Technológia DNS resolvera poskytujúceho preklad externých domén s bezpečnostnými modulmi.

Všeobecné požiadavky na riešenie dodané v skúšobnom nasadení:

- Nevyžaduje modifikáciu na koncovej stanici:
    - Bez potreby inštalácie SW na koncovej stanici
    - Bez potreby manuálnej rekonfigurácie, všetko musí byť vykonávané automaticky
    - Bez potreby inštalácie certifikátov alebo prenastavenia bezpečnostných politík
-

Riešenie má poskytnúť ochranu na úrovni DNS voči:

- Malware
- Zero – Day detection of Domain generation algorithm
- Phishing
- Homograph phishing attack´s
- C&C
- Exploits
- Spam domains
- Malicious coinmining
- DNS Tunneling
- Cache poisoning
- DNS rebinding attacks
- DNS anomaly detection & alerting

Parametre na security filtering engine

- Má mať nulovú latenciu pre používateľa. Security vyhodnocovanie je dodávané v reálnom čase bez over-the-network dotazov
- Nasadenie software bez potreby nasadenia na špeciálne upravený hardware. Schopnosť fungovať vo virtuálnom prostredí
- 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
    - Tracking
    - Reklama
    - P2P connection (torrent, ..)
    - DNS over HTTPS
    - Pornografia
    - Hazard
    - Násilie
    - Drogy
    - Terorizmus

- Zneužívanie detí
- Sociálne siete
- Hry
- Chat
- Audio/video

- Má zabezpešiť ochranu proti zneužitiu DNS prevádzky pre tunelovanie inej komunikácie v technicky validných DNS paketoch a komunikáciu s externými servermi (DNS Tunneling zabezpečenie)
- DNS tunneling vrstva proaktívne rozbíja DNS tunneling na viacerých úrovniach:
  - resolver,
  - neurónová sieť

- Politiky umožňujú administrátorom upraviť:

  - Úroveň ochrany

  - Úroveň detekcie

  - Kategórie hrozieb sú zahrnuté v konkrétnych politikách

  - Vlastné blacklisty a whitelisty

  - Blokované kategorie obsahu

Požadované funkcie a komponenty

Požiadavky na 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

Požiadavky na centrálny management:

- Zobrazuje kompletný DNS traffic v reálnom čase
- Poskytuje a vykonáva:
    - Update databázy per 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

- Zobrazuje kompletný prehľad o obsahovej blokácií v reálnom čase podľa vyššie pomínaných kategórií obsahu vrátane detailného:
    - drilldown jednotlivých udalostí
    - filtrovania,
    - exportu dát,
    - prehľadu trendov

- Lokalizovaný v jazykoch:
    - Slovensky / Česky,

- anglicky,
- ďalšie podľa požiadavky

Požiadavky na 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 v lokálnom jazyku (česky/slovensky)
- 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

- 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

- Lokalizované v jazykoch:
    - Česky / Slovensky
    - Anglicky,

DNS resolver management poskytuje:

- Vzdialenú diagnostiku:
    - Monitorovanie hardwarových problémov
    - Softwarový monitoring
    - Zbieranie logov
    - Vyhodnocovanie latencie prekladu

- Softwarové updates a rollbacks:
    - Možnosť okamžite vykonať rollback akéhokoľvek update do predchádzajúceho stavu
- Lokálny management
    - Plný prístup k logom pre lokálnych administrátorov
    - Lokálne CLI

Požiadavky na funkcie alertingu:

- Konfigurovateľné filtre pre domény, siete, akcie
- Početné možnosti doručenia a protokoly pre doručenie alertov, ktoré zahŕňajú:
    - Email
    - Syslog (TLS)
    - Slack
    - Webhook (REST API)
    - Dodatočné cieľové miesta doručenia alertov (na požiadanie)

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

Reporting:

- Reporty sú dodávane pomocou emailu
- Priebežné reporty sumarizujú
    - Objemy prevadzky
    - Množstvo hrozieb podľa jednotlivých kategórií
    - Podozrivé a nakazené klientské zariadenia
    - Prevládajúce rodiny škodlivého kódu a závadných domén

Požiadavky na integračné procesy:

- Dostupnosť REST API pre získanie informácií
    - Detaily o udalostiach a hrozbach
    - Štatistiky DNS prevadzky
    - REST API parametre pre filtrovanie založené na:
        - Zdrojovej IP adrese
        - Destination domain
        - Type požiadavky
        - Type hrozby
        - IP adrese odpovede
        - Čas

- Syslog integrácia (SIEM, log management, prevádzkový monitoring, a pod.)
    - Konfigurovateľný tok dát cez syslog obsahujúci detekované hrozby
    - Konfigurovateľný tok dát cez syslog obsahujúci DNS prevadzku

Požiadavky na tenkého agenta pre laptopy a mobilné zariadenia:

- pomocou tenkého agenta musí dodávaná technológia chrániť mobilné koncové zariadenia s OS Windows mimo doménu (internú sieť) rovnako ako on-premise resolver v doméne (internej sieti)
- pomocou tenkého agenta musí dodávaná technológia chrániť mobilné koncové zariadenia s operačným systémom iOS a s operačným systémom Android mimo doménu (internú sieť) rovnako ako on-premise resolver v doméne (internej sieti)

Požiadavky na dodávanú technológiu:

- objednanú technológiu je možné dodať a sprevádzkovať naprieč celou spoločnosťou do 48 hodín od zaslania záväznej objednávky, resp. podpísania zmluvy pre pre on-premise resolver
- objednanú technológiu je možné dodať a sprevádzkovať (pre 10 ks laptopov a 10ks mobilných zariadení) do 5 pracovných dní od zaslania záväznej objednávky, resp. podpísania zmluvy

Implementácia riešenia:

- technológia je aktuálne v spoločnosti nainštalovaná a zapojená do sieťovej infraštruktúry
- integrácia možná s technológiami ako: MS AD, SIEM, Log manager, Prevádzkový monitoring, Flowmon ADS,

Rozsah podpory:

- Vzdialená podpora výrobcu (mail, telefonicky, ticketovacím nástrojom) v lokálnom jazyku: česky / slovensky a anglicky (podľa preferencií objednávateľa, najmä pri komunikácií s výrobcami iných technológií nasadeních v prostedí spoločnosti)
- 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:
    - Česky / Slovensky
    - Anglicky
    - Podľa požiadavky