

Název zakázky: Zvýšení kybernetické bezpečnosti v KSÚSV

Předmět plnění: Pořízení systému pro ukládání a správu provozních dat z IT infrastruktury a aplikací.

Obecné požadavky:

- Hardwarová appliance pro zpracování a ukládání dat o událostech z aplikací, operačních systémů a síťového hardwaru bez potřeby externích aplikací.
- podpora vysoké dostupnosti a škálovatelnosti (možnost doplnění o další hardwarový nod s konfigurací v redundantním módu HA/rozšíření výkonu).
- Jednotné webové rozhraní pro administraci i provoz se správou uživatelských rolí a definicí přístupových práv.
- Ověřování uživatelů přes externí LDAP/AD s možností záložního lokálního ověření.
- Konfigurace prostřednictvím grafického rozhraní bez nutnosti znalosti syntaxe kódu a programovacího jazyka.
- Podpora protokolů Syslog (RFC5424), RELP, RAW, CEF, LEEF, JSON (RFC8259).
- Sběr strojových dat z databází MySQL, Oracle a PostgreSQL.
- Převod zpracovávaných logů do jednotného formátu s automatickou normalizací a zachováním originální zprávy.
- Automatické přidávání metadat k událostem a možnost vytváření uživatelských parserů pro nepodporovaná zařízení bez úprav konfiguračních souborů a stejně tak možnost úprav již předdefinovaných parserů.
- Real-time ladění uživatelsky definovaných parserů s okamžitým náhledem výsledků
- Uchování původní časové značky a vytvoření důvěryhodného časového razítka při přijetí dat
- Zabezpečení uložených dat proti mazání nebo úpravě po celou dobu retence
- Jednoznačná identifikace každého zpracovaného logu
- Filtrace nerelevantních událostí přes grafické rozhraní bez nutnosti kódování
- Konsolidace a uložení logů na interním úložišti systému
- Okamžité a jednotné prohledávání všech typů uložených dat bez nutnosti jejich importu nebo dekomprese
- Možnost vytváření různých uživatelských pohledů a export dat
- Aktualizace systému prostřednictvím centrální webové správcovské konzole.
- Lokalizace konfiguračního rozhraní a dokumentace do češtiny a angličtiny.
- Možnost zálohování systému i dat na externí systém automatizovaně i ad-hoc. Zálohy jsou efektivně komprimovány a umožňují obnovení bez ohledu na verzi systému, ve které byly pořízeny.

Hardwarové parametry:

- Hardwarová appliance v rackovém provedení s maximální velikostí 1U včetně příslušenství pro montáž do 19“ racku.
- Min. 24 TB kapacity pro ukládání dat (zabezpečeno RAID 5 nebo 6)
- Konektivita 4× 1Gbit LAN porty + 1× dedikovaný 1Gbit management port
- Redundantní napájecí zdroje a ventilátory vyměnitelné za provozu
- Integrované řešení pro vzdálenou správu hardware

Výkonnostní požadavky:

- Systém umožňuje příjem událostí z neomezeného počtu zařízení bez licenčních omezení. Počet zpracovaných událostí není omezen licencí na základě objemu dat v GB za den.
- Trvalý průměrný příjem alespoň 2000 událostí za sekundu při zprávách o průměrné délce minimálně 700 bajtů.
- Při špičkovém zatížení příjem alespoň 4000 událostí za sekundu po dobu minimálně 10 minut, při průměrné velikosti zpráv 700 bajtů.
- Možnost exportu dat ve formátu vhodném pro strojové zpracování, bez omezení na množství nebo obsah exportovaných dat. Při exportu je možné vybrat specifikovaná pole, která mají být zahrnuta.

Alerty:

- Detekce, korelace a generování upozornění na základě uživatelsky definovaných podmínek
- Nastavení alertů a korelací prostřednictvím grafického rozhraní.
- Uživatelsky definovatelný text e-mailového alertu s podporou automaticky vkládaných proměnných podle vyhodnocení události.

Sběr dat z prostředí Microsoft:

- Sběr dat z prostředí Microsoft s možností centrální konfigurace logovacích politik.
- Nativní sběr dat z prostředí Office 365/Microsoft 365 bez ohledu na typ použité licence a bez nutnosti instalace dodatečných externích komponent.
- Možnost vyloučení konkrétních Event ID při sběru dat z Microsoft prostředí.
- Filtrování událostí při sběru dat z Windows ještě před samotným odesláním logu.

Sběr dat z poboček:

- Centrálně řízený sběr událostí na pobočkách s odolností vůči ztrátě dat i při zatížení linek.
- Sběr dat ze vzdálených poboček je možné realizovat pomocí hardwarové appliance nebo virtuálního appliance pro VMware ESXi a Hyper-V.
- Automatické navázání spojení pobočky s centrálním systémem a šifrování přenášených dat.
- Komunikace přes definovaný TCP/UDP port s podporou firewall konfigurace a QoS.

Záruční a servisní podmínky:

- 5-letá servisní podpora hardware s opravou přímo na místě instalace a garantovanou odezvou následující pracovní den po nahlášení závady.
- 5-letá podpora software zahrnující softwarové aktualizace, opravy chyb a možnost telefonické i e-mailové podpory s diagnostikou přes vzdálený přístup.

Test nabízeného řešení:

- Dodavatel na výzvu zadavatele dodá funkční vzorek v identické konfiguraci s nabízeným systémem, bezplatně a na dobu minimálně 15 pracovních dnů.
- Dodavatel doručí testovací vzorky do 10 pracovních dnů od doručení výzvy na adresu uvedenou zadavatelem.
- Dodavatel zajistí potřebnou součinnost při testování a v případě výzvy se dostaví k testování do 5 pracovních dnů.

- Dodavatel bere na vědomí, že pokud testovaný systém nesplní požadované funkční vlastnosti, bude vyřazen ze zadávacího řízení a smlouva s ním nebude uzavřena.
- Dodavatel převezme testovací vzorky zpět na vlastní náklady po ukončení testování.