Príloha č. 1

Špecifikácia predmetu zákazky:

Všeobecné požiadavky:
- Centrálny samostatne fungujúci bezpečnostný DNS prekladač:
- bez nutnosti zásahu do konfigurácie na koncových zariadeniach,
- bez nutnosti inštalácie certifikátov alebo iného software do koncových zariadení
- bez úprav bezpečnostných politík AD

Riešenie poskytujúce ochranu na úrovni DNS voči:
- Malware
- Zero – Day detection of Domain generation algorithm
- Phishing
- Homograph phishing attack´s
- Exploits
- Spam domains
- Malicious coinmining
- DNS Tunneling
- Cache poisoning
- DNS rebinding attacks
- DNS anomaly detection & alerting

Parametre na security filtering engine
- Má nulovú dodatočnú latenciu pre používateľa. Security vyhodnocovanie je dodávané v reálnom čase bez over-the-network dotazov
- Schopnosť fungovať vo virtuálnom prostredí vSphere 6.7+
- Ochrana voči DNS spoofing útokom založeným na DNSSEC zahŕňajúc NSEC3 podporu a negatívny caching
- Možnosť definovať rozdielne security politiky a priradené sieťam založeným na CIDR
- Detekcia Zero-day hrozieb bez nutnosti predchádzajúcej znalosti danej domény
- Detekcia a alerting anomálií v rámci DNS frafficu
- Možnosť alertovať / blokovať z vnútornej siete prístup k doménam podobne vyzerajúcim ako definovaná doména spoločnosti pre ochranu pri cielených phishingových útokoch
- Možnosť blokovať prístup k doménám podľa kategórie obsahu, aspoň v rozsahu:
- Coinminers
- Hazard
- Násilie
- Tracking
- Reklama
- Sociálne siete
- Hry

Systém umožňuje flexibilne upraviť pre skupiny zariadení:
- Úroveň ochrany
- Úroveň detekcie
- Kategórie hrozieb sú zahrnuté v konkrétnych politikách
- Vlastné blacklisty a whitelisty
- Blokované kategorie obsahu

Funkcie a komponenty
On-premise resolver:

- Plne autonómny DNS resolver so security vrstvou, teda vykonáva samotný resolving a filtering, bez potreby komunikácie s externou službou v cloude
- Security vrstva umožňuje presmerovanie požiadaviek na závadné domény na blokačnú stránku
- Blokačná stránka
• Je webová stránka kam je používateľ presmerovaný keď sa on alebo jeho zariadenie snažilo pristúpiť na závadnú webovú stránku
• Blokačnú stránku je možné akokoľvek upraviť podľa želania objednávateľa
• Funkcia "Bypass" pre definované siete – používateľ môže pokračovať na cieľovoú doménu bez nutnosti spolupráce administrátora (napr. pre guest siete)
- Spĺňajúci RFC štandardy
- Podporujúci DNSSEC validation vrátane NSEC3 negative caching
- Konfiguračné zmeny a update resolverov sa vykonávajú za plnej prevádzky – bez DNS traffic výpadku počas updatov a rekonfigurácií
- DNS traffic management a firewalling
• Konkrétne zóny môžu byť presmerované na vybrané IP adresy
• DNS cache prefetching – záznamy v medzipamäti sú obnovené predtým než expirujú
• DNS záznamy sú držané v pamäti dlhšie, než by kvôli ttl perióde mali byť autoritatívne nameservers pre zónu nedostupné (e.g. domain.com je nedostupná počas jednej hodiny, resolver bude schopný použiť poslednú odpoveď, ktorú mal pre túto doménu).
• DNS Firewall – možnosť definovať pravidlá prístupu na konkrétne domény – povolenie prístupu iba na vybrané domény per IP subnet.
Príklad použitia – povolenie prístupu pre klientské stroje iba na domény Office 365, na ostatné vrátiť odpoveď NXDOMAIN.
• Automatická aktualizácia zoznamu domén Office 365 a ďalších služieb Microsoft Azure použitých v DNS firewalle
- Podporujúce využitie DNS over TLS a DNS over HTTPS

Centrálny management:
- Zobrazuje kompletný DNS traffic v reálnom čase
- Poskytuje a vykonáva:
• Update databázy pre security filtering,
• Manažment resolvera a softwarových updatov
• Centrálne úložisko logov a incidentov a poskytuje možnosti pre ich vyhodnocovanie

- DNS Traffic log vrátane detailov o všetkých unikátnych požiadavkách / odpovediach pre ďalšiu analýzu sú prístupné a exportované zo všetkých resolverov v spoločnosti a dostupné vrátane fulltextového filtrovania v jednom rozhraní (napr. v csv formáte)
- Možnosť analyzovať doménu z pohľadu bezpečnosti a obsahu vrátane integrácie na bezpečnostné služby tretích strán
- Alerting upozorňujúci na anomálie detekované v rámci DNS Trafficu
- Alerting a reporting doručovaný pomocou:
• Email
• Syslog (TLS)
• Slack
• RESP API
- DNS traffic overview umožňuje komplexnú analýzu DNS komunikácie vrátane detailného:
• drilldown jednotlivých udalostí
• filtrovania,
• exportu dát,
• prehľadu trendov

- Lokalizovaný v jazykoch:
• Slovensky,
• anglicky,
• možnosť doplniť ďalšie jazyky.

Administrátorské rozhranie:
- Webové rozhranie pre administrátora je plne prístupné cez moderné webové prehliadače bez potreby doinštalovania add-ons alebo lokálneho software potrebného pre prístup do rozhrania
- Možnosť aktivácie dvojfaktorovej autentizácie a vynútenie dvojfaktorovej autentizácie pre všetkých administrátorov v organizácii
- Dostupnosť nápovedy a dokumentácie
- Rozdielne nastavenie oprávnení (pre jednotlivé skupiny) dostupné pre operátorov najmenej v 2 roliach:
- Administrátor,
- Používateľ s právami na čítanie,

- DNS traffic log z všetkých resolverov je dostupný vrátanie fulltextového fitrovania v jednotnom rozhraní
- Detaily o všetkých unikátnych požiadavkách/odpovedia budú prístupné a exportované pre ďalšiu analýzu v csv formáte

- Detaily o všetkých unikátnych požiadavkách/odpovedia budú prístupné a exportované
- Administrátorské webové rozhranie poskytuje prístup do všetkých funkcií:
• Threat analysis
• DNS traffic analysis
• Security filtering configuration
• DNS resolver management
• Alerting
• Možnosť vytvorenia vlastných whitelistov a blacklistov

DNS resolver management poskytuje:
- Vzdialenú diagnostiku:
• Monitorovanie hardwarových problémov
• Softwarový monitoring
• Zbieranie logov
• Vyhodnocovanie latencie prekladu

Upozorňovanie:
- Konfigurovateľné filtre pre domény, siete, akcie
- Početné možnosti doručenia a protokoly pre doručenie alertov, ktoré zahŕňajú:
• Email
• Syslog (TLS)
• Slack
• Webhook (REST API)
• Možnosť doprogramovania ďalších cieľových miest doručenia alertov

- Upozorňovanie je založené na
• Thresholdoch security udalostí a DNS traffic
• Detekcii dynamických anomálií
• Whitelistoch a blacklistoch

Reporting:
- Reporty sú odosielané zo systému prostredníctvom emailu
- Priebežné reporty sumarizujú
• Objemy prevadzky
• Množstvo hrozieb podľa jednotlivých kategórií
• Podozrivé a nakazené klientské zariadenia
• Prevládajúce rodiny škodlivého kódu a závadných domén

Čas dodania:
- objednanú technológiu je možné dodať do 72 hodín od zaslania záväznej objednávky, resp. podpísania zmluvy

Implementácia riešenia:
- riešenie bude nainštalované, nakonfigurované podľa individuálnych požiadavaiek dodávateľa do existujúcej sieťovej infraštruktúry bez výpadku alebo odstávky prevádzky
- dodávateľ zaškolí administrátorov objednávateľa v rozsahu 4 hodín
- integrácia s technológiami ako: MS AD, SIEM, Log manager, Prevádzkový monitoring, Flowmon ADS

Rozsah podpory:
- Vzdialená podpora výrobcu (mail, telefonicky, ticketovacím nástrojom) v lokálnom jazyku: slovensky/anglicky (podľa preferencií objednávateľa)
- Schopnosť poskytnúť podporu na mieste do 4 pracovných hodín v prípade kritických problémov od nahlásenia (po uzatvorení SLA zmluvy)

Dokumentácia:
- Technická dokumentácia k riešeniu je lokalizovaná do jazykov:
• Slovensky
• Anglicky