Nabídka uchazeče: (název a typ nabízeného řešení)	
Architektura	**Plnění parametrů (Ano /Ne)**
Systém musí být navržen ve vysoké dostupnosti, tj. odolné proti výpadkům a poruchám jednotlivých částí Systému tzv. HA.	Ano
Systém tedy musí být postaven na moderní clusterové architektuře za účelem dosažení vysoké dostupnosti	Ano
Účastník zadávacího řízení uvede v nabídce podrobné blokové schéma zapojení Systému, kterým osvědčí naplnění tohoto požadavku zadavatele	Ano
Více-uzlový nástroj se musí chovat jako 1 celek	Ano
V případě rozšíření clusteru (přidání dalšího uzlu) je podporována funkce virtuální IP adresy – z datových zdrojů se události posílají na jedinou IP adresu a cluster zajišťuje synchronizaci událostí mezi jednotlivými uzly	Ano
Systém musí být odolný vůči výpadku jednoho datového centra nebo lokality	Ano
Implementace systému musí být provedena jako „on premise“	Ano
Řešení musí běžet v provedení aktivního clusteru, tj. po celou dobu běhu aktivně využívat všech hardwarových zdrojů, které jsou k dispozici	Ano
Zadavatel vylučuje nasazení v Režimu aktive/pasiv	Ano
Systém nesmí obsahovat "single-point-of-failure", tj. nesmí obsahovat žádný prvek, jehož výpadek by způsobil ztrátu funkčnosti celého Systému, tj. požadovaný hardware bude dodán v počtech kusů umožňujících redundanci odpovídající High Availability clusteru a bude takto zapojen a konfigurován	Ano
Systém musí poskytovat nejméně 100TB datového prostoru (včetně komprimace) v každém serveru pro archivaci logů	Ano
Zadavatel nepřipouští využití pro provoz Systému jeho stávajících hardwarových zařízení (serverů, virtualizačních platforem, sond, kolektorů apod	Ano
Systém musí být dodán jako kompletní řešení složené z hardware a software, to bez dalších nároků na ICT zdroje zadavatele	Ano
Řešení musí poskytovat možnosti distribuované architektury, kde pomocí kolektorů v jednotlivých prostředích a lokalitách bude docházet ke sběru logů a následnému transportu do centrální komponenty ke zpracování a archivaci logů.	Ano
Aktualizace nástroje jsou možné distribuovat online i offline	Ano
Upgrade i downgrade verzí nástroje musí probíhat bez restartu či rebootu, a to za účelem poskytování nepřetržité funkce nástroje i průběhu upgrade and downgrade	Ano

Řešení musí podporovat tzv. rolling upgrade, tj. postupný upgrade jednotlivých uzlů clusteru bez celkového downtime systému minimálně z pohledu příjmu logů	Ano
Veškerá konfigurace, musí být verzována ve version control systému (např. Git) tak, aby byla zajištěná vysoká úroveň kontroly nad provozním nastavením systému včetně možnosti návratu k předchozí verzi konfigurace	Ano
Nástroj musí mít podporu zrcadlení a clusteru – 2 a více zařízení v režimu active / active	Ano
Nástroj musí být nasazen v nativním plnohodnotném active-active clusteru	Ano
Nástroj musí v případě havárie libovolného uzlu clusteru podporovat přepojení zdrojů logů na zbylé aktivní uzly clusteru bez zásahu administrátora	Ano
Administrátor musí mít přístup ke všem komponentám systému a to až na úroveň příkazové řádky	Ano
Nástroj musí mít mikroservisovou architekturu	Ano
Nástroj musí mít oddělené systémové datové úložiště (s aplikací a operačním systémem) od uložišť logů	Ano
Licencování	
Licence neomezuje počet připojených zdrojů logů	Ano
Licence umožňuje generovat neomezený počet reportů	Ano
Licence umožňuje tvorbu neomezeného množství dashboardů	Ano
Licence umožňuje tvorbu neomezeného množství parserů logů	Ano
Licence umožňuje nasazení jako virtuální appliance do cloudu	Ano
Licence umožňuje nasazení v tzv. multi-tenancy módu. Systém musí poskytovat logicky oddělené samostatné datové prostory, tzv. tenanty	Ano
Systém nesmí být zcela uzavřená aplikace, ale musí být možné jej integrovat nejenom s různými zdroji, ale i s kontextovými informacemi pomocí skriptů	Ano
Systém musí umožňovat integrace tak, aby bylo možné čerpat zkušenosti a návody z internetových komunit a tím zefektivnit provoz a rozšiřovaní systému.	Ano
Systém musí umožňovat trvale zpracovávat (tj. zaznamenával logy) z nejméně 300 zdrojových zařízení;	Ano
Systém musí umožňovat trvale zpracovávat nejméně 1000 EPS (Events Per Second) a nepřetržitě výkonovou špičku po dobu alespoň 60 minut nejméně 5000 EPS bez ztráty dat	Ano
Při překročení maximálního zakoupeného objemu zpracovaných dat nesmí dojít ke ztrátě či k zahození dat, nebo k omezení funkčnosti nástroje	Ano
Při opakovaném překročení maximálního zakoupeného objemu zpracovaných dat musí nástroj upozornit na překročení limitu	Ano

Systém musí být schopen zaznamenávat a vyhodnocovat vlastní logy stejným způsobem jako logy ostatních Zdrojů	Ano
Způsob zpracování: logy jsou zpracovávány pomocí parsingu do strukturovaných eventů, které jsou normalizovány do některého z obecně známých a rozšířených schémat (např. CEF, LEEF, Sigma, ECS);	Ano
Základní požadavky	Ano
Nástroj musí umožnit přístup více uživatelů současně, a to jak na úrovni přístupu ke vstupním/zdrojovým datům systému, tak i k incidentům	Ano
Nástroj umožňuje snadné vytváření uživatelských rolí definujících přístupová práva k uloženým událostem a jednotlivým konfiguračním komponentám nástroje	Ano
Přístup uživatelů musí být založen na volně definovaných, oddělených rolích s možností granulárního přidělování práv v rámci každé role, dle zdrojových dat, identifikace monitorovaných zařízení, skupin zařízení a serverů, typu vstupních dat, apod.	Ano
Role nesmí být vázány na AD, musí být spravovatelné interně	Ano
Nástroj musí podporovat kompletní oddělení přístupu skupin uživatelů k odlišným datům a konfiguracím (multi-tenantnost), kdy jednotlivé instance mají vlastní konfigurace a samostatně oddělená uložiště logů	Ano
Nástroj podporuje ověřování uživatelů nástroje na externím AD / LDAP serveru. V případě výpadku externího LDAP, nástroj musí podporovat ověření z lokální databáze.	Ano
Nástroj obsahuje vícefaktorovou autentikaci uživatelů systému	Ano
Vyžaduje se zejména vícefaktorová autentikace pomocí hardwarového tokenu, TOTP a hardwarového klíče v mobilním telefonu podle speficikace FIDO2.	Ano
Nástroj umožňuje definování uživatelských rolí s možností nastavení přístupových práv (možností granulárního přidělování práv v rámci role podle zdrojů logů, skupin zařízení, jednotlivých serverů, typu logu apod.).	Ano
Nástroj umožňuje nastavit pravidelné automatické přesuny dat z interního do externího úložiště, resp. archivu podle definovaných pravidel, a bez vzniku neautorizovaných změn	Ano
Nástroj podporuje nastavení retence dat s možností nastavení pravidel pro automatické mazání dat	Ano
Nástroj umožňuje retenci (uložení logů) minimálně na 3 měsíce v režimu přímého prohledávání	Ano
Nástroj umožňuje retenci (uložení logů) minimálně 18 měsíců v archivu	Ano
Nástroj umožňuje nastavit nezávislé retenční politiky pro jednotlivá úložiště logových dat	Ano
Nástroj umožňuje snadnou obnovu historických dat z archivu pro zpětnou analýzu	Ano
Nástroj podporuje provoz v prostředí TCP/IP IPv4 i IPv6	Ano
Nástroj umožňuje synchronizaci interního času nástroje s externím NTP serverem	Ano

Nástroj musí pro veškerou kryptografii využívat kryptografickou komponentu, která splňuje platné doporučení NÚKIB pro kryptografické prostředky „Doporučení v oblasti kryptografických prostředků verze 3.0“	Ano
Nástroj poskytuje vlastní provozní a auditní log o aktivitě uživatelů alespoň v rozsahu přihlášení, odhlášení uživatele do/z centrální konzole nástroje, evidence provedených konfiguračních změn a varovná nebo chybová hlášení	Ano
Konfigurační a nástrojové rozhraní a dokumentace musí být identické v českém nebo anglickém jazyce	Ano
Všechny komponenty nástroje, včetně komponent třetích stran, musí být aktuální a nesmí obsahovat zastaralé verze. Za zastaralou verzi komponenty se považuje taková, pro kterou výrobce nebo správce již nevydává nové vyšší „major“ verze, které řeší např. bezpečnostní chyby či jiné zásadní problémy.	Ano
Zadavatel požaduje doložit použité verze u všech komponent	Ano
Bezpečnost systému	
Systém musí umožňovat ochranu integrity "raw" logů digitálními podpisy, přičemž použitý kryptografický algoritmus musí splňovat platná doporučení NÚKIB pro kryptografické prostředky „Doporučení v oblasti kryptografických prostředků verze 3.0“	Ano
Systém musí pro sběr logů musí používat výhradně silné autentizované spojení pro odesílání logů, např. Mutual SSL/TLS tak, aby se vyloučila manipulace se vstupními logy během jejich transportu	Ano
Účastník zadávacího řízení popíše, jaký bude nabízený Systém využívat kryptografický algoritmus pro zajištění integrity uložených logů	Ano
Systém umožňuje řídit přístupy uživatelů např. pomocí systému RBAC (Role-based Access Control).	Ano
Systém musí řídit přístupová práva uživatelů pro konkrétní tenanty, tj. uživatel může mít jiná práva v různých tenantech	Ano
Systém musí nabízet přístup k datům prostřednictvím API pro integraci s dalšími systémy.	Ano
Součástí dodávky musí být podrobná dokumentace API v českém jazyce nebo i anglickém jazyce	Ano
Systém musí být otevřený pro administrátorské zásahy i z příkazové řádky	Ano
Součástí dodávky musí být podrobná administrátorská, provozní a bezpečnostní dokumentace v českém jazyce	Ano
Systém musí dimenzován tak, aby umožňoval následující retenci logů:	Ano
zpracované (parsované) logy musí být dostupné po dobu minimálně 3 měsíců pro vyhledávání a další analytickou práci;	Ano
"raw" logy musí být uloženy po 18 měsíců v archivu, tj. úložišti kde je dostupnost archivovaných dat zajištěna alespoň na úrovni zrcadlení úložiště, tj. toto úložiště musí být integrální součástí Systému.	Ano
Archiv musí být nezávislý na databázi použité pro ukládání zpracovaných logů	Ano
Při archivovaní musí být zajištěno, že nedojde ke změně logů, jejich integrity, ani k změně hashů	Ano

Účastník zadávacího řízení popíše specifikaci této ochrany s ohledem na platné doporučení NÚKIB pro kryptografické prostředky „Doporučení v oblasti kryptografických prostředků verze 3.0“	Ano
Integritu logů v archivu lze ověřit pomocí běžných nástrojů, ověření může provést třetí strana bez přístupu k nástroji	Ano
Systém musí být topologicky distribuovaný, komponenty sběru a zpracování musí být funkčně i technicky oddělené od ostatních částí Systému, přičemž splnění tohoto požadavku musí vyplývat z předloženého blokového schématu	Ano
Sběr a zpracování logů	
Systém musí nabízet konfigurovatelné rozhraní (musí obsahovat alespoň API a vlastní parsery) pro uzpůsobení odlišnostem jednotlivých zdrojů	Ano
Sběr logů alespoň pomocí protokolů Syslog (UDP, TCP, TLS), SNMP, CEF, LEEF, HTTP/S	Ano
Systém musí poskytovat bezagentový sběr logů (sběr bez nutnosti instalovat agenta na cílový systém)	Ano
Systém musí poskytovat sběr Windows Events pomocí WEC/WEF a centralizované konfigurace doménového řadiče, vylučuje se použití agenta instalovaného na počítače s OS Windows	Ano
Systém musí poskytovat sběru logů samostatným kolektorem, který přeposílá logy do centrálního systému	Ano
Systém musí poskytovat sběr logů z dalších bezpečnostních a síťových systémů (alespoň firewall, IDS/IPS, routery, switche, AP controllery, Network Access Control);	Ano
Systém musí poskytovat možnost agregace událostí z logů i podle položek, které nejsou standardně zahrnuty v Systému, tj. Systém musí umožňovat uživatelsky vytvářet vlastní parsery;	Ano
Systém musí poskytovat sběr textových logů ze souborů;	Ano
Systém musí poskytovat sběr logů z databází minimálně pomocí ODBC a JDBC;	Ano
Systém musí poskytovat sběr log záznamů z prostředí Windows a Linux/Unix;	Ano
Systém musí poskytovat sběr logů z API rozhraní v podobě REST-API i SOAP;	Ano
Systém musí poskytovat sběr logů z XML i JSON souborů;	Ano
Systém musí uchovávat logy jak v normalizovaném formátu, tak i v „raw“ formátu a to v technologicky oddělených uložištích	Ano
Při přetížení Systému nesmí dojít ke ztrátě přijímaných zpráv. Všechny přijaté nezpracované logy/události musí být ukládány do vyrovnávací paměti (např. kolektoru) pro následné zpracování	Ano
Systém provádí normalizaci přijímaných událostí a logů minimálně v rozsahu typ činnosti, datum a čas, identifikaci datového zdroje, identifikaci původce a místa činnosti záznamu, úspěšnost nebo neúspěšnost činnosti	Ano
Systém provádí automatické doplňování GeoIP informací k událostem	Ano

Systém provádí automatické doplňování výrobce zařízení z MAC adres v událostech	Ano
Nástroj obsahuje kolektor, který umožňuje sběr událostí ve vzdálených lokalitách a jejich odeslání po saturované lince bez ztráty dat	Ano
Kolektor logů lze provozovat mimo centrální instalaci	Ano
Kolektor musí být k dispozici jako virtuální a hardwarová appliance.	Ano
Nástroj musí podporovat sběr logů v režimu vysoké dostupnosti (HA), tj:	Ano
Zasílání logů ze zdroje logů na dvě a více instancí kolektorů (push)	Ano
Odebíraní logů ze zdroje dvěmi a více instancemi kolektorů (pull)	Ano
Kolektor musí podporovat připojení k centrálnímu systému v režimu vysoké dostupnosti, konkrétně se kolektor musí umět v případě ztráty spojení automaticky připojit na další dostupný uzel a tudíž je zajištěn bezvýpadkový sběr logů	Ano
Nástroj šifruje a komprimuje posílaná data a zabezpečuje je proti jejich modifikaci nebo smazání. Je garantováno doručení do centrálního prvku	Ano
Nástroj podporuje centralizovanou správu sběru dat přímo z centrální konzole bez ohledu, zda sběr probíhá nebo neprobíhá přes kolektor	Ano
Kolektor je schopen automaticky navázat spojení (po instalaci nebo po výpadku) s centrálním nástrojem a přenášená data šifrovat	Ano
Nástroj komunikuje po definovaném IP protokolu s možností nastavení sítě pro zajištění kvality služeb (QoS) pro přenos událostí	Ano
Kolektor poskytuje kapacitu vyrovnávací paměti pro minimálně 1 TB dat pro jejich uchování během výpadku spojení s centrálním nástrojem/serverem	Ano
Nástroj v centrální uživatelské konzoli poskytuje online přehled připojených a nepřipojených kolektorů, včetně přehledového monitoru aktivity přijmu logů na jednotlivých kolektorech.	Ano
Sběr dat probíhá bez-agentním způsobem, tj. bez instalace agenta na zdrojové systémy a zařízení.	Ano
Komponenty nástroje musí být schopny komunikovat s centrálním nástrojem i přes vícenásobný překlad adres (NAT) včetně managementu	Ano
Nástroj nevyžaduje instalaci dalších podpůrných nástrojů a aplikací na zdrojové systémy (kompletně bez-agentový sběr)	Ano
Nástroj podporuje načítání log souborů (jedno a víceřádkové textové logy), kde tyto soubory mají stanovenu strukturu a význam dat.	Ano
Nástroj umožňuje přijímat logy i na uživatelsky definovaných UDP a TPC portech.	Ano
Sběr logů v prostředí Windows musí probíhat přes technologii WEC/WEF.	Ano

Kolektor musí podporovat připojení do Microsoft Windows AD domény pomocí Kerberos.	Ano
Nástroj umožňuje zobrazit logy v původní formě jak byly přijaty, tzv. raw message.	Ano
Při přetížení nástroje nesmí dojít ke ztrátě přijímaných zpráv. Všechny přijaté nezpracované logy/události musí být ukládány do vyrovnávací paměti (např. kolektoru) pro následné zpracování.	Ano
Nástroj umožňuje uložit různé druhy logů po různě dlouhou dobu (retenční perioda). Nástroj musí poskytovat neomezené množství těchto skupin	Ano
Nástroj je schopen detekovat výpadek zdrojů logů (jak typu, tak jednotlivých serverů) v centrální konzoli, včetně upozornění na tento stav	Ano
Nástroj musí detekovat i anomálie ve sběru logů, zejména např. výrazně vyšší příjem logů z konkrétních zařízení, než je předpokládany příjem na základě historických dat	Ano
Sběr logů musí používat výhradně silné autentizované spojeni pro odesílání logů, např. Mutual SSL/TLS tak, aby se vyloučila manipulace se vstupními logy během jejich transportu.	Ano
Kolektor logů musí podporovat automatizovanou obnovu klientských certifikátů. Maximální platnost klientského certifikátu kolektoru logů je 6 měsíců	Ano
Nástroj provádí normalizaci přijímaných událostí a logů minimálně v rozsahu typ činnosti, datum a čas, identifikaci datového zdroje, identifikaci původce a místa činnosti záznamu, úspěšnost nebo neúspěšnost činnosti	Ano
Nástroj musí podporovat přijímání a zpracovávání logů, událostí a další strojově generovaných data prostřednictvím minimálně následujících protokolů a formátů:	Ano
Syslog RFC3164 přes UDP, TCP a SSL	Ano
Syslog RFC5424 přes UDP, TCP a SSL	Ano
Syslog RFC3195 BEEP přes TCP a SSL	Ano
Syslog RFC6587 přes TCP a SSL	Ano
Windows Event Collection (WEC/WEF)	Ano
s autentizací pomocí SSL certifikátů	Ano
s autentizací pomocí Kerberos	Ano
FTP	Ano
SFTP	Ano
SNMP	Ano
ODBC nebo JDBC	Ano
Apache Kafka	Ano
Rest API	Ano

CEF	Ano
LEEF	Ano
JSON	Ano
XML	Ano
Text file, single line	Ano
Text file, multiline	
Zpracování logů	
Přijaté logy nástroj standardizuje do jednotného formátu a logy jsou normalizovány (rozdělovány) do příslušných polí dle jejich typu se současným uchováním originální verze zpráv	Ano
Nástroj zachovává původní informaci ze zdroje logu o časové značce události, ale nedůvěřuje jí a vytváří vlastní důvěryhodné časové razítko ke každému logu, kterým se nástroj defaultně řídí	Ano
Nástroj musí podporovat minimálně dvě obecně rozšířená schémata polí, např. ECS, CEF, LEEF, Sigma	Ano
Všechna pole a položky přijaté nástrojem jsou automaticky indexovány s možností okamžitého vyhledávání bez nutnosti dodatečného ručního indexování administrátorem	Ano
Nástroj provádí automatické doplňování GeoIP informací k událostem a jejich grafické znázornění na mapě	Ano
Nástroj provádí automatické doplňování výrobce zařízení z MAC adres v událostech	Ano
Nástroj provádí automatické doplňování dle informací z externích zdrojů (doplnění hostname k IP, doplnění Jména k ID uživatele, doplnění identifikace lokality k ID čtečky karet apod.)	Ano
Přijímané události jsou automaticky kategorizovány pomocí sady přednastavených tzv. značek. (přihlášení, změna atd. včetně výsledku operace, úspěšná, neúspěšná apod.)	Ano
Archivace logů	
Nástroj musí umožňovat efektivní archivaci logů a všech ostatních zpracovávaných událostí na dobu minimálně 18 měsíců. Efektivita je definována jako poměr místa, které zabírají archivované logy a velikosti logů na vstupu. Požadován je poměr alespoň 1:10, tj. logy jsou při archivaci zkomprimovány alespoň na 10 procent jejich vstupní velikosti, a to včetně všech potřebných metadat.	Ano
Data v archivu musí být komprimovány s učinností minimálně 94%	Ano
Archiv musí podporovat připojení externích uložišť NAS, SAN atp.	Ano
Logy jsou do archivu ukládány ihned po vstupu do centrální komponenty, nezávisle na další zpracování v nástroji, jako je parsing, enrichment atd.	Ano
Archiv musí podporovat ukládání archivních souborů na NAS, SAN.	Ano

Archiv musí podporovat ukládání archivních souborů na pásky, pomocí páskové mechaniky, a to z důvodu požadavku na dvě různé technologie pro dlouhodobou archivaci.	Ano
Archiv musí podporovat ukládání archivních souborů na veřejné cloudy, minimálně Microsoft Azure a AWS S3.	Ano
Nástroj musí podporovat řízení životního cyklu archivovaných dat, ve kterém se stanovuje, kde jsou archivní soubory uloženy a případně kdy se mají přesouvat.	Ano
Archiv musí podporovat repliky archivních souborů tak, aby data mohla být uložena ve více kopiích na různých uložištích a fyzických místech.	Ano
Nástroj garantuje integritu uložených dat v archivu. Nesmí umožnit mazání nebo modifikování již uložených logů. Každý log musí mít unikátní identifikátor, který umožní jeho jednoznačnou identifikaci.	Ano
Pro garanci integrity logů v archivu se využívají kryptografické algoritmy (digitální podpisy, hašovací funkce), které vyhovují platným požadavků organizace ENISA.	Ano
Integritu logů lze ověřit pomocí běžných nástrojů, aby toto ověření mohla provést třetí strana bez přístupu k nástroji.	Ano
Logy v archivu je možné prohledávat pomocí standardních možností z konzole bez nutnosti je importovat zpět do nástroje.	Ano
Nástroj obsahuje přehled logů uložených v archivu, ze kterého je možné snadno dohledat, které archivní soubory obsahují logy ze zvoleného časového intervalu a kde jsou tyto archivní soubory uloženy.	Ano
Logy lze z archivu znovu v případě potřeby nahrát do nástroje. Při takovém nahrávání nástroj volitelně aplikuje detekční pravidla atd.	Ano
Úpravy a přizpůsobení	
Nástroj umožňuje dopsání parsovacích pravidel odpovědným administrátorem za nástroj bez nutnosti spolupráce s výrobcem nebo dodavatelem. Nástroj obsahuje nástroje pro jejich testování a lazení bez rizika negativního dopadu na ostatní funkce nástroje.	Ano
Vlastní zdroje logů, pro které je vyvinuté vlastní parsování, mají stejnou sadu funkcí a vlastností, jako ty nativně podporované výrobcem (sběr, parsování, doplňování dalších informací, filtrace, kategorizace atd.).	Ano
Možnost on-line uprav parsovacích pravidel – při jejich vytváření je možné vložit vlastní testovací zprávy, přičemž je okamžitě zobrazena výsledná podoba rozparsovaných dat a případná chybová hlášení.	Ano
Nástroj pro vývoj parsovacích pravidel musí podporovat automatizované testování vytvořených pravidel tzv. jednotkový test (unit test) a zařazení tohoto nástroje do CI/CD (continuous intergration/continous delivery) nástrojů.	Ano
Nástroj má možnost uložení uživatelem vytvořených pohledů na data (dashboardů) pro budoucí zpracování.	Ano
Text alertu lze uživatelsky definovat a je možné jej doplnit proměnnými z podkladové zprávy.	Ano

Nástroj je dodáván se sadou předpřipraveného obsahu. Uživatelé mohou bez omezení přistupovat k předpisům předpřipraveného obsahu a případně tento obsah měnit nebo rozšiřovat.	Ano
Nástroj musí podporovat full-textové vyhledávání v předpřipraveném a uživatelském obsahu.	Ano
Vyhledávání, zobrazení a reporting	
Nástroj poskytuje centrální webové rozhraní pro přístup k logům, alertům, reportům a pro správu nástroje. Z této konzole se provádí veškerá konfigurace, správa a analýza uložených dat.	Ano
Nástroj umožňuje snadné vyhledávání událostí bez nutnosti dodatečného programování nebo aplikování dotazů v SQL jazyce.	Ano
Nástroj umožňuje rychlé vyhledávání na základě fulltext indexace (vyhledávaní bez nutnosti tvorby parserů), tzn. že velké objemy dat se neprohledávají formou „grep like“ prohledávání po řádcích.	Ano
Nástroj umožňuje unifikované vyhledávání napříč všemi typy uložených dat (filtrování).	Ano
Nástroj obsahuje reportovací nástroj se sadou přednastavených reportů a možností vlastních úprav a vytvoření nových pohledů a reportů.	Ano
Prezentace dat musí být proveditelná v grafické podobě, prezentační rozhraní musí být multiplatformní nebo platformě nezávislé a plně funkční na platformách Windows, Linux, Apple OSX.	Ano
Nástroj obsahuje předpřipravené pohledy na uložená data dle jednotlivých kategorií zdrojových zařízení i dle logického členění.	Ano
Nástroj zajišťuje automatické spouštění definovaných reportů (měsíčně, týdně, denně, nebo v definovaném čase), ukládání na síťové úložiště a jejich zasílání e-mailem přímo ze systému.	Ano
Nástroj podporuje i automatizuje průběžné aktualizace reportů a pohledů výrobcem.	Ano
Nástroj umožňuje vytvářet reporty ve formátech PDF, HTML a CSV, popř. dalších.	Ano
Nástroj umožňuje zobrazení přehledu o využití diskového prostoru v interním úložišti nástroje.	Ano
Nástroj podporuje export vybraných dat přes rozhraní centrální konzole.	Ano
Nástroj podporuje export a sdílení log dat v originálním i ve strukturovaném tvaru.	Ano
Nástroj umožňuje anonymizovat některá vybraná pole (sloupce). Např. z důvodu ochrany citlivých informací, osobních údajů apod. Jejich neanonymizovaná hodnotu je možné zobrazit přímo ve výsledcích vyhledávání pouze vybraným uživatelům s oprávněním k této činnosti.	Ano
Nástroj musí nabízet sadu algoritmů pro deidentifikaci dat za účelem odstranění osobních informací z přijímaných logů. Požadované možnosti jsou: pseudoanynimizace, anonymizace, šifrování, maskování dat a šifrování se zachováním formátu (FPE).	Ano

Nástroj umožňuje drill-down prohlížení logů a eventů a identifikovaných stavů přímo překlikem z jednotlivých položek dashboardu	Ano
Řešení poskytuje analýzu dlouhodobých trendů událostí (vč. reportingu) v rozsahu dvou let.	Ano
Nástroj obsahuje monitor právě přijímaných logů (tzv. tail -f), který průběžně a v reálném čase zobrazuje příchozí logy včetně možnosti filtrování podle všech atributů obsažených v logových datech.	Ano
Nástroj poskytuje světlý a tmavý režim zobrazení pro uživatele kvůli větší ergonomice uživatelské práce.	Ano
Detekce	
Nástroj umožňuje detekce bezpečnostních hrozeb v reálném čase pomocí detekčních pravidel.	Ano
Detekční pravidla jsou dodávány výrobcem nástroje a to průběžně, pomocí online aktualizace.	Ano
Uživatel si může tvořit vlastní bezpečnostní pravidla, jakožto i uzpůsobovat pravidla dodávaná výrobcem.	Ano
Detekce jsou minimálně následujících typů:	Ano
Detekce na základě obsahu jednotlivých políček logu nebo jejich kombinací.	Ano
Detekce v časovém okně (tzv. korelace), tj takové, které sdružují (agregují) události pro specifikovaný sledovaný objekt (uživatele, IP adresu, hosta atd.) v časovém rozsahu.	Ano
Detekce anomálií s využitím mechanismů zdrojového učení.	Ano
Detekce s použitím Threat Intelligence vstupů, konkrétně IP adresy, hashe souborů, obsahy příkazových řádek a URL	Ano
Detekce je možno řetězit, tj. vystup jedné detekce lze použít v jiné detekci.	Ano
Výstupy detekce lze odesílat emailem, nástrojem Slack, Microsoft Teams nebo pomocí protokolu Syslog do nástrojů třetích stran.	Ano
Detekce dále mohou zakládat alerty v alert managementu.	Ano
Detekce mohou spouštět uživatelem definované scripty za účelem automatizace.	Ano
Nástroj obsahuje grafický nástroj pro tzv. Machine Learning, tj. vyhodnocování dat s využitím pokročilých matematických analýz, typicky využívající historická data uložená v systému.	Ano
Detekce anomálií musí být schopná využívat existující historické logy a jiné události pro stanovení běžných vzorů chování a ty pak aplikovat na aktuální vstupy. Odchylky jsou indikovány jako nálezy detekce.	Ano
Nástroj musí detekovat provoz z tzv. exit uzlů známých VPN poskytovatelů	Ano
Nástroj musí detekovat aktivitu z IP adres, které jsou označeny jako nebezpečné. Seznam nebezpečných IP adres poskytuje průběžně výrobce nástroje.	Ano
Nástroj musí umožňovat nasazení detekcí založených na Sigma pravidlech, https://github.com/SigmaHQ/sigma	Ano
Funkčnost systému	

centrální management:	Ano
umožňuje správu sběru logů, distribuci a oprávnění v rámci logování jednotlivých zdrojů	Ano
umožňuje provádění analýz, reportingů a diagnostiky Systému	Ano
umožňuje správu všech komponent a administrativních funkcí ve webovém uživatelském rozhraní	Ano
umožňuje poskytování interní kontroly stavu Systému a upozornění uživatele v případě problému	Ano
možnost ladění upozornění, alertů a vlastních parserů	Ano
sofistikované vyhledávací funkce včetně možnosti rozčlenění vyhledaných dat až na detailní úroveň všech typových polí dostupných ze zdroje událostí	Ano
způsob zadávání vyhledávání: vyhledávací rozhraní musí poskytovat podporu jak pro zadání dotazu s použitím Booleovské logiky, tak i pro regulární výrazy	Ano
poskytování rozhraní pro reporting, pomocí kterého lze vytvářet nové reporty bez vlivu na již existující	Ano
procesně vícestupňová aktualizace s podporou testování aktualizované verze před přechodem do produkčního provozu, a to bez přerušení provozu Systému a bez ztráty dat v jakékoliv jeho části	Ano
všechna pole vyparsovaná z logů musejí být indexovaná	Ano
generování alertu při výpadku logů z konkrétního zdroje	Ano
schopnost odesílat nasbírané logy na více míst ke zpracování najednou	Ano
Systém musí detekovat anomálie v příjmu logů (výpadek logů, větší než obvyklé množství logů, anomální počty chybových úrovní atp) a to v reálném čase, na základě predikcí průběžně vytvářených z historických dat	Ano
Logy v archivu je možné prohledávat pomocí standardních možností z příkazové řádky bez nutnosti je importovat zpět do Systému	Ano
Konfigurace a integrace	
Zadavatel požaduje provedení instalace, implementace, integrace včetně napojení na Zdroje, montáže a konfigurace Systému tak, aby bylo plně provozuschopné v síťové infrastruktuře zadavatele.	Ano
Zadavatel dále požaduje, aby Systém splňoval následující požadavky:	Ano
Systém musí podporovat napojení na SIEM systém bez nutnosti rozšiřovat licenci Systému nebo významné rekonfigurace Systému	Ano
Systém musí podporovat rychlé a snadné získávání "raw" logů z archivu v podobě souborů (a to i v případě nefunkčnosti Systému) a jejich následné načtení do technologií na práci s historickými daty.	Ano
Archiv logů musí být dostupný i v případě nedostupnosti systému.	Ano
Archivace se řídí konfigurovatelnou retenční politikou	Ano

Retenční politiku archivace logů lze konfigurovat odlišnou pro různé typy logů	Ano
Systém musí podporovat integraci s adresářovým systémem Microsoft AD/LDAP pro potřeby autentizace a autorizace uživatelů, přičemž součástí požadavku je rovněž, aby Systém musí tyto funkce podporovat včetně funkcí SSO a vícefaktorové autentizace	Ano
Systém musí podporovat zabezpečení kryptografickými algoritmy pro uživatelská hesla pro lokální účty uložená v Systému	Ano
Použité algoritmy musí splňovat platné požadavky NÚKIB na tyto algoritmy	Ano
Podpora provozu	
Dodavatel musí v rámci placené podpory Systému poskytovat pravidelné profylaktické prohlídky a to nejméně jedenkrát měsíčně. Výstupem profylaktické prohlídky je souhrná zpráva o stavu systému doplněná o případné nálezy a nápravná opatření	Ano
Dodavatel dodavatel v rámci placené podpory Systému implementuje nápravná opatření, v součinnosti se Zadavatelem	Ano
Dodavatel dodavatel v rámci placené podpory Systému nasazuje nové verze Systému.	Ano
Aktualizace nástroje musí být distribuovány online	Ano
Součástí nabídky je podpora výrobce na 60 měsíců	Ano