

Příloha č. 1 - Specifikace předmětu plnění (Část A)

Generační obměna nástroje pro centralizované zaznamenávání událostí z libovolných zdrojů, s možností analýzy a řešení provozních i bezpečnostních událostí/incidentů ze systémů a aplikací zadavatele.

Předmět zakázky:

Dodat a implementovat generační obměnu stávajícího nástroje Logmanager na zaznamenávání událostí. Tento nástroj aktuálně slouží pro sběr a analýzu logů s možností následné analýzy a řešení bezpečnostních událostí/incidentů ze systémů a aplikací zadavatele určeným hodnocením aktiv a bezpečnostních potřeb organizace. Navržené rozšíření nástroje musí umožnit zapojení do clusteru se stávajícím systémem, synchronizaci jeho konfigurace i dříve pořízených dat v rámci databáze. Od rozšíření nástroje očekáváme naplnění požadavků vyplývajících zejména z připravované vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšší povinnosti (NIS2). Nástroj po rozšíření proto musí být schopen zaznamenat všechny bezpečnostní a relevantní provozní události a tyto uchovat nejméně po dobu 18 měsíců. Nástroj musí být dále schopen zajistit vysokou dostupnost dat, přesné časové razítko ke všem pořízeným událostem a umožnit zachování důvěrnosti a integrity pořízených dat po celou dobu jejich životního cyklu. Pro efektivní využití musí i rozšířený nástroj umět generovat reporty o aktivitách systémů i uživatelů, včetně auditních reportů na vyžádání, nebo se stanovenou periodicitou s definovatelným obsahem.

Cílem je mít jednotné a plně resilientní úložiště logů s pokročilými nástroji analýzy a upozorňování, ke kterému budou mít přístup pouze autorizovaní pracovníci zadavatele. Nezbytnou nutností je vyloučit možnost modifikace logů ze strany administrátorů nebo uživatelů. Nástroj i po rozšíření musí dále umožňovat snadnou klasifikaci dat, tvorbu uživatelsky definovaných parserů, filtrů, upozornění a korelací bez účasti výrobce nebo dodavatele ve snadno pochopitelném grafickém rozhraní bez nutnosti používat znalosti programátora. Dokumentace musí poskytnout jednoznačný návod, jak takovéto činnosti provádět, a to včetně široké škály vzorových příkladů.

Zálohování konfigurace i dat a jejich obnova je nezbytnou nutností, kterou musí dodaný systém podporovat i v rámci clusteru. Dodaný nástroj proto musí podporovat možnost i dalšího horizontálního i vertikálního rozšíření formou clusteru N+1 a zálohování vzniklých dat na externí zálohovací systém. Zálohováním dat na externí systém musí umožnit dosáhnout požadavku na délku uložení logovaných událostí po dobu minimálně 18 měsíců. Platí však, že požadujeme, aby systém umožňoval on-line zobrazit hodnoty nad všemi interně uloženými daty za libovolné časové období bez nutnosti nejprve modifikovat konfiguraci systému nebo parametry uložených dat.

Součástí dodávky musí být úplná a podrobná dokumentace systému v češtině. Proto v rámci odpovědi na výběrové řízení požadujeme předložit kompletní dokumentaci k celému systému a poznámky k vydání (release notes) k systému i všem návazným komponentům. Není přípustné předložit českou dokumentaci, která bude odkazovat do dokumentace, která bude v jiném jazyce, než je čeština. Stávající nástroj provozujeme vlastními lidskými zdroji, proto by nabízený systém měl i nadále umožňovat našim pracovníkům IT provádět základní i středně pokročilé konfigurace bez nutnosti konzultovat dodavatele nebo výrobce. Nabízený nástroj proto musí splňovat existující parametry uživatelské přívětivosti a integrity uživatelského

rozhraní a vyhnout se nutnosti používání skriptů, maker, konfigurací v příkazové řádce nebo terminálu. Dále by dokumentace měla poskytnout jednoznačné návody, jak konfigurovat nejčastější zdrojová zařízení pro spolupráci s nabízeným systémem.

Pokud jsou v nabízeném řešení zahrnuty jakékoliv licence, jejich legální používání nesmí být časově omezeno. Nabízené řešení tedy musí být plně funkční i po uplynutí doby placené podpory.

V případě pochybností o vlastnostech nabízeného nástroje si vyhrazujeme právo vyžádat funkční vzorek nabízeného řešení pro ověření funkčních vlastností a provést ověřovací testy ještě před ukončením výběrového řízení. V tomto případě je dodavatel povinen dodat funkční vzorek s technickými parametry nabízeného řešení do 1 týdne od výzvy zadavatele a poskytnout součinnost s testováním. Dále si vyhrazujeme právo vyžádat si kontakt alespoň na 1 referenčního zákazníka z našeho sektoru pro účely zjištění zkušeností s nabízeným systémem.

Zadavatel v rámci generačního upgrade poptává veškeré instalační práce včetně přenesení všech parserů, alertů, dashboardů do nového systému. Součástí je i přenesení logů ze starého zařízení do nového.