Příloha č. 1 – Specifikace

Obecné požadavky na Systém:

- Systém pracuje jako hardwarová appliance s jedním uceleným webovým rozhraním pro všechny administrátorské i operátorské činnosti v grafickém rozhraní. Nevyžaduje instalaci dalších systémů a aplikací, vyjma podpory sběru na pobočkách a agenta pro sběr Windows logů.
- Systém provádí zpracování síťovým provozem doručených dat událostí z předdefinovaných zdrojů logů.
- Systém musí mít možnost uložení uživatelem vytvořených pohledů na data pro budoucí zpracování.
- Konfigurační a Systémové rozhraní a dokumentace k těmto rozhraním musí být identické v anglickém i v českém jazyce. Nepřipouští se omezená dokumentace v českém jazyce nebo zjednodušená dokumentace odkazující na další dokumentaci v anglickém jazyce, případně na dokumentaci třetích stran.
- V případě krátkodobého (do 10 minut) až dvounásobného přetížení Systému proti jeho tabulkovým hodnotám nesmí dojít ke ztrátě logů nebo nesprávnému stanovení časového razítka. Všechny přijaté nezpracované logy/události musí být ukládány do vyrovnávací paměti.
- Dodaný Systém musí obsahovat ucelené all-in-one řešení pro parsování a normalizaci přijatých událostí bez nutnosti dodatečné instalace externích aplikací nebo systémů.
- Jednotná centrální webová konzole s jednotným grafickým rozhraním pro přístup k logům, alertům, reportům a pro správu Systému. Z této konzole se provádí veškerá konfigurace, správa i analýza logů. Není přípustné, aby navrhovaný Systém měl více rozdílných konzolí od různých výrobců s rozdílným ovládáním nebo aby se konfigurace musela provádět mimo jednotné webové rozhraní.
- Možnost sběru událostí minimálně ve formátech RAW, Syslog RFC5424, CEF, LEEF, JSON RFC8259
- Systém zachovává původní informaci ze zdroje logu o časové značce události, ale nedůvěřuje jí a vytváří vlastní důvěryhodné časové razítko ke každému logu, které vzniká v okamžiku přijetí logu Systémem a kterým se Systém defaultně řídí.
- Všechna pole a položky přijaté Systémem jsou automaticky indexovány. Nad všemi položkami je možné ihned provádět vyhledávání bez nutnosti dodatečného ručního indexování administrátorem.
- 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.
- Systém musí umožňovat konfiguraci filtrace nerelevantních událostí v grafickém rozhraní vizuálního programovacího jazyka. Pro psaní filtrace nesmí být použito textové psaní programového kódu ale tzv. vizuální programování, které automaticky opravuje uživatele a upozorňuje ho na chyby.
- Systém musí umožňovat unifikované vyhledávání napříč všemi typy dat a zařízeními dle normalizovaných polí (uživatelské jméno, zdrojová IP, značka/tag apod.).
- Systém provádí ucelenou vizualizaci logů, událostí a strojových dat (grafy událostí). Vizualizace musí být dynamická, tj. volbou v jednom grafu se ostatní příslušné grafy v pohledu na data upraví dle požadované volby automaticky.
- Systém provádí konsolidaci logů na interním storage logovacího Systému.
- Systém provádí automatické doplňování reverzních DNS záznamů a GeoIP informací k událostem a u GeoIP jejich grafické znázornění na mapě bez nutnosti využívat služeb třetích stran či externí aplikace.

- Monitoring stavu Systému – alertování při překročení prahových hodnot nebo chybě Systému, přeposlání upozornění pomocí SMTP nebo Syslog.
- Požadujeme, aby Systém obsahoval REST-API pro integraci s externím monitorovacím systémem (Zabbix, Nagios, MRTG, WhatsUp a další) a umožňoval autorizovaný přístup ke strukturované databázi logů.
- Požadujeme, aby Systém umožňoval jednotné vytváření uživatelských rolí definujících přístupová práva k uloženým událostem a jednotlivým ovládacím komponentům Systému.
- Systém musí podporovat ověřování uživatele Systému na externím LDAP serveru. V případě výpadku externího LDAP systému musí podporovat ověření lokálního účtu. Systém automaticky zaznamenává uživatelská jména u akcí provedených konkrétním uživatelem.
- Systém obsahuje reportovací nástroj s přednastavenými nejběžnějšími reporty a možností vlastních úprav a vytvoření nových pohledů. Pro vytváření nových pohledů na data není přípustné používat povinně SQL jazyk.
- Systém umožňuje snadné vyhledávání událostí a okamžité vytváření grafických reportů (ad hoc) bez nutnosti dodatečného programování nebo aplikování dotazů v SQL jazyce. Reportovací nástroj musí být integrální součástí navrhovaného Systému a musí se obsluhovat v jednotném rozhraní nabízeného produktu.
- Systém umožňuje v grafickém rozhraní vizuálního programovacího jazyka snadno provádět třídění a značkování vstupních dat pro jejich další zpracování. Nepřipouští se nastavování třídění vstupních dat ve formě skriptu/makra zobrazeného v textovém okně.
- Systém umožňuje snadno vytvářet grafické znázornění událostí v dashboardech nad všemi uloženými daty za libovolné časové období bez nutnosti nejprve modifikovat konfiguraci Systému nebo parametrů uložených dat. Historická data v požadované délce retence uložená v Systému je možné prohledávat okamžitě bez časových prodlev opětovného importu nebo dekomprimace starších dat, prohledávání dat nesmí vyžadovat manuální konfiguraci a zásahy uživatele.
- Systém musí mít možnost uložení uživatelem vytvořených pohledů na data (dashboardů) pro budoucí zpracování. Továrně dodané pohledy na data nesmí jít administrátorem ani uživatelem Systému nevratně modifikovat nebo smazat.
- Systém obsahuje předpřipravené pohledy na uložená data dle jednotlivých kategorií zdrojových zařízení i dle logického členění.
- Na základě pohledu na uložená data lze provést export dat ve strukturovaném formátu tak, jak jsou v továrně nastaveném nebo uživatelsky nastaveném pohledu data skutečně zobrazena.
- Systém provádí zpracování událostí z předdefinovaných zdrojů logů napříč výrobci aplikací, operačních systémů a síťového hardware. Minimální podporavaný hardware: aktivní síťové prvky Cisco (switche, routery), Fortinet, Zyxel, servery DELL, HP úložiště DELL, Qnap a další) a minimální podporovaný software (Microsoft AD 2012/2019, VMWARE5/6/7, Fortimail, Kerio Connect, Cisco CUCM, ISE, Oracle DB, MS SQL), viz seznam podporovaných zařízení v příloze č. 2 – Seznam podporovaných systémů).
- Systém umožňuje dopsání parserů pro výše neuvedená zařízení uživatelem bez nutnosti spolupráce s výrobcem nebo dodavatelem (vč. subdodavatelů) nabízeného Systému – Uživatelsky definované parsery. Dokumentace musí obsahovat přehledný návod na vytváření zákaznických parserů a Systém musí obsahovat možnost testování a ladění zákaznických parserů v jednotném ovládacím grafickém webovém rozhraní viz bod č. 1. Vytváření a testování parserů nesmí mít vliv na provoz Systému. Pro psaní parserů nesmí být použito textové psaní programového kódu ale tzv. vizuální programování, které automaticky opravuje uživatele a upozorňuje ho na chyby.
- Systém poskytuje podporu pro vizuální programování pro všechny kroky zpracování strojových dat. Ve webové konzoli se nepřipouští konfigurace za využití skriptů, maker nebo textových konfiguračních polí, do kterých se složité textové skripty/makra vkládají.

- Systém přijímá a zpracovává logy, události a další strojově generovaná data prostřednictvím minimálně následujících protokolů: SYSLOG (dle RFC3164, RFC5424, RFC5425) a RELP. Systém musí umožňovat příjem logů i na rozsahu alespoň 50 UDP a TCP portů pro zjednodušené třídění vstupních zpráv. Dále požadujeme podporu sběru strojových dat z databází s nastavením v grafickém menu Systému minimálně pro databáze MSSQL, MySQL, Oracle a PostgreSQL a to bez nutnosti instalovat na databázový server doplňkový software nebo agenta.
- Přijaté logy Systém standardizuje do jednotného formátu a logy jsou normalizovány (rozdělovány) do příslušných polí dle jejich typu. Zároveň Systém uchovává i originální verzi zpráv. Integrované parsery Systému automaticky přidávají ke zprávám, kterých se to týká, meta informace, o jaký druh zprávy se jedná a její časové razítko, minimálně požadujeme rozlišení těchto druhů zpráv: úspěšné přihlášení, neúspěšné přihlášení, odhlášení, konfigurační změna, značka/tag. Tyto meta informace musí být možné přidávat i v uživatelsky definovaných parserech.
- Hodnoty jednotlivých parsovaných polí je možné v definici parseru přetypovat a standardizovat alespoň na tyto základní druhy: číslo, IP adresa, MAC adresa, URL. Nad uloženými čísly je pak možné při prohledávání dat provádět matematické operace (součty všech hodnot, průměry, nejmenší/největší hodnota apod.).

Výkonnostní a Softwarové parametry Systému:

- Systém funguje formou hardwarové appliance (všechny části Systémů je možné nastavit v centrální webové konzoli a není nutné editovat žádné konfigurační soubory, scripty nebo makra v příkazové řádce).
- Aktualizace Systému jsou distribuovány v jednotném balíku a jejich instalace je prováděna uživatelsky přes centrální webovou správcovskou konzoli. Všechny aktualizace musí být prováděny z webového prostředí bez potřeby asistence dodavatele/výrobce dodávaného Systému.
- Systém musí podporovat downgrade v jednom kroku, pro případ problémů s novou verzí systému po upgrade. Není přípustný downgrade pouze za součinnosti výrobce.
- Průměrný trvalý příjem min. 5000 událostí/s. Výkon musí být dosažen na požadované množství událostí s průměrnou délkou zpráv minimálně 700Byte trvale. Systém musí prokazatelně kompletně zpracovat přijaté události včetně vytváření očekávaných metadat (DNS-PTR, čísla a jména ASN, geolokace), zajišťovat normalizaci, zamezovat ztrátě přijatých událostí nebo posunutí důvěryhodného časového razítka oproti času skutečného příjmu každé události.
- Špičkový příjem minimálně 10000 událostí/s po dobu nejméně 10 minut a průměrnou délkou minimálně 700byte. Systém musí prokazatelně kompletně zpracovat přijaté události, zamezovat ztrátě ukládaných dat nebo posunutí důvěryhodného časového razítka oproti času skutečného příjmu zpráv. Při zpracování dat během špičkového příjmu akceptujeme zpoždění zobrazení zpracovávaných dat. Systém ani ve špičkovém výkonu nesmí dovolit ztrátu dat, skluz důvěryhodného časového razítka nebo jiné prokazatelné vady na zpracovávaných datech oproti zpracování při průměrném trvalému příjmu událostí.
- Licenčně neomezený počet zařízení pro příjem zasílaných událostí. Licenčně neomezený počet událostí v GB za den nebo licence na minimálně 300 GB uložených událostí za den. Integrovaná databáze musí mít čistou velikost nejméně 40 TB a nad to musí podporovat kompresi ukládaných dat.
- Uživatelská konfigurace klasifikace dat, parserů, filtrů a alertů se provádí pomocí vizuálního programovacího jazyka v centrální správcovské webové konzoli. Vizuální programovací jazyk musí uživateli umožnit psát konfigurace bez nutnosti znalosti programování (např. Node-RED, Microsoft VPL, Blockly apod). Vizuální programovací jazyk není prezentován textově, ale graficky formou schémat-symbolů, které reprezentují aplikační logiku a kontrolují syntaxi.

- Konfigurace uživatelských parserů musí umožňovat automatické doplňování DNS reverzních záznamů, GeoIP informace a identifikace výrobce zařízení podle MAC adresy.
- Systém musí podporovat doplňování zpráv o informace z textových prohledávacích tabulek. (Například k uživatelskému jménu doplnit z textové prohledávací tabulky informaci o jeho emailu, členství v AD skupinách a podobně). Pro automatickou aktualizaci takto uložených doplňujících informací musejí být tyto textové prohledávací tabulky naplnitelné pomocí REST API nabízeného Systému a modifikovatelné přes jednotné webové rozhraní.
- Možnost on-line ladění uživatelsky definovaných parserů – při jejich vytváření je možné vložit skupinu testovacích zpráv, při změně je okamžitě zobrazena výsledná podoba rozparsovaných dat a případná chybová hlášení s upozorněním na chybná místa vytvářeného parseru. Pro snadnější vytváření parserů požadujeme mít možnost vložení minimálně 20 testovacích zpráv současně.
- V centrální správcovské konzoli je možné přidávat k jednotlivým zdrojům dat, aplikacím, zařízením nebo IP subnetům tzv. značky, označující například umístění zařízení, typ zařízení, kritičnost zařízení apod. Systém obsahuje předdefinované značky, které automaticky přidává k přijímaným zprávám. Příklady značek: konfigurační změna, úspešné ověření uživatele, neúspěšné ověření uživatele, zpráva přišla z windows, zpráva byla vygenerována firewallem atd...
- Všechny přidávané značky jsou ukládány s každou přijatou událostí, na základě značky je možné filtrovat data nebo omezovat oprávnění uživatelů Systému k jednotlivým událostem.
- Pro budoucí nasazení ve vysoké dostupnosti je vyžadována podpora sestavení v clusteru – požadujeme podporu minimálně 2 nodů. Nastavení clusteru se musí kompletně realizovat v grafickém rozhraní správcovské konzole v jednom kroku, není přípustné konfigurovat sestavení scripty, makry nebo úpravou textové konfigurace Systému a pomocí ručních restartů služeb. Systém ve vysoké dostupnosti musí přehledně informovat o stavu clusteru a procesu synchronizace databází. Dokumentace k realizaci vysoké dostupnosti musí být kompletní a popisovat všechny kroky sestavování a obnovení v případě výpadku komponenty clusteru.
- V případě využití více nodů v clusteru se automaticky zrychluje zpracování vstupních dat a vyhledávání v již uložených datech.
- V případě rozšíření Systému na cluster musí navrhovaný Systém zajistit bezvýpadkovost sběru logů.
- Řešení musí umožňovat rozšíření mezipaměti diskového subsystému o SSD nebo NVRAM typu o kapacitě minimálně 3TB.
- Systém musí umožňovat export dat ve formátu vhodném pro další strojové zpracování bez dodatečných omezení na časové období, množství nebo obsah exportovaných dat. Během exportu je možné označit pouze vybraná pole, která mají být do exportu zahrnuta.
- Podpora zálohování nebo obnovení konfigurace v jednom kroku a jednom souboru pro celý Systém.
- Podpora důvěryhodného zálohování dat na externí systém. Požadováno plánované i ad-hoc zálohování. Zálohy dat musejí být vhodně kompresovány.
- Zálohováním dat na externí systém musí umožnit dosáhnout požadavku na délku uložení logovaných událostí po dobu minimálně 18 měsíců. Požadujeme, aby Systém umožňoval on-line zobrazit hodnoty nad všemi interně uloženými daty za libovolné časové období bez nutnosti nejprve modifikovat konfiguraci Systému nebo dle parametrů uložených dat. A z těchto dat pak umožní veškeré funkce analýzy a vyhledávání.
- Garantovaná podpora výrobce na aktualizaci Systému a parserů na minimálně 5 let s roční platbou. Podpora musí obsahovat aktualizaci software minimálně 4x ročně, opravy chyb a telefonickou a emailovou podporu s diagnostikou vzdáleným přístupem.

Cena za softwarovou podporu na první rok bude součástí základní ceny a za další roky bude placena ročně.

Minimální Hardware parametry požadovaného Systému:

- Systém nabízí kapacitní i výkonovou škálovatelnost.
- Čistá kapacita úložného prostoru (kapacita diskového pole) dostupná pro uložená data nabízeného Systému musí být minimálně 40 TB dat pro integrovanou databázi podporovanou hardwarově akcelerovaným SAS RAID řadičem s read-write cache min. 8 GB. Řadič diskového pole musí obsahovat zálohovací baterii nebo být vybaven flash pamětí.
- Požadujeme, aby ze Systému bylo možné za běhu vytáhnout libovolné dva disky, bez ztráty dat a vlivu na funkčnost řešení. Redundance disků nesmí ovlivňovat požadovanou kapacitu úložiště.
- Z výkonových důvodů požadujeme, aby v Systému bylo minimálně 12 ks stejných RAID edition disků určených pro použití v datacentrech, o rychlosti minimálně 7200 otáček/m.
- Jedna hardwarová appliance o velikosti max. 2U, včetně ramena pro kabelový management umožňujícího vysunutí zapnutého Systému z racku pro servisní účely. Rack s hloubkou 1 m.
- Hardwarová appliance obsahuje veškeré potřebné komponenty (CPU, RAM, diskový prostor) pro svoji činnost a je nezávislá na dalších systémech.
- 2 procesory, min. 12 jader každý, s podporou HyperThreadingu.
- Min. 128 GB DDR-4 a možnost rozšíření o NVMe paměťové pole pro zpracování dat v čase blízkém reálnému (Near Real-Time).
- Minimálně 4x 1Gbit LAN porty + 1x dedikovaný 1Gbit port pro management HW. Konfigurace všech parametrů síťového rozhraní včetně link agregace dle LACP (802.3ad), VLAN a IP adresace v jednotném webovém rozhraní Systému.
- Větráky v Systému musí být vyměnitelné za provozu a redundantní.
- 2x napájecí zdroje s redundancí napájení 1+1.
- Systém pro vzdálenou správu serveru včetně potřebné licence v nejvyšší verzi, pokud je třeba (obdoba HP iLO, Dell iDRAC apod).
- Virtuální KVM (tj. převzetí textové i grafické konzole serveru a zajištění přenosu povelů z klávesnice a myši vzdáleného počítače.
- Požadovaná min. 5letá servisní podpora na hardware appliance s opravou v místě instalace serveru a s garantovanou odezvou následující pracovní den od nahlášení případné závady. Servisní podpora na HW je v ceně zařízení.

Alerty

- Systém je schopen na základě uživatelsky zadaných podmínek splněných v přijatých datech vygenerovat alert.
- Při výraznějším plnění vyrovnávací paměti musí být administrátor Systému automaticky informován.
- Text emailu vygenerovaného alertem musí být uživatelsky definovatelný s proměnnými, které jsou vyplněny z přijaté rozparsované události.
- Systém musí obsahovat výrobcem předpřipravené sety/vzory alertů a korelací.
- Systém musí provádět konfigurace alertů a korelací pomocí vizuálního programovacího jazyka. Vizuální programovací jazyk není prezentován čistě textově, ale textově-grafickou formou, která vizualizuje aplikační logiku vytvářeného alertu. Konfigurace alertů musí umožňovat okamžitou kontrolu funkčnosti výstupu alertu nebo korelace vložením příslušné testovací zprávy, včetně zobrazení upozornění na případné uživatelské chyby.
- Jako výstupní pravidlo Alertu musí Systém umět odeslat událost, která alert vyvolala, na externí systém minimálně prostřednictvím SMTP nebo Syslogu přes TCP protokol.

U Syslog protokolu požadujeme možnost definice formátu odesílaných dat pro snazší integraci se systémy třetích stran.

- V alertech je možné nejen využívat, ale i přiřazovat značky (příklad: pošli alert jen v případě, že se událost stala na kritickém serveru a je označen názvem lokality, nebo pokud událost obsahuje podmínku, přiřaď novou značku).
- Systém podporuje základní funkce SIEM – funkce pro korelace událostí a upozornění s hraničními limity. Definice korelačních pravidel je prováděna pomocí vizuálního programovacího jazyka a musí obsahovat možnost vložení testovací zprávy a výsledku testu o provedené akci.

Sběr událostí z Microsoft prostředí:

- Systém podporuje nativní získávání logů z Office365 prostředí s licencí E3 bez nutnosti instalovat dodatečné externí komponenty. Požadujeme předložit link na dokumentaci popisující nastavení Systému v jednotném grafickém rozhraní tak, aby získával logy z Office365.
- Události z Microsoft prostředí jsou vyčítány pomocí agenta instalovaného přímo v koncových systémech. Windows agent musí současně podporovat jak monitoring interních windows logů, tak monitoring souborových logů. Agent se nesmí instalovat individuálně, ale prostřednictvím MS AD Group Policy a nesmí vyžadovat žádnou konfiguraci na cílovém systému.
- Agent zajišťuje sběr nemodifikovaných událostí a detailní zpracování auditních informací.
- Agent podporuje nastavení filtrace odesílaných událostí pomocí centrální správcovské konzole.
- Filtrace odesílaných událostí agentem se konfiguruje pomocí vizuálního programovacího jazyka z centrální správcovské konzole Systému. Logy nastavené k filtraci jsou filtrovány na straně windows agenta a nejsou nijak odesílány po síti. Vizuální programovací jazyk není prezentován textově, ale textově-grafickou formou, která vizualizuje aplikační logiku vytvářeného alertu. Filtry musejí umožňovat okamžitě testovat jejich účinnost a zobrazit kolik z uložených dat zvolený filtr zasáhne a kolik logů by případně filtroval minimálně za posledních 24 hodin.
- Windows agent nevyžaduje administrátorské zásahy na koncovém systému – je centrálně spravovaný a jeho konfigurace musí být kompletně realizována v grafickém rozhraní Systému bez využití skriptů nebo maker. Konfigurace musí být automaticky distribuována přímo z centrální konzole Systému. Správa a aktualizace Windows agenta se neprovádí z Group Policy.
- Windows agent podporuje sběr nejen ze základních systémových logů (Aplikace, Zabezpečení, Instalace, Systém), ale je možné z centrální konzole v grafickém rozhraní nastavit i sběr všech ostatních logů ve složce Protokoly aplikací a služeb. Dále musí Windows agent podporovat centralizované nastavení z administrátorské konzole Systému pro sběr textových logů včetně možnosti výběru jejich formátu.
- Windows agent má buffer pro případ ztráty spojení mezi koncovým systémem a centrálním úložištěm logů.
- Komunikace Windows agenta a centrálního Systému musí být šifrovaná.
- Windows agent automaticky doplňuje ke všem odesílaným událostem jejich textový popis tak, jak je zobrazen v Prohlížeči událostí (Event Viewer) na koncovém 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 1 200 na dobu předpokládané morální životnosti produktu – 7 let.

Podpora pro sběr událostí z poboček:

- Systém musí obsahovat řešení, které sbírá události na pobočkách a umožní jejich odeslání po saturované lince bez ztráty dat.

- Systém musí podporovat centralizovanou správu pro sběr událostí přímo z centrálního úložiště dat včetně dokumentace požadavků na virtualizaci a komunikační matici pro šifrovaný přenos dat.
- Řešení musí být schopno automaticky navázat spojení s centrálním úložištěm dat a přenášená data šifrovat. V případě výpadku spojení mezi pobočkou a centrálou musí spojení automaticky obnovit.
- Řešení musí komunikovat po definovaném IP protokolu, aby mohla být centrálně nastavena kvalita služby (QoS) pro přenos událostí.
- Řešení musí poskytovat kapacitu vyrovnávací paměti pro minimálně 100GB událostí, které na pobočce mohou vzniknout během výpadku spojení mezi pobočkou a datovým centrem.
- Řešení pro sběr dat z poboček musí mít výkon minimálně 5 tisíc událostí /s, a to i v trvalé zátěži.
- Řešení musí poskytnout podporu pro UDP i TCP zdroje a pro aktivní sběr z Windows agentů.
- Řešení musí být k dispozici jako fyzický systém nebo jako virtuální systém pro VMware ESXi a Hyper-V.
- Řešení musí být schopno komunikovat z pobočky na centrálu i přes vícenásobný překlad adres (NAT).

Testovací provoz po instalaci zařízení:

- 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 předvedení, jakým způsobem se nastavují značky (tagy), filtrování událostí a modifikuje v grafickém rozhraní způsob parsování existujícího zdroje.
- Konfiguraci vybraných systémů Microsoft Windows zadavatele tak, aby posílaly logy do testovaného Systému.
- Ověření funkčních a výkonových parametrů Windows agenta a jeho centralizované správy v nabízeném Systému – viz výše, všechny body z odstavce „Sběr událostí z Microsoft prostředí".
- Vytvoření a uložení vlastního dashboardu a reportu, nastavení pravidelného odesílání reportu mailem vybraným pracovníkům zadavatele.
- Předvedení, jakým způsobem se v jednotném grafickém rozhraní vytvoří klasifikace a filtrování vstupních dat.
- Vytvoření, konfigurace a odladění uživatelsky definovaného parseru – viz výše.
- Značkování událostí, vytvoření upozornění s limitem nebo korelací dle zadání Zadavatele – viz výše" (příklad: pošli alert jen v případě, že se událost stala na skupině Windows serverů X-krát během 10 minut).
- Odeslání události, která vyvolala alert, na externí syslog server přes TCP protokol.
- Provedení zálohy konfigurace a dat na externí systém, nastavení Systému do továrního nastavení a obnovení konfigurace a dat alespoň jednoho pracovního dne ze zálohy.
- Předvedení navýšení a ponížení software nabízeného Systému v grafickém rozhraní a předvedení, že v případě ponížení nedojde ke ztrátě dříve shromážděných dat.
- Předvedení diagnostiky nabízeného Systému a demonstraci, jakým způsobem se nastavuje Systém včetně popisu možných variant zobrazení po výpadku.
- Představení plnohodnotné dokumentace pro nabízený Systém v českém jazyce.
- Nastavení zálohování dat na externí systém pro zajištění délky uložení logovaných událostí na 18 měsíců a předvedení, jak z těchto dat provádět veškeré analýzy a vyhledávání.

Testování bude provádět dodavatel za účasti zástupců zadavatele, který mu poskytne potřebnou součinnost. Testy budou provedeny v prostředí zadavatele. Testovací provoz bude zakončen akceptací. V případě, že testovaný Systém neprojde úspěšným otestováním, bude plnění smlouvy považováno za nesplněné. Lhůta dodání Systému se tímto neprodlužuje.

Implementace

Implementace Systému zahrnuje:

- Instalaci a konfiguraci zařízení dle požadavků zadavatele v místě dodání.
- Nastavení Systému za přítomnosti obsluhy.

Závěrečná akceptace:

Ověření všech požadovaných funkčních vlastností minimálně v rozsahu specifikovaném v odstavci „Testovací provoz po instalaci zařízení".

Provedení následujících výkonnostních testů:

- Prohledání 4 000 000 (čtyřimilióny) záznamů, zobrazení histogramu a TOP hodnot z osmi rozparsovaných polí nejdéle za 10 sekund.
- Průměrný příjem minimálně 5 000 událostí/sekundu. Ověření v 10minutovém intervalu pomocí generátoru událostí. (Dle požadovaného výkonu).
- Špičkový příjem minimálně 10 000 událostí/sekundu, v případě vyššího počtu událostí je Systém uloží do vyrovnávací paměti a zpracuje je později. Ověření v 10minutovém intervalu pomocí generátoru událostí.

Součástí akceptačních testů bude ověření požadované funkcionality a parametrů dodaného Systému dle Technické specifikace zadání.

Uznání úplnosti dokumentace v českém jazyce ke všem komponentům dodaného Systému.