Príloha č. 1: Špecifikácia predmetu zákazky

Predmet obstarávania
Predmetom obstarávania je obstaranie komplexného nástroja pre zvýšenie bezpečnosti IT infraštruktúry, ktoré bude zabezpečovať aktívny zber dát z monitorovaných zariadení a aplikácií v reálnom čase so schopnosťou ich analyzovania a identifikácie správania typického pre narušenie bezpečnosti.
Súčasti požadovaného riešenia
Požadované riešenie musí pokrývať a zabezpečiť min. tieto požiadavky ako 1 funkčný celok a všetky subkomponenty, ktoré musia byť minimálne súčasťou riešenia sú tieto: - Centrálne SIEM riešenie - Log kolektor a archivácia dát - Analytický nástroj pre SOC - Správa bezpečnostných informácií a udalostí SIEM/SOC - Softvér pre identifikáciu a riadenie rizík Verejný obstarávateľ požaduje dané súčasti ako 1 ucelené riešenie, ktoré musí spĺňať kritéria definované nižšie.
Podpora
Softvérové licencie riešenia vrátane 3 ročnej údržby a podpory podľa špecifikácie komponentov riešenia.
Technické požiadavky
Licencia musí byť po obstaraní majetkom Obstarávateľa.
Licencia musí umožňovať prevádzku SIEM on-premise alebo on-cloud.
Licencia musí licenčne a výkonovo podporovať spracovanie relatívne neobmedzeného počtu EPS (Events per second) pre 100 virtuálnych serverov (tzv. MVS).
Licencia nesmie byť obmedzovaná počtom zdrojov udalostí (logov).
Licencia nesmie byť licenčne obmedzená počtom používaných korelačných pravidiel, pretože nemožno vopred určiť finálny počet týchto pravidiel.
Licencia nesmie obmedzovať počet existujúcich reportov alebo počet reportov, ktoré je možné vytvoriť.
Licencia musí podporovať pridanie integrovaného manažmentu rizík na základe sieťových tokov a konfiguráciu aktívnych prvkov do GUI formou navýšenia počtu kusov (jednotiek) tej istej licencie.
Podpora a údržba musí zahŕňať upgrade a aktuálne opravné balíky (fixies, patch) na 3 roky.
Riešenie musí licenčne a výkonovo podporovať spracovanie minimálne 4 000 EPS (Events per second) s možnosťou ďalšieho rozšírenia bez nutnosti dokúpenia/navyšovania licencií.
Riešenie musí licenčne a výkonovo podporovať spracovanie minimálne 50 000 Flow (Záznam toku dát) s možnosťou ďalšieho rozšírenia bez nutnosti dokúpenia/ navyšovania licencií.

Riešenie musí mať schopnosť uchovať interne (tzv. Online) aspoň 70 TB dát bez toho, aby riešenie vyžadovalo použitie externých pamäťových zariadení alebo médií.
Podpora a údržba pre riešenie musí zahŕňať upgrade a aktuálne opravné balíky (fixies, patch) a musí byť realizovaná onsite v režime 24x7 s reakčnou dobou pri kritických problémoch 2 hodiny (best effort).
Riešenie musí licenčne podporovať analýzu sieťových údajov v reálnom čase, aby bolo možné odhaľovať stopy a skryté bezpečnostné hrozby v mnohých scenároch predtým, ako môžu poškodiť organizáciu, vrátane phishingových e-mailov, malvéru, exfiltrácie údajov, zneužívania DNS a iných aplikácií atď.
Riešenie musí licenčne podporovať nepretržitý monitoring zaznamenaných „flows“ v sieti, aby bolo možné identifikovať anomálnu prevádzku. Riešenie musí poskytovať vizualizácie podozrivých záznamov, ktoré sa najviac líšia od ostatných záznamov pozorovaných v rámci siete. Musí taktiež podporovať rýchlu identifikáciu flow-ov s podozrivým správaním v sieti a uprednostniť ich vyšetrovanie.
Funkčné požiadavky
Licencia musí poskytovať centrálnu webovú konzolu, z ktorej je možné spravovať celé riešenie.
Ponúkaná Licencia musí poskytovať webové užívateľské rozhranie a toto rozhranie by nemalo obsahovať pluginy alebo byť založené na technológiách Java, Flash alebo na báze tučného klienta.
Licencia musí podporovať prácu s internými prekrývajúcimi sa rozsahmi adries spolu so sieťovými tokmi, udalosťami a zariadeniami v sieti. Toto umožňuje spravovať v jednom riešení aj podriadené organizácie.
Licencia musí umožňovať definíciu užívateľských oprávnení pre možnosť oddelenia prístupu jednotlivých administrátorov k jednotlivým zariadeniam, ich skupinám či sieťovým segmentom.
Licencia musí umožňovať zber udalostí (logov) bez nutnosti inštalovať agenta na cieľový systém.
Licencia musí v prípade potreby umožňovať inštalovať agenta na cieľový systém pre zber udalostí z Microsoft Windows prostredia.
Licencia musí obsahovať vstavaný mechanizmus na klasifikáciu systémov podľa typu do kategórií (identifikáciu zdrojov logov).
Licencia musí umožňovať použitie šifrovanej komunikácie medzi zdrojmi udalostí a riešením.
Licencia musí podporovať agregáciu udalostí z udalostí i podľa položiek, ktoré nie sú zahrnuté v riešení priamo od výrobcu. Teda je možné agregovať pomocou vlastných pridaných položiek.
Licencia musí podporovať zber udalostí z rôznych prostredí ako sú Windows, Linux / Unix / AIX prostredia, bezpečnostných a sieťových systémov, databáz a súborov.
Licencia musí pre zber udalostí podporovať protokoly: Syslog, Windows Events Collection (WinRE / RPC), FTP, SCP, SNMP, ODBC / JDBC, CP-LEA, SDEE, log file.
Licencia musí umožňovať rozšírenie výberov o užívateľské položky z obsahu logov.
Licencia musí podporovať tzv. near-real-time analýzu udalostí, teda v momente príchodu udalosti do riešenia bude udalosť testovaná korelačnými pravidlami.

Licencia musí umožňovať vykonávať analýzu dlhodobých trendov, ktoré vychádza z prichádzajúcich udalostí. Jedná sa o Network Behavior Anomaly Detection funkcionalitu.
Licencia musí podporovať schopnosť monitorovať históriu útokov (typov udalostí) na kritické komponenty.
Licencia musí v prípade využitia monitoringu sieťových tokov podporovať schopnosť korelovať udalosti DHCP, VPN a Active Directory a sledovať priebeh užívateľskej relácie v rámci celej organizácie.
Licencia musí podporovať schopnosť korelovať dáta o udalostiach so statickými a dynamickými zoznamami pre možnosť vytvárať napríklad zoznamy povolených zariadení a naopak.
Licencia musí podporovať funkcionalitu behaviorálnej analýzy užívateľov pre možnosti skúmania správania užívateľov. Táto funkcionalita musí využívať algoritmy strojového učenia a musí byť úzko previazaná so zvyškom systému a spravovať sa z jednotného rozhrania správcovskej konzoly SIEM systému. Systém musí obsahovať aj základné out-of-the-box pravidlá pre funkcionalitu behaviorálnej analýzy používateľov.
Licencia musí podporovať zobrazenie upozornenia vo webovej konzole riešenia a zasielanie upozornení (email, syslog, atď.) administrátorom.
Licencia musí obsahovať zasielanie upozornení na základe detegovanej hrozby, anomálie, porušenie bezpečnostnej politiky a prekročení nastaveného prahu. Tiež musí riešenie zasielať upozornenia a informovať (mať možnosť zaslať upozornenie) pri výpadku zberu udalostí zo zariadenia.
Licencia musí podporovať nastavenie konkrétnej akcie (napr. Zaslať email, notifikáciu alebo spustiť vopred definovaný skript), ktorá bude vykonaná v závislosti na prijaté udalosti či výsledku korelačného pravidlá.
Licencia musí podporovať zreťazenie udalosti do jedného záznamu o incidente, takže ak korelačné testy označí viac činností súvisia s jedným útokom, vygeneruje riešenie iba jeden incident, aby nedošlo k preťaženiu bezpečnostného operačného tímu.
Licencia musí v centrálnej webovej konzole podporovať vykonávať kombinované hľadanie v aj v indexovaných audítorských dátach s použitím regulárnych výrazov a fulltextového vyhľadávania v neštruktúrovanom texte súčasne.
Licencia musí podporovať pokročilé detailné vyhľadávania tzv. Drill-down s možnosťou filtrácie až na úroveň IP adresy, typu udalosti, protokolu, portu atď.
Licencia musí podporovať zrozumiteľný spôsob vyhľadávania s podporou zadaní dotazu s použitím Booleovej logiky alebo pomocou regulárneho výrazu.
Licencia musí podporovať vytvárať vlastné reporty pomocou grafického rozhrania, kde možno vytvárať nové zostavy bez nutnosti zostavovať SQL dotazy.
Licencia musí podporovať riešenie pre nezmenenú funkcionalitu reportingu aj pri zmene alebo náhrade niektoré technológie ako napr. Firewallu alebo IDS.
Licencia musí podporovať riešenie formou distribuovanej architektúry, kedy komponent pre spracovanie a ukladanie udalostí na úložisko bude vo forme HW zariadenia a všetky ostatné komponenty môžu byť umiestnené vo forme virtuálneho zariadenia do virtuálneho prostredia.
Licencia musí podporovať riešenie v možnej kombinácii HW a Virtual alebo iba Cloud.

Licencia musí podporovať pre budúce rozšírenie vzdialený zber logov lokálnym kolektorom s následným preposielaním v komprimovanej podobe a šifrovane v rámci riešenia.
Licencia musí podporovať vykonávať automatické aktualizácie riešenia bez pomoci profesionálnych služieb výrobcu.
Licencia musí podporovať mechanizmus na internú kontrolu stavu komponentov riešenia a upozornenia administrátora v prípade problému.
Licencia musí natívne podporovať budúce rozšírenie o nasadenie v režime vysokej dostupnosti bez nutnosti využitia ďalších softvérov iných ako výrobca alebo riešenia tretích strán.
Licencia musí podporovať ukladanie prichádzajúcich udalostí v štandardizovanom formáte a zároveň aj v originálnom "raw" formáte.
Licencia musí podporovať mechanizmus pre zabezpečenie integrity ukladaných dát.
Licencia musí podporovať mechanizmus pre plánované archivovanie uložených dát na externé úložisko.
Licencia musí obsahovať funkcionalitu automatickej tvorby záloh konfigurácie s následnou možnosťou obnovy.
Licencia musí podporovať integráciu pomocou otvoreného API rozhrania. API môže slúžiť pre strojovú interakciu s riešením alebo pre integráciu s riešeniami tretích strán.
Licencia musí podporovať overenie užívateľov pomocou integrácie s adresárovým systémom Active Directory.
Licencia musí podporovať prácu s reputačnými službami výrobcu alebo s reputačnými službami tretích strán. Reputačné služby poskytujú napríklad IP geolokáciu, botnet kanály atp. Súčasťou riešenia bude licencia pre využitie reputačné služby výrobcu.
Licencia musí podporovať agregáciu záznamov o sieťovej prevádzke z oboch strán dátového toku do jedno záznamu popisujúceho obojsmernú komunikáciu.
Špecifikácia prostredia
Všetky požadované licencie a k ním prislúchajúce softvérové komponenty, ktoré budú tvoriť 1 celok pozostávajúci zo subkonentov: - Centrálne SIEM riešenie - Log kolektor a log archivácia - Analytický nástroj pre SOC - Správa bezpečnostných informácií a udalostí SIEM/SOC - Softvér pre identifikáciu a riadenie rizík Budú inštalované do virtuálneho prostredia zákazníka, ktoré je postavené na platforma VMware vSphere.
Inštalačné a konfiguračné práce
Celé riešenie sa požaduje dodať ako 1 celok vrátane uvedenia do prevádzky, nastavenia zberu dát, archivácie dát. Vytvorenie základných 5tich use case a vrátane zaškolenia personálu.

Parameter	**Minimálna požiadavka obstarávateľa**
Položka	**Ochrana Webu**
Architektúra, prepojiteľnosť a výkon	Riešenie musí podporovať 500 užívateľov Produkt by mal poskytovať rôzne spôsoby implementácie. Mal by exitovať ako fyzické zariadenie, virtuálne zariadenie a softvérové riešenie. Produkt musí byť schopný zvládnuť prenos >850 Mbps HTTP a HTTPS na jednom porte. Produkt musí byť schopný zvládnuť viacero bodov konektivity, hlavný/zálohový pre centrálu a konektivitu vo veľkých pobočkách Riešenie musí podporovať mobilné bezpečnostné schopnosti umožňujúce ochranu užívateľov, keď sa nachádzajú mimo hlavnej siete Užívatelia mimo hlavnej siete sa musia riadiť rovnakými pravidlami ako keby sa nachádzali v rámci nej. Architektúra by mala poskytovať schopnosti riadiť a kontrolovať využitie šírky pásma na zabezpečenie dostupnosti pásma pre kritické aplikácie alebo protokoly Produkt by malo byť možné inštalovať na vlastný hardware ako software bez potreby hardware alebo virtuálnej appliance Fyzicky appliance musí poskytovať možnosť optickej konektivity V prípade zlyhania všetkých proxy umiestnených on-premise by mal produkt previezť automaticky fall-back do cloudovej prevádzky bez obmedzenia služby Riešenie musí mať možnosť tunelovania prevádzky na firemný cloud aplikácie (minimálne O365 a Google Suite) s možnosťou autentizcie až v cloudovej službe (authentication bypass) Produkt by mal obsahovať klientský software pre vynútenie konektivity do webu cez cloud proxy Produkt by mal obsahovať klientstký software pre vynútenie kontroly a blokovanie prenášaného obsahu v cloud riešeniu dodávateľa, ale s priamym prístupom na cieľový server (cieľový server je kontaktovaný priamo bez proxy)

Manažment	Riešenie musí byť spravované z jednej spoločnej webovej konzoly/dashboard-u pre WEB/Email a DLP Management systém musí poskytovať schopnosti monitorovať užívateľov v reálnom čase, zahrnúť informácie o užívateľskej identite a detaily o cieľovej URL adrese Management systém musí poskytovať zobrazenie všetkých konfiguračných nastavení v jednom okne alebo tabe pre zníženie zaťaženia administratívnymi prácami Riešenie musí podporovať viacero role-based administratívnych kônt, ktoré poskytujú granulárnu kontrolu a obmedzenia Riešenie musí podporovať centralizovanú správu a reporting naprieč viacerými lokalitami vrátane vzdialených užívateľov, ktorí nie sú lokalizovaní na žiadnej internej sieti Riešenie bude podporovať administratívne role umožňujúce jednotlivcom alebo skupinám prístup k výhradne len k reportingovým údajom pre určených užívateľov alebo skupiny
Reporting	Riešenie musí poskytnúť preddefinované reporty pre reporting užívateľov, skupín alebo lokalít o správaní, vývoji atď. Riešenie musí umožniť spárovanie zaznamenanej prevencie hrozieb, kontroly obsahu webu a aktivity na prevenciu úniku údajov, s IP adresou, užívateľským menom a kategóriou navštívenej webovej stránky Riešenie musí poskytovať detailné informácie o aktivite užívateľa vrátane logovania celej URL a zobraziť primárnu lokalitu a akékoľvek prepojené stránky Riešenie musí podporovať anonymné reportovanie správania sa a aktivít a odstrániť alebo zamaskovať citlivé osobné informácie Produkt musí podporovať zobrazenie prenosu v reálnom čase pre okamžité riešenie problémov

	Riešenie musí vedieť zobraziť informáciu o browseroch a operačných systémoch používaných pri browsovaní. Report by mal obsahovať pomerné zastúpenie OS a typu browseru a ich celkovej hodnoty najmenej za posledných 30 dní. Riešenie musí poskytovať prehľad o využívaných cloud aplikáciách. Informácia musí byť definovaná podľa špecifického názvu aplikácie, nie len podľa kategórie. Súčasťou musí byť aj katalóg cloud aplikácií s informáciami o type potencionálnych hrozbách danej cloud aplikácii Riešenie musí mať reporting vstavaný do management serveru bez nutnosti inštalovať software tretej strany Produkt musí zobraziť informáciu o historii prehliadania stránok pre daného užívateľa bez ohľadu na to, či prechádzal cez on-premise proxy alebo cloud proxy. Produkt môže ukladať ľubovolne dlhé obdobie všetkých logovaných udalostí s možnosťou okamžitého prístupu s dátami z rozhrania reportingu

Správa hrozieb	Riešenie musí zahŕňať vopred zostavený zoznam URL a webových stránok, o ktorých sa vie, že sú ohrozené alebo infikované. Riešenie musí identifikovať a zablokovať známy škodlivý softvér bez ohľadu na vstupný sieťový port. Riešenie musí odhaliť a zablokovať odchádzajúcu škodlivú Botnet a Trojan komunikáciu pochádzajúcu z infikovaných systémov. Systém musí zaznamenať a poskytnúť detailné informácie o pôvodnom systéme, dostatočné k úspešnej identifikácii infikovaného systému. Riešenie musí byť schopné skontrolovať v SSL kódovanom prenose malware a iné hrozby. Opíšte aká metóda sa používa na prerušenie SSL komunikácie. Riešenie musí chrániť pred známymi spustiteľnými súbormi v binárnej forme, script based exploitmy a maskovaným kódom alebo skriptami prichádzajúcimi do siete. Riešenie musí byť schopné zablokovať zoznam Uniform Resource Locators (URLs) stránok prepojených na stránky infikované škodlivým kódom. (Aj keď stránka sama o sebe nie je infikovaná). Riešenie musí byť schopné dynamicky blokovať legitímnu webovú stránku, ktorá sa nainfikovala a odblokovať dočasné obmedzenie stránky, keď sa hrozba odstráni nezávisle na zabudovanej databáze URL. Toto musí platiť aj pre prenos SSL. Riešenie musí mať možnosť blokovať prístup k špecifickej cloud aplikácii (podľa názvu) podľa vstavaného katalógu aplikácií - počet katalogizovaných aplikácií by mal byť väčší než 5000 Riešenie musí obsahovať katalóg cloud aplikáciu podľa ich rizikovosti definovanej výrobcom Produkt musí mať možnosť odosielať súbory na analýzu do sandboxingu pre analýzu pokročilých hrozieb volitelne on-premise alebo do cloudu

Kontrola obsahu webu	Riešenie má zahŕňať vopred zostavený zoznam URL Vstavaná URL databáza by mala obsahovať najmenej 130 rôznych kategórií Riešenie má byť schopné skontrolovat SSL komunikáciu v súvislosti s porušeniami politiky Riešenie musí byť schopné klasifikovať webové stránky a prvky dynamicky, aby umožnilo presadenie politiky na webových stránkach, ktoré nie sú zahrnuté v databáze URL. Riešenie má byť schopné prepísať kategóriu uvedenú v databáze URL aktualizovanou kategóriou určenou dynamickou klasifikáciou na zabezpečenie príslušného presadenia politiky. Riešenie je schopné poskytnúť špecifické kontroly aplikácie rôznym spoločným protokolom a aplikáciám používaným ako vektory hrozby. Prosím poskytnite zoznam protokolov a aplikácií. Riešenie by malo byť schopné identifikovať a zablokovať špecifické aplikácie bez ohľadu na použitý port TCP
Filtrovanie obsahu - DLP	Produkt musí poskytovať DLP skenovanie obsahu ako natívnu funkciu Citlivý obsah nesmie byť skenovaný mimo zariadenia Produkt musí poskytovať klasifikáciu dokumentov/súborov Riešenie musí umožniť skontrolovať obsah súborov pri odosielaní vo formáte obrázku pre analýzu DLP. Musí byť schopné čítať text v .pdf aj keď nie je v textovom formáte
Licencovanie	Produkt musí byť licencovaný na počet chránených užívateľov Pri dočasnom / chvíľkovom prekročení licencií nie je užívateľská prevádzka blokovaná a administrátori sú na fakt upozornení Je licencovaný pre použitie on-premise rovnako ako v hybrid/cloude Je možné kedykoľvek prechod z licencie on-premise do cloudu bez ďalších licenčných nákladov Licencie na virtuálne appliances sú v cene užívateľskej licencie Licenciou sa myslí subskripčný model s prístupom k update počas platnosti subskripcie **na dobu 3 roky**