PŘÍLOHA Č. 1

Technická specifikace

„Dodávka, implementace a podpora při provozu nástroje podporujícího účinnou detekci a zvládání pokročilých kybernetických hrozeb“

Specifikace plnění

Předmětem plnění je dodávka, implementace a podpora provozu řešení pokročilé IT bezpečnosti, které bude nástrojem pro bezpečnostní specialisty dodavatele, IT a bezpečnostní specialisty Zadavatele a které umožní získat informace a vizibilitu na dění v počítačové síti s cílem detekce, identifikace a zamezení pokročilých útoků. 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
- Záznam informací o síťové komunikaci a dění na stanicích v podobě meta-dat, která umožní jejich pozdější analýzu
- Síťové DLP pro detekci a zamezení úniku dat
- Nástroj pro automatizaci řešení bezpečnostních incidentů (Incident Response – dále jen IR) na koncových stanicích (známé jako Automation Detection and Response)

Systém musí poskytovat jednotné uživatelské webové rozhraní pro práci specialistů s dodávaným řešením (tedy pro síťovou část i endpoint). 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 na jiné stanici), tak z hlediska stejných IP adres apod.

Plnění bude obsahovat

1) Dodávka technologie
2) Implementační práce a základní zaškolení obsluhy zařízení
3) Podpora výrobce - Podpora výrobce na 3 roky
4) Servisní podpora - Servisní podpora spojená s provozem technologie na 3 roky
5) Podpora pracovníků Zadavatele při bezpečnostní analýze síťového provozu a při řešení bezpečnostních událostí a incidentů po dobu 3 let

1. Technické požadavky na požadované řešení

Systém musí poskytovat funkcionality umožňující automatizaci mnoha kroků a procesů v rámci vyšetřování a IR s cílem snížit zatížení specialistů. Uchazeč popíše oblasti procesu vyšetřování a IR, které je možné pokrýt automatizací. 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.
- Systém bude provádět automatikou validaci projevů hrozeb detekovaných na síti rozpoznáním jejich projevů na stanicích. A 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 datové linky s linkovou propustností 500 Mbps.
- Zadavatel zajistí zrcadlení provozu vhodného pro monitoring (komunikace vnitřních sítí vůči internetu) na portu přepínače.
- Monitoring bude probíhat v primárním DC zadavatele.
- Počet stanic zahrnutých do projektu je 2000 stanic s OS Windows 7 a vyšší.
- Požadovaná retence kompletních meta-dat o síťovém provozu a činnosti stanic je 3 měsíce.
- Požadovaná integrace se zadavatelem provozovaným prostředím SIEM na platformě IBM Qradar.

Tabulka požadavků na dodávané řešení:

Parametr	Požadovaná hodnota (pro jedno fyzické zařízení)	Splňuje Ano/Ne	Nabízená hodnota (Popis)
Analýza síťového provozu	Analýza síťového provozu probíhá pro veškerý síťový provoz a bez ohledu na použité komunikační protokoly a monitorována jsou tedy všechna probíhající spojení na všech síťových portech.	ANO	Nástroj analyzuje veškerý provoz a pro identifikace obsahu neprovádí selekci dle protokolových čísel.
Analýza síťového provozu	Funkcionalita analýzy a záznamu síťového provozu pracuje nad zrcadleným provozem, který Zadavatel poskytne na vyhrazeném portu přepínače.	ANO	SPAN port přepínače síťové infrastruktury zákazníka, nebo TAP síťový rozbočovač.

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	Provoz podléhá plnému dekódování obsahu včetně obsahu vícenásobně vnořeného a neberou se ohledy na souborové přípony a čísla komunikačních portů.
Analýza síťového provozu	Podpora monitorování provozu na rozhraních Ethernet s rychlostmi 100Mbps a 1Gbps pro budoucí rozšiřování systému pro monitorování provozu vnitřní sítě.	ANO	Řešení disponuje 2x1Gbps metalické síťové rozhraní pro monitoring provozu.
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.	ANO	Řešení umožňuje na základě vlastních pravidel výrobce, nebo uživatelem definovaných pravidel, provádět detekci jednotlivých událostí i událostí souvisejících. Tyto detekce probíhají v reálném čase, nebo nad historickými daty (retrospektivně).
Analýza síťového provozu	Systém poskytuje webové uživatelské rozhraní pro analýzu zaznamenaného provozu bezpečnostními specialisty, které bude součástí jednotného uživatelského rozhraní.	ANO	Jednotné a plně spolu integrované WEB rozhraní.
Analýza síťového provozu	K dispozici jsou historické informace o provozu s určenou dobou retence pro následnou analýzu.	ANO	Řešení obsahuje ve své konfiguraci komponentu typu „kolektor", která umožňuje ukládání historických dat a dostatečnou kapacitou pro uložení požadované 3 měsíce.
bezpečnostní dohled koncových stanic	Záznam činnosti koncového bodu alespoň v rozsahu spouštěných procesů, modifikovaných nebo vytvářených souborů, manipulaci s registry, paměťovými médii zapojenými na USB a síťové činnosti.	ANO	Všechny požadované informace z koncového bodu dokáže nabízené řešení zaznamenat.

bezpečnostní dohled koncových stanic	Možnost definovat pravidla, která budou vyhodnocovat činnosti a vytvářet alerty v případě shody (například Word zapisuje spustitelný soubor na disk).	ANO	Uživatelem definovaná pravidla umožňuje nabízené řešení definovat pro síťový provoz i pro chování koncového bodu.
bezpečnostní dohled koncových stanic	Má funkcionality antivirového a anti-malware systému (tedy schopnost zabránit spuštění procesu v případě nalezení viru/malware).	ANO	Pro koncový bod disponuje řešení schopností automatické reakce při zaznamenání virové/malwarové aktivity.
bezpečnostní dohled koncových stanic	Umožňuje vzdáleně šetřit incident (získání směrovací tabulky, arp tabulky, hodnoty klíčů v registech, seznam přihlášených uživatelů, bezpečnostní analýza obsahu paměti stanice bez nutnosti přenosu memory dumpu po síti...)	ANO	Řešení umožňuje povelování endpoint agenta pro účely dodatečného získávání informací a šetření událostí, pokud k tomuto šetření nepostačují již uložené meta-informace.
bezpečnostní dohled koncových stanic	Umožňuje vzdáleně řešit incident (mazání souborů, modifikace klíču registrů, odinstalace SW, izolace stanice, hledání souboru dle hash, mazání souborů, ...)	ANO	Řešení umožňuje povelování endpoint agenta pro účely vzdáleného řešení incidentů v požadovaném rozsahu.
bezpečnostní dohled koncových stanic	Systém implementuje velmi granulární RBAC pro určení práv jednotlivých bezpečnostních specialistů. Umožní, aby případní vnější specialisté měli přístup k přesně vymezené množině alarmů.	ANO	Řešení umožňuje využít širokou škálu rolí pro řízení přístupů uživatelů systému.
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.	ANO	Inspekce provozu není omezena na určité komunikační protokoly, ale je prováděna nad veškerým provozem.
DLP funkcionalita	Funkcionalita DLP je schopná odhalit obsah přenášený jako součást souborových archivů (ZIP, RAR, TAR, GZIP, ...) a obsah detekovat k dokumentech typu MS Word, MS Excel, MS PowerPoint, OASIS dokumentech, PDF a dalších běžných kancelářských formátech) – bez	ANO	Všechny požadované typy souborů a archivů jsou podporovány.

	omezení hloubky vnoření.		
DLP funkcionalita	Funkcionalita DLP je schopna odhalit obsah v dokumentech vložených (embedovaných) do jiných formátů (Excel jako objekt je Wordu, JavaScript jako objekt v PDF, ZIP jako objekt v PowerPoint) bez ohledu na počet a hloubku vložení.	ANO	Řešení provádí kompletní dekompozivi obsahu a vůči každé dekódované úrovni je prováděna inspekce.
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).	ANO	Výhode nabízeného řešení spočívá v kooperaci všech jeho detekčních technik. Lze tedy kombinovat libovolná pravidla a navzájem je podmiňovat.
Oblast detekce malware	Detekce malware je prováděna pomocí vyhledávání signatur, detekcí typického chování (behavioral analýza) a detekce jeho virtuálním provedením.	ANO	Všechny požadované metody nabízené řešení splňuje.
Oblast detekce malware	Součástí dodávky je kontinuální služba aktualizace signatur/definice chování malware/aktualizace pravidel sandboxu z komerčního zdroje.	ANO	K tomuto je využívána služba Threat-Intelligence výrobce, která je součástí nabízeného řešení.
Oblast detekce malware	Obdobně jako pro DLP je systém schopný malware detekovat i skrytý hluboko v přenášeném obsahu – bez omezení hloubky vnoření.	ANO	Přístup nástroje k detekci malware je identický jako u funkcionality DLP, dochází tedy k rozkladu komunikace bez omezení hloubky.
Detekce a ochrana proti APT	Viditelnost všech fází APT útoku (dle fází kill-chain – od iniciální kompromitace do ex-filtraci dat).	ANO	Uživatel má k dispozici rozhraní pro vyšetřování, které je rozděleno dle fází v nichž byly zachyceny jednotlivé fáze útoku.
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.	ANO	Webové rozhraní obsahuje přehlednou časovou osu pro analýzu šetřeného a souvisejícího provozu a

			provazbou na související události.
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.	ANO	Řešení disponuje velice propracovanýcm systémem vyhledávání s možností definice téměř libovolných filtrů.
Reporting	Schopnost vygenerovat report (ideálně v podobě PDF dokumentu) a tento s danou periodicitou odesílat na emailové adresu.	ANO	Reporting je nedílnou součástí nástroje a umožňuje reporty generovat a odesílat a to i plánovaně.
Reporting	Řešení nabízí předpřipravenou sadu typických reportů s možností jejich úpravy.	ANO	Reporty dle šablon výrobce jsou součástí nabízenho řešení.
Reporting	Vlastní report bude možné definovat v editoru šablon reportů.	ANO	Vlastní tvorba šablon je možná dle požadavku.
Podpora vyšetřování	Systém umožní realizovat alespoň základní workflow pro práci se zaznamenanými alerty (stav, přiřazení řešiteli, historie činností).	ANO	Systém předpokládá zapojení více specialistů do šetření událostí a umožňuje tak jednotlivé aktivity delegovat na jiného uživatele.
Otevřenost platformy	Dokumentované aplikační rozhraní pro zákaznické integrace s dalšími bezpečnostními komponentami. Preferujeme http & XML nebo JSON API rozhraní.	ANO	Systém disponuje API s požadovanými formáty vstupu/výstupu.
Otevřenost platformy	Předpřipravené integrační vazby na aplikace typu SIEM.	ANO	Systém lze integrovat přímo s nástroji SIEM díky předpřipraveným konektorům. Výrobce IBM Qradar je mezi podporovanými.
Integrace	Systém musí podporovat provoz v hierarchickém režimu pro případné budoucí zahrnutí nadřízených či	ANO	Výcevrstvé SOC pracoviště, tedy

	podřízených subjektů do bezpečnostního dohledu.		hiearchická struktura zapojení nabízeného řešení je možná.
Reporting	Možnost zaznamenávat statistiky provozu řešení a incidentů, vytvářet exportovatelné výstupy včetně grafů. Možnost posílání logu na externí úložiště minimálně ve formátu syslog.	ANO	Všechny požadované parametry systém splňuje. Části provozu je možné uložit do souboru, meta-data je možné exportovat a logy jsou zasílány na syslog servery.

2. Požadavky na vykonání implementačních prací a podporu řešení

Dodavatel provede úplnou implementaci v datovém centru Magistrátu hl. m. Prahy. Součástí implementačních prací je i základní zaškolení obsluhy zařízení v rozsahu 1 pracovního dne.

3. Podpora výrobce celkem na 3 roky

Nedílnou součástí dodávky zařízení je i technická podpora výrobce obsahující:

- Dodávku Upgrade, Update operačního systému a bezpečnostních databází
- Výměna vadného dílu zařízení – odeslání NBD (následující pracovní den po nahlášení závady)

4. Servisní podpora spojená s provozem technologie

- Servisní podpora spojená s provozem technologie na 3 roky v režimu 5 x 12 (od 8:00 do 20:00).
- Dodavatel zajistí dodání náhradního provizorního HW a zprovozní systém do 24h od nahlášení závady zařízení.
- Dodavatel zajistí implementaci vyměněného vadného dílu dodaného výrobcem do 24 hodin od jeho obdržení výrobcem a zajistí celkové zprovoznění systému.
- Dodavatel zajistí instalaci Upgrade, Update verzí systému neprodleně po jejich obdržení od výrobce zařízení

4.1. Služba helpdesku

Dodavatel je povinen zajistit službu helpdesku, která zajistí příjem a evidenci všech požadavků přes email, telefonní linku a webové rozhraní. Služba bude provozována v režimu 5 x 12.

4.2. Řešení vad a provozních incidentů spojených se systémem

Kategorie vad

(i) **Vady kategorie A (kritická):**
Vady, které způsobují provozní problémy a neumožňují využívání systému k účelu, ke kterému je určen.

(ii) **Vady kategorie B (vysoká):**
Méně závažné vady a nedostatky, které funkčně nebo kapacitně omezují využívání systému k účelu, ke kterému je určen.

(iii) **Vady kategorie C (střední a nízká):**

Vady a nedostatky, které neomezují využívání dodaného systému k účelu, ke kterému je určen, ale nejsou v souladu se správnou funkcí a dokumentací systému.

Garance	Vada kategorie A (režim 24x7)	Vada kategorie B (režim 24x7)	Vada kategorie C (režim 24x7)
Potvrzení příjmu požadavku a oznámení jména řešitele zákazníkovi.	Do 30 minut od okamžiku nahlášení vady.	Do 30 minut od okamžiku nahlášení vady.	Do 1 hodiny od okamžiku nahlášení vady.
Analýza provozního incidentu, předání incidentu na výrobce	Do 4h od nahlášení incidentu	Do 12h od nahlášení incidentu	Do 24h od nahlášení incidentu

Vady mohou být nahlášené buď přes záznam v helpdesku poskytovatele, nebo hlášením z monitoringu proaktivně vedeného Poskytovatelem.

4.3. Nadstavbové služby (v maximálním rozsahu 40 MD ročně)

- Implementace mechanismů upravujících aplikační provoz a pro vytváření aplikačně specifických „skriptů", které umožní manipulovat s provozem nebo provoz omezit
- Implementace nových bezpečnostních politik pro nové služby a aplikace
- Pokročilá konfigurace bezpečnostních politik, aktualizace politik a jejich řízená modifikace
- Pravidelný reporting změnových aktivit pro odpovědné osoby
- Zavedení ochrany v souvislosti např. s
    - výsledky penetračních testů
    - auditních nálezů
    - nově publikovaných hrozeb

4.4. Podpora pracovníků Zadavatele při bezpečnostní analýze síťového provozu a při řešení bezpečnostních událostí a incidentů (v maximálním rozsahu 74 MD ročně)

Zadavatel zajistí podporu pracovníkům Zadavatele v následujícím rozsahu:

- Přidělení bezpečnostního analytika do 30 minut po nahlášení Incidentu
- Zajištění podpory pracovníků Dodavatele po celou dobu šetření Incidentu buď vzdáleným přístupem či osobní účastí v místě instalace systému
- Souhrnný report o šetření bezpečnostních incidentů 1 x měsíčně