Príloha č. 1: Technická špecifikácia

Porovnávacia tabuľka- vlastný návrh
„Prevádzkový Log manažment“

Parameter	**Vlastný návrh na plnenie *** **Značka:** Logmanager **Typ:** XL s VF **Výrobca:** Logmanager a.s. **Parametre:** viď nižšie	**Požadované technické parametre a špecifikáciu predložením vlastného návrhu** **splnil/nesplnil** (posúdi verejný obstarávateľ)
Centrálny logovací systém by mal pracovať 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 pre zber Windows logov.	Centrálny logovací 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 pre zber Windows logov.	
Konfigurácia systému sa musí vykonávať v grafickom rozhraní jednotnej užívateľskej konzoly, Systém poskytuje podporu pre vizuálne programovanie pre všetky kroky spracovania strojových dát. Systém má umožňovať doplnenie parseru pre zariadenia, aplikácie alebo systémy mimo uvedeného zoznamu užívateľov 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 parserov bez vplyvu na ostatné produkčné funkcie systému.	Konfigurácia systému sa vykonáva v grafickom rozhraní jednotnej užívateľskej konzoly, Systém poskytuje podporu pre vizuálne programovanie pre všetky kroky spracovania strojových dát. Systém umožňuje doplnenie parseru pre zariadenia, aplikácie alebo systémy mimo uvedeného zoznamu užívateľov bez nutnosti spolupráce s výrobcom alebo dodávateľom ponúkaného systému. Dokumentácia systému obsahuje prehľadný návod na vytváranie zákazníckych parserov a systém obsahuje možnosť testovania a ladenia parserov bez vplyvu na ostatné produkčné funkcie systému.	
Prijaté logy má systém štandardizovať do jednotného formátu a logy sú rozdeľované do príslušných polí podľa ich typu. Systém musí zároveň uchovávať originálne verzie správ.	Prijaté logy systém štandardizuje do jednotného formátu a logy sú rozdeľované do príslušných polí podľa ich typu. Systém uchováva originálne verzie správ.	
Pre hodnoty jednotlivých parsovaných polí musí byť možné v definícii parseru zmeniť typ a štandardizovať minimálne na tieto základné druhy: číslo, IP adresa, MAC adresa, URL. Nad uloženými dátami typu číslo je možné pri vyhľadávaní vykonávať matematické operácie (súčty všetkých hodnôt, priemery, najmenšia/najväčšia hodnota a pod.).	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 je možné pri vyhľadávaní vykonávať matematické operácie (súčty všetkých hodnôt, priemery, najmenšia/najväčšia hodnota a pod.).	

Centrálny logovací systém musí zachovávať pôvodné informácie zo zdroju logu o časovej značke udalosti, ale nedôveruje jej a vytvára vlastné dôveryhodné časové razítko ku každému logu, ktorá vzniká v okamihu prijatia logu systémom a ktorým sa systém riadi. Všetky polia a položky prijaté systémom musia byť automaticky indexované. Nad všetkými položkami musí byť možné ihneď vykonávať vyhľadávanie bez nutnosti dodatočného ručného indexovania administrátorom. Centrálny logovací systém musí umožňovať zber udalostí vo formátoch RAW, Syslog.	Centrálny logovací systém zachováva pôvodné informácie zo zdroju logu o časovej značke udalosti, ale nedôveruje jej a vytvára vlastné dôveryhodné časové razítko ku každému logu, ktorá vzniká v okamihu prijatia logu systémom a ktorým sa systém riadi. Všetky polia a položky prijaté systémom sú automaticky indexované. Nad všetkými položkami je možné ihneď vykonávať vyhľadávanie bez nutnosti dodatočného ručného indexovania administrátorom. Centrálny logovací systém umožňuje zber udalostí vo formátoch RAW, Syslog.	
Centrálny logovací systém neumožňuje mazanie alebo modifikovanie uložených logov ani konfiguračnou zmenou administrátorovi systému s najvyššími oprávneniami. Každý log musí mať unikátny identifikátor, ktorý umožní jeho jednoznačnú identifikáciu.	Centrálny logovací systém neumožňuje mazanie alebo modifikovanie uložených logov ani konfiguračnou zmenou administrátorovi systému s najvyššími oprávneniami. Každý log má unikátny identifikátor, ktorý umožní jeho jednoznačnú identifikáciu.	
Centrálny logovací systém musí umožňovať konfiguráciu filtrácie nerelevantných správ, konsolidáciu logov na vlastnom storage priestore, 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 systému a aj súčasťou jednotného rozhrania.	Centrálny logovací systém umožňuje konfiguráciu filtrácie nerelevantných správ, konsolidáciu logov na vlastnom storage priestore, jednoduché vyhľadávanie udalostí a okamžité vytváranie grafických reportov (ad hoc) bez nutnosti dodatočného programovania alebo aplikovania dopytov v SQL jazyku. Reportovací nástroj je integrálnou súčasťou systému a aj súčasťou jednotného rozhrania.	
V prípade krátkodobého preťaženia systému nemôže dochádzať k strate logov. Všetky prijaté nespracované logy/udalosti sú ukladané do vyrovnávacej pamäte.	V prípade krátkodobého preťaženia systému nedôjde k strate logov. Všetky prijaté nespracované logy/udalosti sú ukladané do vyrovnávacej pamäte.	
Centrálny logovací systém musí umožňovať jednoducho vytvárať grafické znázornenie udalostí nad všetkými uloženými dátami za ľubovoľné časové obdobie bez nutnosti modifikácie konfigurácie systému alebo parametrov uložených dát. Historické dáta v požadovanej dĺžke retencie uložené v systéme je možné prehľadávať okamžite bez časových strát opätovného importu alebo dekomprimácie starších dát, prehľadávanie nevyžaduje manuálnu konfiguráciu a zásahy používateľa.	Centrálny logovací systém umožňuje jednoducho vytvárať grafické znázornenie udalostí nad všetkými uloženými dátami za ľubovoľné časové obdobie bez nutnosti modifikácie konfigurácie systému alebo parametrov uložených dát. Historické dáta v požadovanej dĺžke retencie uložené v systéme je možné prehľadávať okamžite bez časových strát opätovného importu alebo dekomprimácie starších dát, prehľadávanie nevyžaduje manuálnu konfiguráciu a zásahy používateľa.	
Systém musí podporovať natívne získavanie logov z M365.	Systém podporuje natívne získavanie logov z M365.	
Centrálny logovací systém musí umožňovať unifikované vyhľadávanie naprieč všetkými typmi dát a zariadení podľa normalizovaných polí a musí spĺňať požiadavky normy STN/ISO 27001:2013 pre získavanie auditných záznamov.	Centrálny logovací systém umožňuje unifikované vyhľadávanie naprieč všetkými typmi dát a zariadení podľa normalizovaných polí a spĺňa požiadavky normy STN/ISO 27001:2013 pre získavanie auditných záznamov.	

Centrálny logovací systém má mať možnosť uloženia užívateľom vytvorených pohľadov na dáta (dashboardov) pre budúce spracovanie.	Centrálny logovací systém má možnosť uloženia užívateľom vytvorených pohľadov na dáta (dashboardov) pre budúce spracovanie.	
Centrálny logovací systém musí obsahovať reportovací nástroj s prednastavenými najbežnejšími reportami a možnosťou vlastných úprav a vytváranie nových pohľadov.	Centrálny logovací systém obsahuje reportovací nástroj s prednastavenými najbežnejšími reportami a možnosťou vlastných úprav a vytváranie nových pohľadov.	
Centrálny logovací systém musí umožňovať kapacitnú i výkonovú škálovateľnosť.	Centrálny logovací systém umožňuje kapacitnú i výkonovú škálovateľnosť.	
Monitoring stavu systému - alertovanie pri prekročení prahových hodnôt alebo chybe systému, preposlanie upozornenia pomocou SMTP alebo Syslog.	Monitoring stavu systému - alertovanie pri prekročení prahových hodnôt alebo chybe systému, preposlanie upozornenia pomocou SMTP alebo Syslog.	
Centrálny logovací systém musí obsahovať REST-API pre integráciu s externým monitorovacím systémom (Zabbix, Nagios, PRTG a pod.)	Centrálny logovací systém obsahuje REST-API pre integráciu s externým monitorovacím systémom (Zabbix, Nagios, PRTG a pod.)	
Centrálny logovací systém musí umožňovať jednoduché vytváranie užívateľských rolí definujúcich prístupové práva k uloženým udalostiam a jednotlivým ovládacím komponentom systému, vykonávať parsovanie a normalizáciu prijatých udalostí bez nutnosti inštalovať externé aplikácie alebo systémy a to priamo vo svojom rozhraní.	Centrálny logovací systém umožňuje jednoduché vytváranie užívateľských rolí definujúcich prístupové práva k uloženým udalostiam a jednotlivým ovládacím komponentom systému, vykonávať parsovanie a normalizáciu prijatých udalostí bez nutnosti inštalovať externé aplikácie alebo systémy a to priamo vo svojom rozhraní.	
Centrálny logovací systém musí podporovať overovanie užívateľa systému na externom LDAP serveri. V prípade výpadku externého LDAP systému musí podporovať overenie z lokálnej databázy. Systém má automaticky zaznamenávať užívateľské meno ku každej akcii užívateľom.	Centrálny logovací systém podporuje overovanie užívateľa systému na externom LDAP serveri. V prípade výpadku externého LDAP systému podporuje overenie z lokálnej databázy. Systém automaticky zaznamenáva užívateľské meno ku každej akcii užívateľom.	
Aktualizácie systému by mali byť distribuované v jednotnom balíku a ich inštalácia je vykonávaná cez centrálnu správcovskú konzolu. Všetky aktualizácie by mali byť vykonávané z webového rozhrania systému bez potreby asistencie výrobcu/dodávateľa.	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	Systém podporuje downgrade, napríklad pri problémoch s novou verziou systému po upgrade	
Licenčne musí byť neobmedzený počet zariadení pre príjem zasielaných udalostí. Licenčne musí byť neobmedzený počet udalostí v GB za deň. Integrovaná databáza musí podporovať kompresiu ukladaných dát.	Licenčne je neobmedzený počet zariadení pre príjem zasielaných udalostí. Licenčne je neobmedzený počet udalostí v GB za deň. Integrovaná databáza podporuje kompresiu ukladaných dát.	
Centrálny logovací systém musí podporovať zálohovania alebo obnovy konfigurácie v jednom kroku a jednom súbore pre celý systém a taktiež musí podporovať zálohovanie dát na externý systém, požadované je plánované aj ad-hoc zálohovanie.	Centrálny logovací systém podporuje zálohovania alebo obnovy konfigurácie v jednom kroku a jednom súbore pre celý systém a tiež zálohovanie dát na	

	externý systém, a to aj pre je plánované aj pre ad-hoc zálohovanie.	
Centrálny logovací systém musí byť schopný na základe zadaných podmienok splnených v prijatých dátach vygenerovať alert. Text emailu vygenerovaného alertom môže byť užívateľsky definovaný s premennými z prijatej rozparsovanej udalosti. Centrálny logovací systém by mal obsahovať výrobcom predpripravené sety/vzory alertov a korelácií. Užívateľská konfigurácia alertov musí byť možná pomocou vizuálneho programovacieho jazyka v centrálnej správcovskej konzole. Vizuálny programovací jazyk nemôže byť prezentovaný čisto textovo, ale textovo-grafickou formou, ktorá vizualizuje aplikačnú logiku. Konfigurácia alertu alebo korelácie umožňuje okamžitú kontrolu. Ako výstupné pravidlo alertu systém musí vedieť odoslať udalosť, ktorá alert vyvolala na externý systém prostredníctvom SMTP alebo Syslog cez TCP protokol. Pre Syslog protokol musí byť možnosť definície formátu dát pre jednoduchšiu integráciu so systémami tretích strán. V alertoch by mala byť možnosť využívať značky. Systém musí podporovať funkcie SIEM - korelácie udalostí a upozornenia s hraničnými limitmi. Definícia korelačných pravidiel má mať možnosť vloženia testovacej správy a výsledku testu vykonanej akcie	Centrálny logovací systém je schopný na základe zadaných podmienok splnených v prijatých dátach vygenerovať alert. Text emailu vygenerovaného alertom môže byť užívateľsky definovaný s premennými z prijatej rozparsovanej udalosti. Centrálny logovací systém obsahuje výrobcom predpripravené sety/vzory alertov a korelácií. Užívateľská konfigurácia alertov je možná pomocou vizuálneho programovacieho jazyka v centrálnej správcovskej konzole. Vizuálny programovací jazyk je prezentovaný textovo-grafickou formou, ktorá vizualizuje aplikačnú logiku. Konfigurácia alertu alebo korelácie umožňuje okamžitú kontrolu. Ako výstupné pravidlo alertu systém vie odoslať udalosť, ktorá alert vyvolala na externý systém prostredníctvom SMTP alebo Syslog cez TCP protokol. Pre Syslog protokol je možné definovať formát dát pre jednoduchšiu integráciu so systémami tretích strán. V alertoch je možnosť využívať značky. Systém podporuje funkcie SIEM - korelácie udalostí a upozornenia s hraničnými limitmi. Definícia korelačných pravidiel má možnosť vloženia testovacej správy a výsledku testu vykonanej akcie	
Centrálny logovací systém by mal získavať udalosti z Microsoft prostredia buď pomocou agenta inštalovaného priamo na koncovom zariadení s Windows systémom, alebo iným spôsobom. Agent súčasne musí podporovať monitoring interných Windows logov, a aj monitoring textových súborových logov. Agent musí zaisťovať zber nemodifikovaných udalostí a detailné spracovanie auditných informácií. Agent musí podporovať nastavenie filtrácie odosielaných udalostí pomocou centrálnej správcovskej konzoly. Filtrácia odosielaných udalostí agentom sa musí konfigurovať pomocou vizuálneho programovacieho jazyka v centrálnej správcovskej konzole. Nerelevantné logy majú byť filtrované na strane agenta a nie sú odosielané po sieti. Vizuálny programovací jazyk nesmie byť prezentovaný textovo, ale textovo-grafickou formou, ktorá vizualizuje aplikačnú logiku. Agent nesmie vyžadovať administrátorské zásahy na koncovom systéme – je centrálne spravovaný a automaticky aktualizovaný priamo z centrálnej správcovskej konzoly systému. Správa a aktualizácia agenta sa nevykonáva z Group Policy. Komunikácia Windows agenta a centrálneho logovacieho systému je šifrovaná. Agent musí podporovať zber nielen zo základných systémových logov (Aplikácie, Zabezpečenie, Inštalácie, Systém), ale aj zber všetkých ostatných logov v zložke	Centrálny logovací systém získava udalosti z Microsoft prostredia štandardne pomocou agenta inštalovaného priamo na koncovom zariadení s Windows systémom, alebo iným spôsobom. Agent súčasne podporuje monitoring interných Windows logov, a aj monitoring textových súborových logov. Agent zaisťuje zber nemodifikovaných udalostí a detailné spracovanie 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 agenta a nie sú odosielané po sieti. Vizuálny programovací jazyk je textovo-grafickej formy, ktorá vizualizuje aplikačnú logiku. Agent nevyžaduje administrátorské zásahy na koncovom systéme – je centrálne spravovaný a automaticky aktualizovaný priamo z centrálnej správcovskej konzoly systému. Správa a aktualizácia agenta sa nevykonáva z Group Policy. Komunikácia Windows agenta a centrálneho logovacieho systému je šifrovaná.	

protokoly aplikácií a služieb. Agent musí podporovať centralizované nastavenie z administrátorskej konzoly systému pre zber textových logov vrátane možnosti výberu ich formátu. Agent musí automaticky dopĺňať ku všetkým odosielaným udalostiam ich textový popis tak, ako je zobrazený v prehliadači udalostí (Event Viewer) na koncovom systéme. Počet inštalácií agenta nemôže byť licenčne ani časovo obmedzený.	Agent podporuje zber nielen zo základných systémových logov (Aplikácie, Zabezpečenie, Inštalácie, Systém), ale aj zber všetkých ostatných logov v zložke protokoly aplikácií a služieb. Agent podporuje centralizované nastavenie z administrátorskej konzoly systému pre zber textových logov vrátane možnosti výberu ich formátu. Agent automaticky dopĺňa ku všetkým odosielaným udalostiam ich textový popis tak, ako je zobrazený v prehliadači udalostí (Event Viewer) na koncovom systéme. Počet inštalácií agenta nie je licenčne ani časovo obmedzený.	
Súčasťou výstupu bude: • technický návrh riešenia, ktorý zahŕňa popis nasadených produktov, schému zapojenia do infraštruktúry a spôsob napojenia na jednotlivé systémy obstarávateľa, • technický popis riešenia pri odovzdávke diela, • metodický postup, ponaučenia z projektu a best practice, ktoré budú využiteľné pre iné štátne organizácie a orgány verejnej moci pri zavádzaní Log manažment systému.	V rámci výstupu sa vypracuje: - technický návrh riešenia, ktorý zahŕňa popis nasadených produktov, schému zapojenia do infraštruktúry a spôsob napojenia na jednotlivé systémy obstarávateľa, - technický popis riešenia pri odovzdaní diela, - metodický postup, ponaučenia z projektu a best practice, ktoré budú využiteľné pre iné štátne organizácie a orgány verejnej moci pri zavádzaní Log manažment systému.	
HW musí byť v rackovom prevedení o výške max. 2U. HW bude obsahovať všetky potrebné komponenty a musí byť nezávislý na ďalších systémoch. V cene dodania musí byť aj zberná sonda (forwarder).	Zariadenie LogManager XL spĺňa všetky požadované parametre vrátane nasledujúcich: - Zariadenie je dodávané v rackovom prevedení s maximálnou výškou 2U. - Hardvér obsahuje všetky potrebné komponenty a je plne nezávislý na ďalších systémoch. - V rámci dodávky je zahrnutá aj zberná sonda (forwarder).	
HW bude dodaný tak, aby spĺňal nasledovné minimálne parametre: • min. 9500 udalostí za sekundu pri priemernej veľkosti jednej udalosti 1 KB, s možnosťou výkonu pri útoku min 19000 udalostí po dobu min. 10 minút. • retencia logov min. pol roka; • diskový subsystém s čistou dostupnou kapacitou min. 100TB pre integrovanú databázu a s redundanciou; • Min. 4x 10Gbit SFP+ 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, t. j. prevzatie textovej i grafickej konzoly serveru a prenos povelov z klávesnice a myši vzdialeného počítača; • Systém pre vzdialenú správu serveru vrátane potrebnej licencie, • Hardvérová min. 5 ročná záručná servisná podpora na	Zariadenie LogManager XL spĺňa všetky požadované minimálne parametre: - Zariadenie zvláda 10000 udalostí za sekundu pri priemernej veľkosti jednej udalosti 1 KB a umožňuje zvýšenie výkonu až na 20000 udalostí po dobu min. 10 minút v prípade útoku. - Retencia logov je zabezpečená na min. pol roka. - Diskový subsystém poskytuje čistú dostupnú kapacitu. 120 TB pre integrovanú databázu a je vybavený redundanciou. - Zariadenie obsahuje. 4x 10Gbit SFP+ porty a 1x dedikovaný 1Gbit port pre manažment hardvéru. - LogManager XL je vybavený redundantnými ventilátormi, ktoré sú vymeniteľné za chodu.	

hardware appliance s opravou na mieste inštalácie serveru a s garantovanou odozvou nasledujúci pracovný deň od nahlásenia prípadnej závady	- Napájacie zdroje s redundanciou 1+1 sú tiež vymeniteľné za chodu a dosahujú účinnosť min. 94%. - Podporuje virtuálne KVM, čo umožňuje prevziať textovú i grafickú konzolu servera a prenos príkazov z klávesnice a myši vzdialeného počítača. - Obsahuje systém pre vzdialenú správu serveru vrátane potrebných licencií. - LogManager XL poskytuje hardvérovú záruku a servisnú podporu na 5 rokov, vrátane opravy na mieste inštalácie serveru s garantovanou odozvou nasledujúci pracovný deň po nahlásení prípadnej závady.	
Licencie na používanie Log manažment systému a bezplatné softvérové aktualizácie minimálne po dobu min. 4 rokov	Licencie na používanie systému LogManager sú poskytované na 4 roky, vrátane bezplatných softvérových aktualizácií počas tohto obdobia.	
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. Výsledkom verejného obstarávanie bude nainštalovaný a funkčný systém zbierania logov nad nasledovnými systémami obstarávateľa: * Microsoft 365/intune, Azure AD/ * Active directory, * Exchange * Optimidoc tlačový server * Tlačiarne * sieťové prvky obstarávateľa /Aruba AP, Cisco Switche, FortiGate FW, FortiToken/, * windows pracovne stanice /cca 720ks/ * windows servre * VMware platforma * Linux servre * Docker platforma * Aplikacie Uradu /Registratura - Nuaktiv, SQL server/ * integrácia na SIEM.	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. Nainštalovaný systém zbierania logov bude fungovať nad nasledovnými systémami obstarávateľa: * Microsoft 365/intune, Azure AD/ * Active directory, * Exchange * Optimidoc tlačový server * Tlačiarne * sieťové prvky obstarávateľa /Aruba AP, Cisco Switche, FortiGate FW, FortiToken/, * windows pracovne stanice /cca 720ks/ * windows servre * VMware platforma * Linux servre * Docker platforma * Aplikacie Uradu /Registratura - Nuaktiv, SQL server/ * integrácia na SIEM.	
Súčasťou dodávky je školenie v rozsahu 2 školiacich dní. Školenie zahŕňa: vytvorenie a uloženie 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; zaškolenie obsluhy a správy systému pre relevantné správcovské roly, ukážka integrácie na SIEM	Súčasťou dodávky je školenie v rozsahu 2 školiacich dní. Školenie zahŕňa: vytvorenie a uloženie 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; zaškolenie obsluhy a správy systému pre relevantné správcovské roly, ukážka integrácie na SIEM	

*Vyplní uchádzač podľa vlastného návrhu

* Dodávateľ ako súčasť dodania predmetu zákazky zabezpečí záručný servis podľa platných právnych predpisov a v zmysle ustanovení obchodného zákonníka a to počas celej záručnej doby.