dodávané řešení ani žádná z jeho částí nesmí být v době podání nabídky v režimu End of Sale / End of Support	Ano	Odkaz na politiku technické podpory výrobce: https://www.ekransystem.com/sites/default/files/file_resources/Ekran%20System%20Support%20and%20Maintenance%20Policy.pdf
1.1	celé řešení bude podporovat provoz ve virtualizovaném prostředí KÚZK	Ano	Nástroj lze ve virtualizovaném prostředí provozovat bez omezení.
1.2	záznam všech aktivit spojených s použitím privilegovaného účtu na monitorovaných systémech (servery a koncové stanice) - možnost záznamu grafickou formou (zejména screenshot, videozáznam) - v rámci nahrávky jsou zaznamenávány uživatelské vstupy (key-logging) a výstupy na obrazovku - <u>přířazení nových relací patřičným uživatelům</u>	Ano	Toto je hlavní funkcionality nástroje - zaznamenávání video logů uživatelských relací s metadaty a volitelně též zaznamenávání stisků kláves.
1.3	získávání detailních metadat během nahrávané uživatelské relace (stisknuté klávesy, názvy aktivních oken, textové řetězce z oblastí, kde proběhla aktivita (např. klik myši na definované tlačítko/záložku/...))	Ano	Snímky lze zaznamenávat v definované časové periodě nebo (a to je obvyklejší) jen při aktivitě uživatele. Ke každému snímku jsou zaznamenána metadaty.
1.4	v metadatech musí být možné vyhledávat dle textových řetězců	Ano	V rámci nahraných uživatelských relací lze v metadatech vyhledávat i zadáním klíčových slov.
1.5	ukládání nahraných uživatelských relací na definované úložiště Objednatele v šifrované podobě	Ano	Data lze šifrovaně ukládat v databázi nebo do souborového systému.
1.6	přehlednou správu politik pro monitoring nejen privilegovaných účtů	Ano	Uživatelské rozhraní je přímočaré a intuitivní. Politiky lze tvořit pro skupiny nebo i pro jednotlivá zařízení.
1.7	počet monitorovaných systémů: - 1x Terminal server (Windows Server 2012 R2 a vyšší) – Jump Server GW - 5x Published App Agent – určeno pro monitoring publikovaných aplikací, licence pro každý terminálový server - 10x Windows Server (Windows Server 2012 R2 a vyšší) - 5x Windows Desktop (Windows 7 Enterprise a Windows 10 Enterprise)	Ano	Naše nabídka plně pokrývá požadovaný rozsah licencí. Námi nabízený nástroj nevyžaduje extra licenci pro "Published App Agent", postačuje licence pro terminálový server.
1.8	aplikace musí umožnit správu rolí (auditor, správce apod.)	Ano	Nástroj podporuje detailní škálování přístupových oprávnění.
1.9	uživatelé mohou být dle nastavení Objednatele upozorněni na skutečnost, že jejich aktivita je nahrávána	Ano	Po přihlášení může být uživateli zobrazeno informační dialogové okno s definovatelným textem. Lze vynutit i uvedení důvodu přihlášení k systému.
1.10	auditování, monitoring a nahrávání aktivit administrátorů na serverech při vzdáleném i lokálním přihlášení	Ano	Nabízíme agentský systém, nahrává i lokální uživatelské relace.
1.11	auditování, monitoring a nahrávání aktivit externích uživatelů vykonávající vzdálenou správu v LAN Objednatele, pomocí předřazené virtuální administrační stanice nebo terminálového serveru	Ano	Nahrávány jsou i uživatelské relace realizované přes vzdálenou plochu. Včetně podpory pro terminálový server a publikované aplikace.
1.12	auditování, monitoring a nahrávání aktivit vybraných interních zaměstnanců využívajících virtuální desktopy, počítače nebo notebooky	Ano	Nahrávání lze omezit i jen na konkrétní uživatele.
1.13	schopnost zpětně přehrávat uživatelské relace ve formě videosekvence	Ano	Jedná se o hlavní funkcionality nástroje.
1.14	schopnost exportu nahraných uživatelských relací (formou printscreenů obrazovek a to včetně metadat) pro tvorbu dokumentace, nebo prokazování incidentů	Ano	Nástroj podporuje export do podoby spustitelného souboru, který umožňuje přehrávání zaznamenané relace stejným způsobem jako webové rozhraní.
1.15	každá událost v logu, má vazbu pomocí URL adresy na konkrétní místo videosekvence, kde k této události došlo	Ano	Událost v tzv. "SIEM" logu obsahuje odkaz na konkrétní místo videosekvence.
1.16	integrována funkce šifrování nahraných uživatelských relací, před jejich uložením	Ano	Data lze šifrovaně ukládat v databázi nebo do souborového systému.

1.17	integrována funkce integrity nahraných uživatelských relací, pokud je integrita porušena, jsou tyto relace v přehledu označeny	Ano	Nástroj při přehrávání relace kontroluje její integritu. Lze aktivovat i mechanismus explicitní kontroly integrity nahraných relací.
1.18	politikou je možné definovat uživatele, kteří budou, nebo naopak nebudou nahrávání	Ano	Nahrávání lze omezit i jen na některé uživatele. Pozitivním nebo negativním filtrem.
1.19	politikou je možné definovat aplikace (aplikace, nebo URL adresa v případě webových aplikací), které budou, nebo naopak nebudou nahrávány	Ano	Nahrávání lze omezit i jen na některé aplikace. Pozitivním nebo negativním filtrem.
1.20	integrováný reporting, s možností tvorby vlastních reportů o aktivitách uživatelů, vč. exportu do CSV nebo XLS nebo XML nebo HTML pro následné analýzy	Ano	Nástroj podporuje i tvorbu vlastních reportů s možností exportu do všech uváděných i dalších formátů.
1.21	Integrace do MS AD KÚZK	Ano	Při instalaci na server v doméně lze bez potřeby další konfigurace přiřazovat přístupová oprávnění uživatelům nebo skupinám z AD.
1.22	Integrace do provozovaného SIEM KÚZK	Ano	Nástroj podporuje generování tzv. "SIEM" logu ve formátu CEF nebo LEEF.
1.23	Pro chod VApp/VM v prostředí TCK KÚZK bude možnost vyhrazení HW prostředků s následující charakteristikou: - počet podporovaných vCPU: 8 - počet virtuálních NIC: 2 - velikost úložiště virtuálního stroje / při integraci na SIEM: 80 GB / 500 GB - velikost operační paměti virtuálního stroje: 16 GB - velikost databáze / instance na sdíleném MS SQL 2014/2016 řešení KÚZK: 10 GB	Ano	Nabízené HW parametry VM jsou zcela dostatečné pro provozování námi nabízeného nástroje, konkrétně komponenty EKRA Server.
2.	Požadované služby		
2.1	Služby v rámci dodávky		
2.1.1	Projektové řízení dodávky řešení.	Ano	Dodávka řešení bude řízena projektovým manažerem firmy DATASYS.
2.1.2	Zpracování návrhu řešení implementace jednotlivých částí – Prováděcí projekt včetně návrhu řešení specifikovaný v Příloze č. 3 Povinná struktura Prováděcího projektu včetně návrhu řešení.	Ano	Zpracujeme prováděcí projekt včetně návrhu řešení v takto definované struktuře.
2.1.3	Dodávka, implementace, instalace, zapojení a konfigurace všech částí dle Prováděcího projektu včetně návrhu řešení.	Ano	Nabízíme kompletní dodávku řešení.
2.1.4	Vytvoření a předání Objednateli zálohy konfigurace.	Ano	Po dokončení implementace předáme Objednateli zálohu konfigurace (export databáze) a zálohu tzv. master certifikátu.
2.1.5	Ověření funkčnosti dodaného řešení a jeho částí.	Ano	Akceptační testování je běžnou součástí námi realizovaných projektů.
2.1.6	Dodávka dokumentace dodaného vybavení a jeho částí.	Ano	V návaznosti na prováděcí projekt zpracujeme po dokončení implementace též tzv. "Provozní dokumentaci". Součástí dodávky nástroje je samozřejmě též poskytnutí standardní produktové dokumentace od výrobce.
2.1.7	Kvalifikované seznámení administrátorů – seznámení s funkcionalitami, obsluhou dodávaného řešení a jeho budoucím provozem v rozsahu minimálně 1MD.	Ano	Provedeme zaškolení administrátorů Objednatele v rozsahu 1 MD. Doporučujeme rozdělit do dvou termínů po čtyřech hodinách.
2.1.8	Implementace metodik a pracovních postupů.	Ano	Doporučíme osvědčené postupy a po jejich odsouhlasení Objednatelem je zaneseme do konfigurace nástroje.
2.1.9	Provedení zkušebního provozu.	Ano	Součástí naší nabídky je zesílená technická podpora během dvoutýdenního ověřovacího provozu.
2.2	Podpora provozu		
2.2.1	Poskytnutí podpory provozu díla min. 66 měsíců.	Ano	Součástí naší nabídky je i podpora výrobce na požadovanou dobu.
2.2.2	Požadavek na servisní zásah může být objednatel uplatněn: - systémem helpdesk na adrese (Zhotovitel je povinen zpřístupnit svůj helpdesk Objednateli nejpozději v průběhu fáze 2.) - e-mailem na adrese upřesněné Zhotovitelem, pokud není možno použít helpdesk, Objednatel požadavek do helpdesku dodatečně doplní - telefonem na čísle upřesněné Zhotovitelem, pokud není možno použít helpdesk, Objednatel požadavek do helpdesku dodatečně doplní	Ano	DATASYS provozuje vlastní helpdeskové středisko v režimu 24x7 a servisní zásah může být Objednatelem uplatněn všemi třemi uváděnými kanály.

2.2.3	Systém helpdesk musí zajistit: - jednoduché a pohodlné vkládání požadavků uživatelem podle jeho oprávnění - seznam všech hlášených požadavků s historií a aktuálním stavem řešení a řešitelem - e-mailové notifikace při změně stavu řešení požadavku - možnost nastavení priorit řešení - přístup k aplikaci přes webový prohlížeč 24 hodin denně – bez nákladů na software pro Objednatele	Ano	Webové rozhraní našeho helpdesku je dostupné na adrese https://helpdesk.datasys.cz .
2.2.4	Smluvní podpora díla zahrnuje především následující: - Odstranění nedostatků implementace zjištěných ve fázi 3 uvedeně ve smlouvě o dílo. - Řešení závad SW v místě instalace v souladu s SLA dle 2.2.5 - Změna konfigurace dodaného SW v souladu s SLA dle 2.2.5 - Konzultace. - Poskytování update a upgrade SW, jejich instalace. - Přístup k technické podpoře výrobce dodaného SW. - Provoz helpdesk systému sloužícího pro evidenci veškerých požadavků na podporu a reporting řešení závad a požadavků za fakturační období	Ano	Nabízíme zajistit smluvní podporu v kompletním požadovaném rozsahu.
2.2.5	Specifikace požadovaných služeb (SLA), které je zhotovitel povinen zajistit: Závady a požadavky jsou klasifikovány dle jejich závažnosti a provozních podmínek na tři kategorie důležitosti: Vysoká - závady vylučující užívání systému nebo jeho důležité a ucelené části (tj. problémy zabraňující provozu systému), provoz systému je zastaven. - požadavky vysoké priority řešení, zejména ohrožující provoz nebo bezpečnost díla či jeho částí - potvrzení o přijetí závad a požadavků do 1 hodiny - max. doba do vyřešení závad a požadavků od nahlášení do 3 pracovních dnů* Střední - závady způsobující problémy při užívání a provozování systému nebo jeho části, ale umožňující provoz systému. Provoz systému je omezen, ale činnosti mohou pokračovat určitou dobu náhradním způsobem. - požadavky střední priority řešení - potvrzení o přijetí závad a požadavků do 1 hodiny - max. doba do vyřešení závad a požadavků od nahlášení do 5 pracovních dnů* Nízká - provoz systému je závadou ovlivněn, ale může pokračovat jiným způsobem, např. organizačními opatřeními. - ostatní požadavky - potvrzení o přijetí závad a požadavků do 1 hodiny - max. doba do vyřešení závad a požadavků od nahlášení do 10 pracovních dnů* Řešení závad a požadavků probíhá v režimu 8 x 5 tj. v pracovní dny od 8:00 do 16:00. *pracovním dnem se rozumí doba od 8.00 do 16.00 hodin v pracovní dny pondělí až pátek (mimo víkendy a svátky platné v České republice), přičemž platí, že max. doba vyřešení závad a požadavků se počítá od hodiny nahlášení závady či požadavku.	Ano	Nabízíme zajistit smluvní podporu v kompletním požadovaném rozsahu.
2.3	Dokumentace		
2.3.1	V rámci plnění bude dodána zhotovitelem kompletní dokumentace řešení (dokumentace může být jedním dokumentem, nicméně musí obsahovat všechny relevantní informace) obsahující minimálně:	Ano	Dodáme formou jednoho dokumentu, který bude obsahovat všechny relevantní informace.
2.3.2	Podrobná systémová a bezpečnostní dokumentace (administrátorská dokumentace) v českém jazyce: - popis skutečného provedení řešení min. ve struktuře dle Prováděcího projektu včetně návrhu řešení; - princip aktualizace; - seznam licencí.	Ano	Dokument s názvem "Provozní dokumentace" bude obsahovat popis skutečného provedení, popis principů aktualizace i přehled licencí.
2.3.3	Kompletní provozní dokumentace ke všem částem v českém nebo anglickém jazyce.	Ano	Dokument s názvem "Provozní dokumentace" bude zpracován v českém jazyce, standardní produktová dokumentace je výrobcem zpracována v jazyce anglickém.