Příloha č. 01A Specifikace předmětu plnění veřejné zakázky

Server pro dlouhodobé uchovávání logů systémů provozovaných na UHK

Zadavatel při stanovení technických podmínek vychází z reálné stávající ekonomické, personální a technologické situace na UHK.

Obecné zadání:

Předmětem dodávky je pořízení fyzického serveru pro centrální sběr, uchovávání a správu logů ze systémů provozovaných na síti UHK s možností následné analýzy při řešení bezpečnostních incidentů/událostí. Řešení musí zachovávat originál logů za účelem bezpečnostního auditu a umožňovat splnění legislativních norem a požadavků, zejména pak doložením souladu nabízeného systému s požadavky ISO/ČSN 27001:2013 pro pořizování auditních záznamů. Systém musí být schopen shromáždit provozní data ze všech důležitých systémů na jednom místě a dlouhodobě je uchovávat. Tímto operátor IT/Bezpečnosti dostane možnost zjistit informace o bezpečnostních incidentech, provozních stavech a případných závadách v IT v reálném čase i v pohledu do minulosti nejméně jeden rok zpětně. Toto úložiště musí být schopné generovat reporty o aktivitách systémů i uživatelů, včetně auditních reportů na vyžádání, nebo se stanovenou periodicitou s definovatelným obsahem, a to bez nutnosti používat SQL syntaxi.

Řešení musí obsahovat možnost procházení těchto logů integrovaným grafickým rozhraním s předdefinovanými pravidly pro rychlé vyhledávání (např. jako jsou změny v systémech provedené administrátory; seznam nově vytvořených účtů v MS AD a Office365 za zvolenou periodu; změny v přístupových právech pro zadaného uživatele nebo k zadané složce; monitoring privilegovaných účtů, sdílených účtů a změn konfigurací; sledování souborových systémů apod.) Dále musí systém umožňovat sledovat chování uživatelů a systémů s možností upozorňování na překročení pravidel, a to na základě limitů nebo korelací událostí stanovených administrátorem systému.

Cílem vytvořit jednotné úložiště logů s pokročilými nástroji analýzy a upozorňování, ke kterému budou mít přístup pouze správci systému. Nezbytnou nutností je vyloučit možnost modifikace logů ze strany administrátorů nebo uživatelů. Systém 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 znalostí programátora. Dokumentace musí poskytnout jednoznačný návod, jak takovéto činnosti provádět, a to včetně široké škály vzorových příkladů.

Protože není předem známo přesné množství logů vznikajících V prostředí UHK, požadujeme, aby dodaný systém byl dostatečně naddimenzován tak, aby umožňoval délku uložení logovaných událostí po dobu minimálně 12 měsíců.

Součástí dodávky musí být úplná a podrobná dokumentace systému v češtině. Ne všichni naši správci a případní budoucí správci systému dokonale ovládají angličtinu, proto požadujeme, aby součástí dodávky byla i dokumentace v českém jazyce, obsahem i kvalitou srovnatelná s aktuální dokumentací

v angličtině. Proto v rámci nabídky 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. Dodaný systém plánujeme provozovat pouze vlastními lidskými zdroji, proto by nabízený systém měl umožňovat pracovníkům OIT provádět základní i středně pokročilé konfigurace bez nutnosti konzultovat dodavatele nebo výrobce. Nabízený systém proto musí splňovat očekávané parametry uživatelské přívětivosti a integrity uživatelského rozhraní a vyhnout se nutnosti používaní 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 nebo záruky.

Veškeré dokumentované funkcionality a minimální technické požadavky popsané v sekci „technická specifikace“ již musí být přítomny v aktuálním release daného systému. Budoucí nebo v budoucnu uvažované vlastnosti nebo funkcionality nelze považovat za vlastnosti či funkcionality nabízeného řešení v době podání nabídek.

Zadavatel si vyhrazuje právo vyžádat funkční vzorek nabízeného řešení pro ověření funkčních vlastností a provést ověřovací testy ještě před podpisem předávacího protokolu či vystavení faktury. V tomto případě je dodavatel povinen dodat funkční vzorek do 5 dnů od výzvy zadavatele. Zadavatel následně ve lhůtě 10dní provede testování dodaného zapůjčeného zařízení, jehož výsledkem bude potvrzení či vyvrácení funkčních definovaných vlastností popsaných v technické specifikaci. Více viz obchodní podmínky.
Zadavatel v rámci testovacího provozu na dodaném testovacím vzorku, vycházeje z dodané dokumentace k nabízenému systému, provede tyto práce a vytvoří záznam o jednotlivých činnostech a jejich výsledcích:

- Základní nastavení systému a jeho konfigurace tak, aby mohl pracovat v prostředí zadavatele, včetně vytvoření uživatelů s rozdílným systémovým i databázovým oprávněním
- Zapojení několika vybraných zdrojových systémů logů a událostí zadavatele a otestování následujících vlastností:
    - nastavení klasifikace zdrojů
    - nastavení značek (tagů)
    - filtrování událostí
    - modifikace parsování existujícího zdroje v grafickém rozhraní nástroje
    - vytvoření reportů a exportu logů a vybraných údajů z logů
- Konfiguraci vybraných systémů Microsoft Windows tak, aby posílaly logy do testovaného systému
- Konfiguraci kolektoru logů z prostředí Microsoft Office365 tak, aby byly logy testovaného systému přijaty a zpracovány na testovacím vzorku, včetně transportních logů SMTP provozu na Office365, případně předvedení daných funkcí již na existujícím systému jiného zákazníka
- Ověření funkčních a výkonových parametrů Windows agenta a jeho centralizované správy v nabízeném systému – viz Technická specifikace, všechny body z odstavce „Sběr událostí z Microsoft prostředí“
- Vytvoření a uložení vlastního dashboardu a reportu, nastavení pravidelného odesílání reportu mailem vybraným pracovníkům zadavatele

- Otestování, jakým způsobem se v jednotném grafickém rozhraní vytvoří klasifikace a filtrování vstupních dat.
- Vytvoření, konfigurace a odladění jednoduchého uživatelsky definovaného parseru – viz Technická specifikace, odstavec „SW parametry“
- Značkování událostí, vytvoření upozornění s limitem nebo korelací dle zadání Zadavatele – viz Technická specifikace, odstavec „SW parametry“ a odstavec „Alerty“ (příklad 1: pošli alert jen v případě, že se událost stala na skupině Windows serverů X-krát během 10 minut. Příklad 2: pošli alert v případě, že uživatel za posledních 15 minut smazal na všech Windows serverech více než 30 souborů, bez započtení smazání dočasných souborů)
- Odeslání události, která vyvolala alert, na externí syslog server přes TCP protokol
- Oprava ze záloh po simulovaném úplném selhání nabízeného systému v následujících krocích:
- Provedení zálohy konfigurace a dat na externí systém
- Nastavení systému do továrního nastavení
- Obnovení konfigurace a všech dat z vytvořených záloh
- Kontrola úplnosti obnovené konfigurace a dat ze záloh.
- Navýšení a ponížení software nabízeného systému v grafickém rozhraní a provedení kontroly, že v případě ponížení nedojde ke ztrátě dříve shromážděných dat. Kontrolu změny funkčních vlastností po navýšení software s ohledem na popis v poznámkách k danému vydání software (release notes k jednotlivým testovaným verzím software)
- Kontrola, jakým způsobem se nastavuje systém ve vysoké dostupnosti (Cluster), včetně kontroly popisu možných variant zotavení po výpadku
- Kontrola kompletnosti dokumentace pro nabízený systém v českém jazyce
- Součástí ověření funkčních vlastností bude ověření požadované funkcionality a parametrů dodaného funkčního vzorku systému dle Technické specifikace tohoto zadání.

Ověření funkčních vlastností nabízeného systému bude provádět zadavatel, vycházeje z dokumentace k nabízenému systému. V případě nejasností zadavatel vyzve k účasti zástupce dodavatele/uchazeče, který mu poskytne potřebnou součinnost, a to maximálně do 3 pracovních dnů po doručení výzvy uchazeči. Testy budou provedeny v prostředí zadavatele. Po ukončení testování budou funkční vzorky uchazeči vráceny (uchazeč si vyzvedne vzorky na vlastní náklady v místě plnění).

Ověřování bude zakončeno vyhotovením zápisu. V případě, že testovaný systém neprojde úspěšným ověřením funkčních vlastností, zadavatel si vyhrazuje právo s takovým uchazečem odstoupit od kupní smlouvy.

Součástí dodání řešení bude jeho odborná fyzická instalace u zadavatele výrobcem certifikovaným technikem, konfigurace serveru i typické klientské části (Windows/linux) a aplikací v rozsahu takovém, jak je popsáno v sekci „testovací provoz zařízení“. Součástí bude také zaškolení obsluhy systému v počtu minimálně 3 osob vybraných zadavatelem.

Technické Specifikace:

- 2x CPU (každý min. 16 jader), podpora HyperThreadingu a turboboost, průměrný výkon minimálně 44000 bodů podle nezávislých testů cpubenchmark.net
- 128 GB RAM, min. DDR4, min. 24 slotů pro RAM
- HW 12Gb SAS RAID řadič s podporou min. RAID 0/1/5/6/10/50/60 s cache 8GB, která je zálohována baterií nebo flash pamětí
- 12 ks stejných RAID edition disků určených pro použití v datacentrech, o rychlosti 7200 otáček, s možností odpojení a vyjmutí současně až 2 disků bez ztráty dat a vlivu na funkčnost
- čistá kapacita úložného prostoru (kapacita výše popsaného „integrovaného diskového pole“) dostupná pro uložená data musí být minimálně 160TB
- minimálně jeden NVMe disk pro akceleraci o celkové kapacitě min. 6TB
- 2x 1Gbit LAN porty, 1x dedikovaný 1Gbit port pro management HW
- 2 napájecí zdroje s redundancí napájení 1+1 s dostatečným výkonem
- Ventilátory vyměnitelné za provozu a redundantní
- systém pro vzdálenou správu včetně „enterprise“ licence, pokud tato funkčnost podléhá licenční potřebě (obdoba HP iLO nebo Dell iDRAC apod)
- virtuální KVM (tj. převzetí textové i grafické konsole zařízení a zajištění přenosu povelů z klávesnice a myši vzdáleného počítače)
- včetně ramena pro kabelový management umožňujícího vysunutí zapnutého systému z racku pro servisní účely
- jedno hardwarové zařízení (tzv. appliance) k umístění do racku o velikosti max. 4U
- HW musí podporovat operační systémy MS windows server 2019 a VMWare ESXi7
- zařízení je z hlediska HW a SW vybavení samostatné a soběstačné (nezávislé), obsahuje veškeré nutné HW komponenty a nevyužívá pro svůj běh žádné prostředky připojené infrastruktury a systémů, které monitoruje (nebo obecně jiné infrastruktury a systémů, např. diskový prostor apod.), tzn. obsahuje pro veškerý běh aplikacích provozovaných pro sběr a vyhodnocování logů své vlastní CPU, RAM a diskový prostor
- všechny části zařízení a jeho systémů je možné nastavit ve webové centrální správcovské konzoli, není nutné editovat žádné konfigurační soubory (to se týká i IP adresace systému)
- jednotná centrální webová konzole slouží také pro přístup k logům, alertům, reportům
- veškerá uživatelská rozhraní jsou v českém jazyce
- možnost definice uživatelských rolí definujících přístupová práva k uloženým událostem a jednotlivým ovládacím komponentám systému
- integrace s Active Directory (Windows server) pro možnost ověřovat uživatele systému na externím LDAP serveru
- aktualizace systému (v rámci maintenance výrobce) jsou distribuovány v jednotném balíku a jejich instalace je prováděna přes centrální správcovskou konzoli nebo jiným způsobem obdobné nebo nižší náročnosti
- průměrný příjem a zpracování min. 10 tisíc událostí za vteřinu
- špičkový příjem až min. 20 tis událostí za vteřinu v případě vyššího počtu událostí je systém uloží do vyrovnávací paměti (bufferu) a zpracuje je později
- podpora zrcadlení a clusteru – při budoucím rozšíření na 2 a více zařízení v režimu active/active
- rozšířený clusterový systém se pak chová jako 1 celek, tzn. má jedno uživatelské rozhraní (centrální konzolu), dále se rozšiřuje kapacita, zrychluje se vyhledávání, a jsou automaticky prohledávána všechna data na všech zařízeních v clusteru, vůči sledovaným zařízením pak cluster vystupuje jako jeden komunikační uzel, přičemž si cluster dále zajišťuje synchronizaci dat mezi jednotlivými zařízeními clusteru
- uživatelská konfigurace vlastních parserů pomocí vizuálního programovacího jazyka v centrální správcovské webové konzoli. Tento vizuální programovací jazyk musí uživateli umožnit psát

vlastní parsery bez nutnosti znalosti programování (např. NodeRED, Microsoft VPL, Blockly apod). Programové elementy jsou uživateli prezentovány graficky formou schémat, které obsahují aplikační logiku

- konfigurace uživatelských parserů musí umožňovat automatické doplňování DNS reverzních záznamů, GeoIP informace a identifikace výrobce zařízení podle MAC adresy
- Možnost on-line ladění uživatelsky definovaných parserů - při jejich vytváření je možné vložit vlastní testovací zprávy, při změně je okamžitě zobrazena výsledná podoba rozparsovaných dat
- Možnost sběru událostí minimálně ve formátech RAW, Syslog, CEF, JSON RFC7159
- Systém zachovává původní informaci ze zdroje logu o časové značce události, ale nedůvěřuje jí a vytváří vlastní důvěryhodné časové razítko ke každému logu, kterým se systém defaultně řídí. Každá událost musí mít navíc unikátní identifikátor, který zůstává jedinečný po celou životnost produktu.
- Všechna pole a položky přijaté systémem jsou automaticky indexovány. Nad všemi položkami je možné ihned provádět vyhledávání bez nutnosti dodatečného ručního indexování administrátorem.
- Systém podporuje nativní získávání logů z Office365. Požadujeme předložit link na dokumentaci popisující nastavení systému v jednotném grafickém rozhraní tak, aby získával logy z Office365.
- Systém nesmí v žádném případě umožnit mazání nebo modifikování již uložených logů v rámci požadované retence. A to ani libovolnou konfigurační změnou - administrátorovi s nejvyššími oprávněními k navrhovanému systému. Každý zpracovaný log musí mít dohledatelný unikátní identifikátor, který umožní jeho jednoznačnou identifikaci.
- Licenčně neomezený počet zařízení pro příjem zasílaných událostí. Licenčně neomezený počet událostí v GB za den nebo licence na minimálně 500GB uložených událostí za den. Integrovaná databáze musí mít čistou velikost nejméně 100 TB a nad to musí podporovat kompresi ukládaných dat.
- Dále je možné tvořit parsery i nad daty v databázích MS SQL Serveru (k nimž musí poptávané zařízení umožňovat přístup), je tedy možné parsovat logy obecně libovolných informačních systémů, které vytvářejí databázové logovací záznamy
- uživatelské rozhraní umožňuje kategorizovat/značkovat jednotlivé zdroje dat (aplikace, zařízení nebo IP subnety) pomocí značek, označujících například umístění zařízení, typ zařízení, kritičnost zařízení apod.
- uživatelské rozhraní umožnuje při definici vlastního parseru možno přidávat kategorizovat/značkovat jednotlivé typy událostí (např. login, logout apod.)
- na základě značek je možné filtrovat data nebo omezovat oprávnění uživatelů systému k jednotlivým událostem
- Systém je schopen na základě zadaných podmínek nad přijatými daty generovat hlášení (alerty)
- Text alertu může být uživatelsky definovaný a může obsahovat proměnné, které jsou v konkrétních případech hlášení nahrazeny informacemi na základě dané zpracovávané události
- Zařízení obsahuje předpřipravené vzory a skupiny vzorů pro základní a obvyklé alerty
- Podobně jako u parserů zařízení umožňuje konfigurace alertů pomocí vizuálního programovacího jazyka, který není prezentován textově, ale graficky formou schémat, která obsahují požadovanou aplikační logiku
- Aletry je možné dále konfigurovat z hlediska priority zpracovávaných dat (resp. důležitosti monitorovaných zdrojů, z jejichž logů byly spouštěcí události alertu vytěženy)
- Grafické znázornění událostí (grafy událostí)
- Grafické znázornění TOP událostí nad všemi daty za určité časové období
- Automatické doplňování GeoIP informací k událostem a jejich grafické znázornění na mapě

- Automatické doplňování reverzních DNS záznamů k IP adresám
- Předpřipravené pohledy na uložená data
- Reportovací nástroj s přednastavenými nejběžnějšími reporty a možností vlastních úprav a vytvoření nových pohledů
- Možnost uložení uživatelem vytvořených pohledů na data (reporty a dashboardy) pro opakované budoucí zpracování
- Monitoring stavu systému - alertování při překročení prahových hodnot nebo chybě systému, přeposlání upozornění pomocí SMTP nebo Syslog
- Možnost dotazování externím monitorovacím systémem pro další zpracování alertů a prahových hodnot (Icinga, Nagios, MRTG a další)
- Snadné a unifikované vyhledávání událostí (ad hoc) bez nutnosti programování napříč všemi typy dat a zařízení
- Podpora pro: antivirové systémy Eset včetně Eset Remote Administrator
- Podpora pro: webové servery Apache (httpd, Tomcat)
- Podpora pro: Switche Cisco IOS, Nexus, WLC, Dell PowerConnect, HPE Procurve, Mikrotik
- Podpora pro: ISC DHCP
- Podpora pro: JSON
- Podpora pro: Linux služby (Bash log, Cron, FreeRadius, IPTables, OpenSSH server)
- Podpora pro: Dell iDRAC/HPE iLo
- Podpora pro: FlowMON
- Podpora pro: Ubuntu UniFI
- Podpora pro: WMvare vcenter i ESX
- Podpora pro: Routery a firewally Fortinet
- Podpora pro: Microsoft SharePoint, Windows log DHCP, DNS, Firewall, IIS (web a ftp server), libovolné logy Event Vieweru a libovolné textové logy v souborovém systému
- Podpora pro: Databáze MS SQL Server, OracleDB, PostgreSQL
- Podpora pro: Nginx
- Podpora pro: Office365
- Podpora pro: Synology NAS DSM
- Události z prostředí Microsoft jsou vyčítány pomocí instalovaných agentů, kteří umožňují zpracování interních logů (např. Event Log) a libovolných textových logů v souborech v rámci souborového systému
- Agent podporuje nastavení filtrace odesílaných událostí pomocí centrální správcovské konzole, omezení zpracovávaných událostí je tak možné nastavovat již na hranici monitorovaného zařízení/systému, čímž lze eliminovat výraznější zatížení společného komunikačního rozhraní
- Výše uvedené filtrování agentem odesílaných událostí se konfiguruje pomocí vizuálního programovacího jazyka z centrální správcovské konzole tento jazyk není prezentován textově, ale pomocí grafických schémat, které obsahují aplikační logiku
- Windows agent musí současně podporovat jak monitoring interních windows logů, tak monitoring textových souborových logů. Agent se nesmí instalovat individuálně, ale prostřednictvím MS AD Group Policy a nesmí vyžadovat žádnou konfiguraci na cílovém systému.
- Počet instalací Windows agenta by neměl být licenčně a časově omezen, pokud je licenčně nebo časově omezen, tak požadujeme dodání licencí na Windows agenty v množství 1000ks. na dobu předpokládané morální životnosti produktu – 10 let
- Agent nevyžaduje administrátorské zásahy na monitorovaném systému – je centrálně spravovaný a automaticky aktualizovaný přímo z centrální konzole systému, správa a aktualizace agenta se neprovádí prostřednictvím Group Policy
- Agent je vybaven bufferem pro případ ztráty spojení s centrálním úložištěm logů
- Komunikace agenta a monitorovacího zařízení je šifrována

- V případě události Event Logu, agent automaticky doplňuje ke všem odesílaným událostem jejich textový popis tak, jak je zobrazen v Event Viewerem na monitorovaném systému
- Systém musí podporovat vygenerování TSR (technického support reportu) pro možnost diagnostiky bez vzdáleného přístupu.
- potvrzení od výrobce, že dodavatel je certifikovaným nebo autorizovaným partnerem pro nabízený systém.
- Systém požadujeme dodat se standardní zárukou a podporou výrobce v režimu NBD minimálně do 31.12.2022, součástí podpory bude pravidelný reporting o incidentech na zařízení, souhrn doporučení na profylaxe, aktualizace firmware s pravidelnou frekvencí