Názov predmetu zákazky:
LOGmanager – dodávka a implementácia

Predmetom verejného obstarávania je dodávka a implementácia systému pre centralizované ukladanie a správu logov s integrovaným systémom analýzy a riešenia bezpečnostných udalostí/incidentov zo systémov a aplikácií obstarávateľa a jeho podriadenej organizácie SMÚ

Všetky technické parametre/funkcionality, resp. vlastnosti požadovaného predmetu zákazky predstavujú minimálne požiadavky, ktoré musia byť splnené v ponuke uchádzača.
V prípade, že by sa záujemca/uchádzač cítil dotknutý vo svojich právach, t.j., že by týmto opisom dochádzalo k znevýhodneniu alebo k vylúčeniu určitých záujemcov/uchádzačov alebo výrobcov, alebo že tento predmet zákazky nie je opísaný dostatočne presne a zrozumiteľne, tak vo svojej ponuke môže uchádzač použiť technické riešenie ekvivalentné, ktoré spĺňa kvalitatívne, technické, funkčné požiadavky na rovnakej a vyššej úrovni, ako je uvedené v tejto časti výzvy, túto skutočnosť však musí preukázať uchádzač vo svojej ponuke.

Zadaniu vyhovuje LOGmanager od českej spoločnosti Sirwisa a. s..

Všeobecné požiadavky na systém:

- Systém pracuje ako fyzická appliance s jedným uceleným webovým rozhraním pre všetky administrátorské i operátorské činnosti. Nevyžaduje inštaláciu ďalších systémov a aplikácií okrem podpory zberu na iných lokalitách (mimo centrálu) a agenta pro zber Windows logov.
- Konfigurácia systému sa musí vykonávať v grafickom rozhraní jednotnej užívateľskej konzoly, Systém musí poskytovať podporu pre vizuálne programovanie pre všetky kroky spracovania strojových dát. Vo webovom rozhraní nesmie byť povinná konfigurácia s využitím skriptov, makier alebo textových konfiguračných polí, do ktorých sa skripty a makrá vkladajú
- Systém umožňuje doplnenie parseru pre zariadenia, aplikácie alebo systémy mimo uvedeného zoznamu užívateľom bez nutnosti spolupráce s výrobcom alebo dodávateľom ponúkaného systému - užívateľsky definované parsery. Dokumentácia systému musí obsahovať prehľadný návod na vytváranie zákazníckych parserov a systém musí obsahovať možnosť testovania a ladenia zákaznickych parserov bez vplyvu na ostatné produkčné funkcie systému. Pre vytváranie nesmie byť použité textové písanie programového kódu, ale tzv. vizuálne programovanie, ktoré automaticky opravuje a upozorňuje na chyby.
- Systém umožňuje v grafickom rozhraní vizuálneho programovacieho jazyka jednoducho vykonávať triedenie a značkovanie vstupných dát pre ich ďalšie spracovanie. Nie je prípustné nastavenie triedenia vstupných dát vo forme skriptu/makra zobrazeného v textovom okne.
- Systém prijíma a spracováva logy, udalosti a ďalšie strojovo generované dáta prostredníctvom minimálne nasledujúcich protokolov: UDP/TCP 514 (SYSLOG), TCP 20514 (RELP, nešifrovane) a TCP 20515 (RELP, šifrovane). Systém musí umožnovať príjem logov i na rozsahu minimálne 50 UDP a TPC portov.
- Prijaté logy systém štandardizuje do jednotného formátu a logy sú rozdeľované príslušných polí podľa ich typu. Systém musí zároveň uchovávať originálne verzie správ.
- Pre hodnoty jednotlivých parsovaných polí je možné v definícii parseru zmeniť typ a štandardizovať minimálne na tieto základné druhy: číslo, IP adresa, MAC adresa, URL. Nad uloženými dátami typu číslo musí byť možné pri vyhľadávaní vykonávať matematické operácie (súčty všetkých hodnôt, priemery, najmenšie/najväčšia hodnota a pod.)
- Systém zachovává pôvodné informácie zo zdroju logu o časovej značke udalosti, ale nedôveruje jej a vytvára vlastné dôveryhodné časové razítko ku každému logu, která vzniká v okamihu prijatia logu systémom a ktorým sa systém riadi.

- Všechny polia a položky prijaté systémom sú automaticky indexované. Nad všetkými položkami je možné ihneď vykonávať vyhľadávanie bez nutnosti dodatočného ručného indexovania administrátorom.
- Možnost zberu udalostí minimálne vo formátoch RAW, Syslog, CEF, LEEF, JSON RFC7159.
- Systém nesmie umožniť mazanie alebo modifikovanie uložených logov ani konfiguračnou zmenou administrátorovi systému s najvyššími oprávneniami. Každý log musí mať unikátny identifikátor, ktorý umožní jeho jednoznačnú identifikáciu.
- Systém musí umožňovať konfiguráciu filtrácie nerelevantných správ
- Systém vykonáva konsolidáciu logov na vlastnom storage priestore.
- Systém umožňuje jednoduché vyhľadávanie udalostí a okamžité vytváranie grafických reportov (ad hoc) bez nutnosti dodatočného programovania alebo aplikovania dopytov v SQL jazyku. Reportovací nástroj musí byť integrálnou súčasťou navrhovaného systému a byť súčasťou jednotného rozhrania
- Systém vykonáva ucelenú vizualizáciu logov, udalostí a strojových dát (grafy udalostí). Vizualizácia musí byť dynamická, t.j. voľbou v jednom grafe sa ostatné príslušné grafy v pohľade na dáta upravia podľa požadovanej voľby automaticky.
- Systém umožňuje jednoducho vytvárať grafické znázornenie udalostí nad všetkými uloženými dátami za ľubovoľné časové obdobie bez nutnosti modifikácie konfigurcie systému alebo parametrov uložených dát.Historické dáta v požadovanej dĺžke retencie uložené v systéme j možné prehľadávať okamžite bez časových strát opätovného importu alebo dekomprimácie starších dát, prehľadávanie nesmie vyžadovať manuálnu konfiguráciu a zásahy používateľa
- Systém vykonáva automatické doplňovanie reverzných DNS záznamov a GeoIP informácií k udalostiam a v prípade GeoIP ich grafické znázornenie na mape bez nutnosti využívať služby tretích strán či externé aplikácie.
- Systém musí podporovať natívne získavaie logov z Office365.
- V prípade krátkodobého preťaženia systému nesmie dôjsť k strate logov. Všetky prijaté nespracované logy/udalosti musia byť ukladané do vyrovnávacej pamäte.
- Systém musí umožňovať unifikované vyhľadávanie naprieč všetkými typmi dát a zariadení podľa normalizovaných polí
- Systém musí spĺňať požadavky normy STN/ISO 27001:2013 pre získavanie auditných záznamov. Toto potvrdenie nie je možné nahradiť certifikátom na spoločnosť dodávateľa (subdodávateľa) alebo výrobcu ponúkaného systému. Nie je ho možné nahradiť ani čestným vyhlásením.
- Systém musí mať možnosť uloženia užívateľom vytvorených pohľadov na dáta (dashboardov) pre budúce spracovanie. Výrobcom dodané typy pohľadov nesmie byť možné nevratne modifikovať
- Systém obsahuje reportovací nástroj s prednastavenými najbežnejšími reportami a možnosťou vlastných úprav a vytváranie nových pohľadov. Pre vytváranie nových pohľadov na dáta nie je prípustné používať povinne SQL jazyk.
- Systém obsahuje predpripravené pohľady na uložené dáta podľa jednotlivých kategórií zdrojových zariadení i podľa logického členenia.
- Na základe pohľadu na uložené dáta je možné vykonať export dát v štruktúrovanom formáte tak, ako sú v pohľade skutočne zobrazené
- Konfiguračné a systémové rozhranie a dokumentácia musia byť identické v anglickom i v slovenskom alebo českom jazyku. Nepripúšťa sa obmedzená dokumentácia v slovenskom alebo českom jazyku.
- Systém musí umožňovať kapacitnú i výkonovú škálovatelnosť.

- Monitoring stavu systému - alertovanie pri prekročení prahových hodnôt alebo chybe systému, preposlanie upozornenia pomocou SMTP nebo Syslog.
- Systém musí obsahovať REST-API pre integráciu s externým monitorovacím systémom (Zabbix, Nagios, PRTG a pod.)
- Jednotná centrálna webová konzola pre prístup k logom, alertom, reportom a pre správu systému. Z tejto konzoly sa vykonáva kompletná konfigurácia, správa a analýza logov. Nie je prípustné, aby dodaný systém mal viacero konzol pre jednotlivé časti systému.
- Systém musí umožňovať jednoduché vytváranie užívateľských rolí definujúcich prístupové práva k uloženým udalostiam a jednotlivým ovládacím komponentom systému.
- Systém musí vykonávať parsovanie a normalizáciu prijatých udalostí bez nutnosti inštalovať externé aplikácie alebo systémy a to priamo vo svojom rozhraní. Jedinou prípustnou výnimkou je monitorovanie systémov Windows, ktoré cez WMI protokol neumožňujú monitorovať textové logy.
- Systém musí podporovať overovanie užívateľa systému na externom LDAP serveri. V prípade výpadku externého LDAP systému musí podporovať overenie z lokálnej databázy. Systém musí automaticky zaznamenávať užívateľské meno ku každej prevedej akcii užívateľom.

Minimálne HW parametre požadovaného systému

- HW appliance v rackovom prevedení s výškou max. 1U, vrátane ramena pre organizáciu zapojených káblov umožňujúceho vysunutie zapnutého systému z racku pre servisné účely.
- HW appliance obsahuje všetky potrebné komponenty (CPU, RAM, diskový priestor) a je nezávislá na ďalších systémoch.
- 1 procesor, min. 12 jader s podporou HyperThreadingu.
- RAM Min. 64GB DDR-4.
- Diskový sybsystém s čistou dostupnou kapacitou minimálne 12TB pre integrovanú databázu; HW akcelerovaný SAS RAID radič s read-write cache min. 8GB. Radič diskového poľa musí obsahovať zálohovaciu batériu alebo byť vybavený flash pamäťou.
- Z výkonnostných dôvodov požadujeme, aby v systéme byli minimálne 4 ks rovnakých RAID edition diskov určených pre použitie v datacentrách, s rýchlosťou minimálne 7200 otáčiek/m.
- Minimálne 4x 1Gbit LAN porty + 1x dedikovaný 1Gbit port pre management HW.
- Redundantné ventilátory, vymeniteľné za chodu.
- Napájacie zdroje s redundanciou 1+1, vymeniteľné za chodu, účinnosť min. 94%
- Virtuálne KVM, tj. prevzatie textovej i grafickej konzoly serveru a prenos povelov z klávesnice a myši vzdialeného počítača.
- Systém pre vzdialenú správu serveru vrátane potrebnej licencie, pokiaľ je potrebná (obdoba HP iLO, Dell iDRAC apod).

Výkonnostné a SW parametre systému

- Systém funguje formou HW appliance (všetkych časti systému je možné nastavit v centrálnej webovej konzole a nie je potrebné upravovať žiadne konfiguráčné súbory, scripty, alebo makra v príkazovom riadku).
- Aktualizácie systému sú distribuované v jednotnom balíku a ich inštalácia je vykonávaná cez centrálnu správcovskú konzolu. Všetky aktualizácie sú vykonávané z webového rozhrania systému bez potreby asistencie výrobcu/dodávateľa.
- Systém musí podporovať downgrade, napríklad pri problémoch s novou verziou systému po upgrade.
- Priemerný trvalý príjem min. 2000 udalostí za sekundu pri priemernej veľkosti jednej udalosti 700Byte. Systém musí preukázateľne kompletne spracovať prijaté udalosti vrátane vytvorenia očakavaných metadát (DNS-PTR, čisla a mená ASN, geolokácie), zaisťovanie

normalizácie, zamedzovania straty prijatých udalostí, alebo posunutiu dôverychodného časového razítka udalosti.

- Špičkový príjem minimálne 4000 udalostí za sekundu po dobu najmenej 10 minút pri priemernej veľkosti jednej udalosti 700Byte. Systém musí pri špičkovom príjme preukázateľne kompletne spracovať prijaté udalosti vrátane vytvorenia očakavaných metadát (DNS-PTR, čisla a mená ASN, geolokácie), zaisťovanie normalizácie, zamedzovania straty prijatých udalostí, alebo posunutiu dôverychodného časového razítka udalosti.
- Licenčne neobmezený počet zariadení pre príjem zasielaných udalostí. Licenčne neobmezený počet udalostí v GB za deň alebo licencia na minimálne 200GB uložených udalostí za deň. Integrovaná databáza musí mať čistú veľkosť najmenej 12 TB a musí podporovať kompresiu ukladaných dát
- Užívateľská konfigurácia vlastných parserov pomocou vizuálneho programovacieho jazyka v centrálnej správcovskej webovej konzole. Vizuálny programovací jazyk musí užívateľovi umožniť písať vlastné parsery bez nutnosti znalosti programovania (napr. Node-RED, Microsoft VPL, Blockly apod). Vizuálny programovací jazyk nie je prezentovaný textovo, ale graficky formou blokov, ktoré obsahujú aplikačnú logiku.
- Konfigurácia užívateľských parserov musí umožňovať automatické doplňovanie DNS reverzných záznamov, GeoIP informácie a identifikáciu výrobcu zariadenia podľa MAC adresy.
- Systém musí podporovať doplňovanie správ o statické informácie z textových tabuliek, napríklad k užívateľskému menu doplniť informáciu o jeho emailovej adrese, členstve v AD skupinách a pod. Pre automatickú aktualizáciu takto uložených doplnkových informácií musí byť možné tieto textové tabuľky doplniť pomocou REST API systému a modifikovateľné cez webové rozhranie systému.
- Možnosť on-line ladenia užívateľsky definovaných parserov - pri ich vytváraní je možné vložiť vlastné testovacie správy, pri zmene je okamžite zobrazená výsledná podoba rozparsovaných dát a prípadné chybové hlásenia.
- V centrálnej správcovskej konzole je možné pridávať k jednotlivým zdrojom dát, aplikáciám, zariadeniam alebo IP subnetom tzv. značky, označujúce napríklad umiestnenie zariadenia, typ zariadenia, kritickosť zariadenia a pod. Systém musí obsahovať preddefinované značky, ktoré automaticky pridáva k prijímaným správam (napríklad konfiguračná zmena, úspešné overenie užívateľa, neúspešné overenie užívateľa, správa z Windows, správa generovaná firewallom a pod.)
- Všetky pridávané značky sú ukladané s každou prijatou udalosťou, na základe značky je možné filtrovať dáta alebo obmedzovať oprávnenia užívateľov systému k jednotlivým udalostiam.
- Systém musí byť predpripravený pre zrkadlenie a clustrové zapojenie – 2 nody.
- V prípade zapojenia ako dvojnodový cluster sa systém správa ako jeden celok.
- V prípade využitia dvoch nodov v clustri sa zrýchľuje vyhľadávanie a sú automaticky prehľadávané všetky dáta na všetkých zariadeniach v clustri.
- V prípade rozšírenia systému na cluster musí navrhovaný systém zaistiť bezvýpadkovosť zberu logov.
- Systém musí umožňovať export dát ve formáte vhodnom pre ďalšie strojové spracovanie bez dodatočných obmedzení na časové obdobie, množstvo, alebo obsah exportovaných dát.
- Podpora zálohovania alebo obnovy konfigurácie v jednom kroku a jednom súbore pre celý systém.
- Podpora zálohovania dát na externý systém, požadované je plánované aj ad-hoc zálohovanie.

Alerty

- Systém je schpný na základe zadaných podmienok splnených v prijatých dátach vygenerovať alert.

- Text emailu vygenerovaného alertom môže byť užívateľsky definovaný s premennými z prijatej rozparsovanej udalosti.
- Systém musí obsahovať výrobcom predpripravené sety/vzory alertov a korelácií
- Užívateľská konfigurácia alertov pomocou vizuálneho programovacieho jazyka v centrálnej správcovskej konzole. Vizuálny programovací jazyk nie je prezentovaný čisto textovo, ale textovo-grafickou formou, ktorá vizualizuje aplikačnú logiku. Konfigurácia alertu alebo korelácie musí umožňovať okamžitú kontrolu
- Ako výstupné pravidlo alertu musí systém vedieť odoslať udalosť, ktorá alert vyvolala na externý systém minimálne prostredníctvom SMTP alebo Syslog cez TCP protokol. Pre Syslog protokol je poadovaná možnosť definície formátu dát pre jednoduchšiu integráciu so systémami tretích strán.
- V alertoch je možné využívať značky (napríklad: pošli alert iba v prípade, že sa udalosť stala na kritickom serveri, který beží v lokalite Bratislava).
- Systém podporuje funkcie SIEM - korelácie udalostí a upozornenia s hraničnými limitmi. Definícia korelačných pravidiel musí mať možnosť vloženia testovacej správy a výsledku testu vykonanej akcie

Zber udalostí v prostredí Microsoft

- Udalosti z Microsoft prostredí sú získavané pomocou agenta inštalovaného priamo na koncovom Windows systéme. Windows agent musí súčasne podporovať ako monitoring interných windows logov, tak i monitoring textových súborových logov.
- Agent zaisťuje zber nemodifikovaných udalostí a detailné spracovánie auditných informácií.
- Agent podporuje nastavenie filtrácie odosielaných udalostí pomocou centrálnej správcovskej konzoly
- Filtrácia odosielaných udalostí agentom sa konfiguruje pomocou vizuálneho programovacieho jazyka v centrálnej správcovskej konzole. Nerelevantné logy sú filtrované na strane windows agenta a nie sú odosielané po sieti. Vizuálny programovací jazyk nie je prezentovaný textovo, ale textovo-grafickou formou, ktorá vizualizuje aplikačnú logiku.
- Windows agent nevyžaduje administrátorské zásahy na koncovom systéme – je centrálne spravovaný a automaticky aktualizovaný priamo z centrálnej správcovskej konzoly systému. Správa a aktualizacia Windows agenta sa nevykonáva z Group Policy.
- Komunikácia Windows agenta a centrálného systému musí být šifrovaná.
- Windows agent musí podporovať zber nielen zo základných systémových logov (Aplikácie, Zabezpečenie, Inštalácie, Systém), ale je možné z centrálnej správcovskej konzoly nastaviť i zber všetkých ostatných logov v zložke Protokoly aplikácií a služieb. Windows agent musí podporovať centralizované nastavenie z administrátorskej konzoly systému pre zber textových logov vrátane možnosti výberu ich formátu.
- Windows agent musí automaticky dopĺňať ku všetkým odosielaným udalostiam ich textový popis tak, ako je zobrazený v Prohliadači udalostí (Event Viewer) na koncovom systéme.
- Počet inštalácií Windows agenta nesmie byť licenčne ani časovo obmedzený.

Podpora pre zber udalostí z pobočiek

- Systém musí obsahovať centrálne spravované riešenie, ktoré zbiera udalosti na pobočkách alebo v záložnom datacentre a umožňuje ich odoslanie po saturovanej linke bez straty dát.
- Systém musí podporovať centralizovanú správu pre zber udalostí z viacerých lokalít priamo z centrálneho úložiska dát vrátane požiadaviek na virtualizáciu a komunikačnú maticu pre šifrovaný prenos dát
- Riešenie pre zber udalostí z iných lokalít musí byť schopné automaticky nadviazať spojenie s centrálnym úložiskom dát a prenášané dáta šifrovať. V prípade výpadku spojenia medzi inou lokalitou a centrálou musí spojenie automaticky obnoviť.

- Riešenie musí komunikovať po definovanom IP protokole, aby mohla byť centrálne nastavená kvalita služby (QoS) pre prenos udalostí.
- Riešenie musí poskytovať kapacitu vyrovnávacej pamäte pre minimálne 100GB udalostí, ktoré na inej lokalite môžu vzniknúť počas výpadku spojenia medzi inou lokalitou a dátovým centrom.
- Riešenie pre zber udalostí z iných lokalít musí mať výkon minimálne 5 tisíc udalostí /s. a to i pri trvalej záťaži.
- Riešenie pre zber udalostí z iných lokalít musí poskytovať podporu na identických UDP i TCP portoch ako hlavný systém a pre aktívny zber z lokálnych Windows agentov.
- Riešenie pre zber udalostí z iných lokalít musí byť poskytované ako fyzický systém aj ako virtuálny systém pre VMware ESXi a Hyper-V. Výber fyzického alebo virtuálneho riešenia je voliteľný na základe možností dostupných na predmetnej vzdialenej lokalite podľa voľby obstarávateľa.
- Riešenie pre zber udalostí z iných lokalít musí byť schopné komunikovať s centrálou i skrze viacnásobný preklad adries (NAT).

SW Podpora a záruka na hardware

- HW - Požadovaná min. 3-ročná servisná podpora na hardware appliance s opravou na mieste inštalácie serveru a s garantovanou odezvou nasledujúci pracovný deň od nahlásenia priípadnej závady.
- Systém musí podporovať vygenerovanie TSR (technického support reportu) pre možnost diagnostiky bez vzdialeného prístupu.
- SW - Predplatné SW modulov systému vrátane aktualizácií systému a parserov na 1 rok je súčasťou dodávky. Podpora musí obsahovať aktualizáciu SW minimálne 3 x ročne, opravy chýb a telefonická a emailová podpora s diagnostikou vzdialeným prístupom.

Služby

- Súčasťou dodávky systému sú jednorazové implementačné služby minimálne v nasledujúcom rozsahu: zber požiadaviek od obstarávateľa, nastavenie a konfigurácia systému v IT prostredí obstarávateľa; konfigurácia Windows systémov pre zasielanie logov do systému; overenie funkčných a výkonových parametrov Windows agentov; predvedenie vytvorenia a uloženia vlastného dashboardu a reportu; predvedenie vytvorenia a uloženia užívateľsky definovaného parseru; predvedenie nastavenia značkovania udalostí a vytvárania upozornení s limitom alebo koreláciou; nastavenie pravidelného zasielania definovaných reportov vybraným zamestnancom obstarávateľa; zaškolenie obsluhy a správy systému pre roly administrátor, supervízor, operátor

Osobitné požiadavky na plnenie

- vrátane dodania na miesto plnenia v lehote do 31.12.2021
- Dodávateľ sa zaväzuje preukázať objednávateľovi doklad, že je autorizovaným obchodným partnerom spoločnosti oprávneným predávať produkt
- Dodávateľ sa zaväzuje preukázať objednávateľovi odbornú spôsobilosť osôb vykonávajúcich implementáciu predmetu zákazky doložením relevantných technických certifikátov vydaných výrobcom technológie
- Dodávateľ sa zaväzuje preukázať objednávateľovi odbornú spôsobilosť doložením overiteľných min. 3 referencii za posledné 3 roky rovnakého, alebo obdobného charakteru
- Predmet dodania musí byť nový, doposiaľ nepoužitý, zabalený v originálnom balení bez známok poškodenia tovaru aj obalu

- Dodávateľ sa zaväzuje preukázať objednávateľovi platné certifikáty systému riadenia kvality podľa ISO 9001, systému manažérstva služieb IT podľa ISO 20000-1 a systému manažérstva bezpečnosti informácií podľa ISO 27001
- Súčasťou cenovej ponuky musí byť školenie 1 MD na zaškolenie pracovníkov obstarávateľa

Súčasťou zmluvy bude post implementačná podpora na 3 roky v predpokladanom rozsahu 20 človekodní

Služby na vyžiadanie, konzultácie a Pravidelné práce údržby v rozsahu 20 človekodní v priebehu 3 rokov predpokladajú vykonávanie nasledovných činností:

- Profylaxia zariadení, kontrola logov, úprava konfigurácii, návrh riešenia zistených stavov
- Správa, zabezpečenie prevádzky zariadenia, čím sa rozumie zabezpečenie administrácie systému vedúcej k zabezpečeniu funkčnosti Systému, jeho každodennej prevádzky a údržby podľa požiadaviek Objednávateľa.
- Inštalácia Software, updates a upgrades
- Vzdialená diagnostika
- Opatrenia na nápravu chyby v SW alebo HW a výkon obmedzujúce faktory
- Vzdialená podpora a údržba systému
- Reakcia na email-ové a telefonické požiadavky
- Kontrola pravidiel

Post implementačná podpora bude výhradne na základe objednávok objednávateľa. Platnosť zmluvy bude 36 mesiacov od nadobudnutia účinnosti zmluvy alebo do vyčerpania finančných prostriedkov uvedených v zmluve podľa toho, ktorá skutočnosť nastane skôr.