## Příloha č. 1 – Technická specifikace

### Technická specifikace

### „DODÁVKA A IMPLEMENTACE ŘEŠENÍ PRO AUTOMATIZOVANOU DETEKCI A REAKCI NA BEZPEČNOSTNÍ INCIDENTY V SÍTI“

## Specifikace plnění

Předmětem plnění je dodávka řešení (Systém) monitorování pokročilé IT bezpečnosti, které bude nástrojem pro bezpečnostní specialisty a IT specialisty Zadavatele. Řešení umožní získat informace a vizibilitu o dění v počítačové síti s cílem detekce, identifikace a zamezení pokročilých kybernetických útoků označovaných jako APT (Advanced Persistent Threat) v rámci chráněného prostředí.

Řešení poskytne tyto funkcionality:

- Detekce a ochrana proti sofistikovaným útokům obvykle označovaným jako APT;
- Detekce a ochrana proti průniku malware na síti i na stanicích;
- Řešení musí zaznamenávat informace o síťové komunikaci v podobě meta-dat, a to po dobu 60 kalendářních dnů. Na základě těchto meta-dat pak provádět bezpečnostní analýzu;
- Funkce síťového DLP (Data Loss Prevention) pro detekci a zamezení úniku dat.

Systém musí poskytovat jednotné uživatelské webové rozhraní pro práci specialistů s dodávaným řešením (tedy pro síťovou část). Současně řešení musí umožnit integraci se stávajícím řešením ochrany koncových stanic. Tato integrace musí zajistit využití automatizačních funkcí, korelaci dat mezi síťovým provozem a aktivitami na koncových zařízeních a automatizovanou validaci incidentů.

Rozhraní musí umožnit rychlé zkoumání události, dostupností kontextu události v podobě záznamů o relevantním síťovém provozu a dalších souvisejících událostech/alertech – jak typově (stejný typ události/alertu), tak z hlediska stejných IP adres apod.

Plnění bude obsahovat:

1) Dodávka technologie;
2) Podpora výrobce (maintenance) včetně zajištění záruky výrobce na 2 roky;
3) Implementační práce včetně plné integrace dodávaného řešení s implementovaným řešením ochrany koncových stanic a logmanagerem včetně dokumentace skutečného provedení díla.
4) Zaškolení administrátorů Objednatele – Zaškolení administrátorů v potřebném rozsahu pro plnou správu a administraci Systému na úrovni „administrátor“, v sídle Objednatele. Minimální rozsah školení je jeden den.

Realizace bude rozdělena do několika částí. Mezi jednotlivými částmi vždy proběhnou dílčí akceptační testy. Projekt bude řídit projektový tým Dodavatele a Objednatele.

a) Část 1 - Analýza stavu infrastruktury Objednatele

- Analýza stávající infrastruktury a koncových zařízení Objednatele;
- Vypracování technicko-realizačního dokumentu, včetně časového harmonogramu;
- Návrh akceptačních testů pokrývajících testování funkčních požadavků na Systém ze strany Objednatele, včetně testování vybraných výkonových parametrů.

Všechny požadované výstupy Analýzy budou Objednateli předloženy k odsouhlasení. Pokud Objednatel shledá nesoulad nebo nejasnosti navrhovaného řešení oproti této technické specifikaci a svým požadavkům, provede Dodavatel nápravu. Teprve po akceptaci bez výhrad všech požadovaných výstupů Objednatelem je Analýza považována za ukončenou a Dodavatel tak může pokračovat v realizaci dodávky dle časového harmonogramu.

b) Část 2 – Dodávka SW a všech potřebných licencí a zajištění Záruky výrobce

- Dodání veškerého souvisejícího SW;
- Zajištění Záruky výrobce na veškerý SW a poskytovaní záručního servisu v rámci Záruky za jakost v délce 2 let od řádného ukončení Části 2 Předmětu plnění.

c) Část 3 – Příprava Systému, instalace Systému do vybraného síťového segmentu pro ověření funkcionality, monitorovací mód.

- „Pilotní" instalace Systému do vybraného síťového segmentu Objednatele pro otestování navržené funkcionality. Objednatel společně s Dodavatelem provede testy funkcionalit;
- Propojení na stávající síťové služby Objednatele;
- Otestování funkcí Systému na vybraném síťovém segmentu Objednatele v monitorovacím módu;
- Otestování funkcí Systému na vybraném síťovém segmentu Objednatele v monitorovacím módu;

d) Část 4 – Plné nasazení Systému do síťové infrastruktury Objednatele;

- Finální distribuce Systému na síťové segmenty Objednatele a otestování funkcionalit.
- Integrace Systému se implementovaným řešením ochrany koncových stanic a logmanagerem Objednatele.

e) Část 5 – Akceptační testy, dokumentace a školení

- Provedení Akceptačních testů a spuštění 1 měsíčního testovacího provozu Systému – plné nasazení všech jeho funkcionalit;
- Finální akceptační testy Systému;
- Vypracování a předání kompletní dokumentace k Systému (dokumentace skutečného provedení), návodů a postupů;
- Zaškolení administrátorů Objednatele – Zaškolení administrátorů v potřebném rozsahu pro plnou správu a administraci Systému na úrovni „administrátor", v sídle Objednatele.

## Technické požadavky na požadované řešení

Systém musí poskytovat funkcionality umožňující automatizaci mnoha kroků a procesů v rámci vyšetřování a Incident Response s cílem snížit zatížení specialistů. Uchazeč popíše oblasti procesu

vyšetřování a IR, které je možné pokrýt automatizací (samostatně nebo integrací se současnou ochranou koncových stanic, která je u Zadavatele implementována).

Minimálně je požadováno pokrytí těchto oblastí:

- Systém musí pomoci bezpečnostnímu specialistovi s rutinní činností. Například v případě rozpoznání incidentu na síti musí připravit podklady pro další analýzu sběrem určených informací z dotčených koncových bodů (preferováno je řešení, které provede automatizovaně).
- Dodaný systém umožní provádět automatickou validaci projevů hrozeb detekovaných na síti rozpoznáním jejich projevů na stanicích (prostřednictvím jejich vzájemné integrace), případně bude modifikovat důležitosti alertu dle výsledku této automatické validace.
- Umožní provádět další šetření pomocí vzdáleného přístupu k dotčenému bodu s cílem detekce, izolace, analýzy a odstranění škod.
- Monitorování datových linek s celkovou propustností 500 Mbps. Zadavatel zajistí zrcadlení odpovídajícího provozu na portu přepínače.
- Minimální počet rozhraní pro monitorování je požadován v počtu 4 síťových rozhraní.
- Monitoring bude probíhat ve dvou lokalitách a to v primárním DC zadavatele a v záložním DC.
- Požadovaná retence kompletních meta-dat o síťovém provozu je 60 dní.
- Požadovaná integrace se zadavatelem provozovaným prostředím LogManagement.
- Požadovaná integrace se zadavatelem provozovaným řešením ochrany koncových stanic.
- Dodaný systém musí podporovat jednu z následujících virtualizačních platforem (Vmware ESX 6.x nebo Microsoft HyperV )
- Dodavatel řešení v rámci nabídky uvede požadavky na virtualizační platformu v následujících parametrech:
    - Platforma: Vmware / HyperV;
    - Počet požadovaných serverů;
    - Požadavky na zajištění kapacity pro každý server v parametrech:
        - Požadovaný počet virtuálních procesů/core;
        - Požadovaná Velikost operační paměti;
        - Požadovaná velikost diskové kapacita;
        - Počet virtuálních a fyzických rozhraní.

Tabulka požadavků na dodávané řešení:

| Parametr | Požadovaná hodnota (pro jedno fyzické zařízení) | Nabízená hodnota (Popis) |
|---|---|---|
| Analýza síťového provozu | Analýza síťového provozu probíhá pro veškerý síťový provoz a bez ohledu na použité komunikační protokoly. Monitorována jsou tedy všechna probíhající spojení na všech síťových portech. | Nativní funkce produktu |
| Analýza síťového provozu | Funkcionalita analýzy a záznamu síťového provozu pracuje nad zrcadleným provozem, který Zadavatel poskytne na vyhrazeném portu přepínače. | Nativní funkce produktu |
| Analýza síťového provozu | Pravidla pro analýzu provozu umožní definovat podmínky odkazující se na přenášený obsah a parametry aplikační vrstvy - například odhalit přenášené soubory, kde koncovky soborů nesouhlasí s obsahem, nebo čísla typických portů TCP a UDP nesouhlasících s typem rozpoznaného komunikačního protokolu. | Ano, nastavení pravidel je velmi granulární a pomocí logických operátorů lze tvořit složité kombinace |
| Analýza síťového provozu | Podpora monitorování provozu na rozhraních Ethernet s rychlostmi 100Mbps, 1Gbps a 10Gbps pro budoucí rozšiřování systému pro monitorování provozu vnitřní sítě. | Sizing řešení je možný i pro desítky Gbps |
| Analýza síťového provozu | Je možné definovat pravidla hledající souběh událostí nebo posloupnost událostí v síťovém provozu a generovat upozornění (alerty) a to kontinuální analýzou okamžitého dění i analýzou již uložených historických záznamů o provozu zpětně. | Produkt disponuje funkcionalitou tzv. Analytics rules, která požadavek plně naplňuje |
| Analýza síťového provozu | Systém poskytuje webové uživatelské rozhraní pro analýzu zaznamenaného provozu bezpečnostními specialisty, které bude součástí jednotného uživatelského rozhraní. | Nativní funkce produktu |
| Analýza síťového provozu | K dispozici jsou historické informace o provozu s určenou dobou retence pro následnou analýzu. | Nativní funkce produktu |
| DLP funkcionalita | Funkcionalita DLP pro data in motion není závislá výhradně na použití SMTP nebo HTTP proxy, ale je možné ji realizovat jiným transparentním způsobem nezávislým na komunikačním protokolu. | Jsou analyzovány datové toky tak jak protékají bodem s nastaveným SPAN portem a tedy není třeba dalších technologií ke kompletní analýze nešifrovaného provozu |
| DLP funkcionalita | Funkcionalita DLP je schopná odhalit obsah přenášený jako součást souborových archivů (ZIP, RAR, TAR, GZIP, ...) a obsah detekovat v dokumentech typu MS Word, MS Excel, MS PowerPoint, OASIS dokumentech, PDF a dalších běžných kancelářských formátech) – bez omezení hloubky vnoření. | Nativní funkce produktu |

| | | |
|---|---|---|
| DLP funkcionalita | Funkcionalita DLP je schopna odhalit obsah v dokumentech vložených (embedovaných) do jiných formátů (Excel jako objekt ve Wordu, JavaScript jako objekt v PDF, ZIP jako objekt v PowerPoint) bez ohledu na počet a hloubku vložení. | Nativní funkce produktu |
| DLP funkcionalita | Politiky pro DLP lze doplňovat o nová pravidla s odkazem na parametry komunikačního kanálu (například síla šifrování, typ protokolu), lokaci cíle a zdroje dokumentu (IP adresy, příslušnost odesilatele emailu k určitému oddělení Zadavatele, země dle geolokace cílové adresy) a obsahu (klíčová slova, regex, otisky dokumentů, části dokumentů, rozpoznání naučených obrázků). | Nativní funkce produktu |
| Oblast detekce malware | Detekce malware je prováděna pomocí vyhledávání signatur, detekcí typického chování (behavioral analýza) a detekce jeho virtuálním provedením. | Nativní funkce produktu |
| Oblast detekce malware | Retrospektivní detekce pomocí aktuálního threat-intel (detekce průniku proběhlého v minulosti s využitím aktuálního threat-intel) | Nativní funkce produktu |
| Oblast detekce malware | Součástí dodávky je kontinuální služba aktualizace signatur/definice chování malware/aktualizace pravidel sandboxu z komerčního zdroje. | Požadované je součástí, zároveň produkt umožňuje napojení vlastních či jiných externích zdrojů. |
| Oblast detekce malware | Obdobně jako pro DLP je systém schopný malware detekovat i skrytý hluboko v přenášeném obsahu – bez omezení hloubky vnoření. | Nativní funkce produktu |
| Detekce a ochrana proti APT | Viditelnost všech fází APT útoku (dle fází kill-chain – od iniciální kompromitace do ex-filtraci dat). | Nativní funkce produktu, navíc je v prooduktu zavedeno mapování na MITRE ATT&CK |
| Detekce a ochrana proti APT | Možnost zobrazení všech relevantních síťových aktivit a událostí při vyšetřováni určitého incidentu pomocí vyhledávání v událostech a vyhledávání v záznamech o síťových aktivitách. | Nativní funkce produktu |
| Detekce a ochrana proti APT | Síťové aktivity vztahující se k jednomu koncovému bodu bude systém schopen zobrazit v jedné obrazovce uživatelského rozhraní dle nastavených filtrů z hlediska času, síťového protokolu, čísla portu nebo portů, IP adres nebo rozsahů, dle hash nebo jména přenášeného souboru, emailových adres a subjektu zprávy pro emaily, apod. | Nativní funkce produktu |
| Reporting | Schopnost vygenerovat report (ideálně v podobě PDF dokumentu) a tento s danou periodicitou odesílat na emailové adresy. | Nativní funkce produktu |
| Reporting | Řešení nabízí předpřipravenou sadu typických reportů s možností jejich úpravy. | Nativní funkce produktu |
| Reporting | Vlastní report bude možné definovat v editoru šablon reportů. | Nativní funkce produktu |

| | | |
|---|---|---|
| Podpora vyšetřování | Systém umožní realizovat alespoň základní workflow pro práci se zaznamenanými alerty (stav, přiřazení řešiteli, historie činností). | Nativní funkce produktu |
| Otevřenost platformy | Dokumentované aplikační rozhraní pro zákaznické integrace s dalšími bezpečnostními komponentami. Preferujeme http & XML nebo JSON API rozhraní. | Nativní funkce produktu |
| Otevřenost platformy | Předpřipravené integrační vazby na aplikace typu SIEM. | Jsou předpřipraveny obousměrné integrační vazby pro několik značek SIEM řešení |
| Integrace | Systém musí podporovat provoz v hierarchickém režimu pro případné budoucí zahrnutí nadřízených či podřízených subjektů do bezpečnostního dohledu. | Nativní funkce produktu |
| Reporting | Možnost zaznamenávat statistiky provozu řešení a incidentů, vytvářet exportovatelné výstupy včetně grafů.<br>Možnost posílání logu na externí úložiště minimálně ve formátu syslog. | Nativní funkce produktu |
| Nasazení systému | Řešení musí být implementováno a plně funkčně (tedy i s provedenou integrací dodané endpoint ochrany) v prostředí Zadavatele nejpozději do 2 měsíců od podpisu smlouvy. | Zadaný časový rámec , pro kompletní implementaci nabízeného řešení, plně postačuje |
| Práce s řešením | Systém bude implementovat granulární RBAC definující práva uživatelů vůči systému.<br>Oddělení přístupových oprávnění pro různé skupiny operátorů za účelem zamezení přístupů k citlivým informacím, nebo do kontextů dat jiného vyšetřovatele. | Nativní funkce produktu |