**Příloha č. 5 – Technická specifikace**

Zadavatel požaduje dodávku systému proaktivní ochrany 1900 koncových stanic s navázáním na stávající technologii NextGenFirewall Palo Alto PA-3220 a PA-3250 a s centrální správou dle požadavků uvedených v příloze.

Součástí dodávky je instalace řídícího systému do prostředí objednatele - na platformu VMware 7.0, dokumentace a příprava automatizované instalace klientů prostřednictvím služeb Microsoft Active Directory 2019.

Součástí dodávky je podpora dodaného systému na 3 roky s reakcí 9x5 NBD s dodáním kontaktního tel. čísla, email adresy a URL adresy pro přístup do servicedesku dodavatele k zakládání servisních a konzultačních požadavků.

Akceptace se uskuteční na základě předání funkčního řídícího systému napojeného na NGFW a instalovaných 20 koncových stanic objednatele.

Součástí dodávky bude školení 3 pracovníků zadavatele.

Kontakty pro zadávání požadavků: tel.: [DOPLNIT]
e-mail: [DOPLNIT]
web: [DOPLNIT]

**Tabulka požadovaných parametrů:**

| | **Nástroj typu XDR (Extended Detection and Response), zajišťující prevenci před útoky, detekci pokročilých útoků a poskytující data a nástroje pro forenzní analýzu.** | |
|---|---|---|
| | | |
| | **Obecné požadavky** | **Ano/Ne** |
| 1 | Všechny požadované funkce týkající se koncového bodu, jakými jsou zejména, ale nikoliv výlučně ochrana před nákazou, sběr dat k analýze, zajištění shody s pravidly (compliance), jsou prováděny výhradně jediným agentem běžícím na koncovém bodě. | |
| 2 | Všechny úkony týkající se zejména, ale nikoliv výlučně konfigurace systému, správy a ochrany koncových zařízení, forenzní analýzy jsou prováděny v jednotné konzoli, přístupné pomocí webového rozhraní. | |
| 3 | Dodávaný systém je zprovozněn bez nutnosti instalace jakýchkoliv dodatečných hardwarových či softwarových komponent do prostředí zadavatele, s výjimkou instalace agentů na koncová zařízení a systémů uvedených v následujících dvou řádcích. | |
| 4 | Dodávaný systém umožňuje správu koncových zařízení, která nedisponují přímou konektivitou do internetu. K tomu je možno použít on-premise virtuální server, sloužící jako proxy pro komunikaci s managementem, a který je bezplatnou součástí dodávaného systému. | |
| 5 | Dodávaný systém musí umožnit volitelné rozšíření o funkci pro sběr dat z on-premise zdrojů, jako jsou Windows event logy, syslog, netflow. K zaslání těchto logů do centrálního managementu je možno použít on-premise virtuální server, který je bezplatnou součástí dodávaného systému. | |

| | | |
|---|---|---|
| 6 | Dodávaný systém zajišťuje sběr takových dat z koncových zařízení, která jsou relevantní k zastavení nebo detekci útoku a následné forenzní analýze. | |
| 7 | Dodávaný systém musí umožnit volitelné rozšíření o funkci pro detekci a prevenci bezpečnostních incidentů pro data zejména, nikoliv výlučně z následujících zdrojů: Netflow, firewallové logy nezávislé na výrobci FW, Windows Event logy. | |
| 8 | Dodávaný systém umožňuje napojení na zdroje identit minimálně následujících typů: Azure AD, on-premise AD, Okta. | |
| 9 | Dodávaný systém poskytuje RBAC (role-based access control) umožňující granulární přiřazení oprávnění jednotlivým správcům systému. | |
| 10 | Dodávaný systém obsahuje možnost zapnout multifaktorovou autentizaci pro správce bez nutnosti poskytnout toto řešení ze strany zákazníka. | |
| 11 | Dodávaný systém obsahuje API pro umožnění integrace nástrojů třetích stran a pro provádění administrativních úkonů. | |
| 12 | Dodávaný systém umožňuje export dat ve formátu syslog pro nástroj správy logů třetí strany. | |
| 13 | Dodávaný systém umožňuje tvorbu dynamických dashboardů, čerpající data definovaná libovolným uživatelským pohledem do databáze. | |
| 14 | Data jsou uchována výhradně v rámci EU. | |
| 15 | Data jsou uchována výhradně v datových centrech certifikovaných na SOC2 Type II+. | |
| 16 | Dodávaný systém má platnou certifikaci ISO 27001. | |
| | | |
| | **Prevence útoků** | **Ano/Ne** |
| 17 | Dodávaný systém poskytuje ochranu před známým škodlivým kódem i bez nutnosti pravidelné aktualizace databáze signatur. | |
| 18 | Dodávaný systém poskytuje ochranu před známým i neznámým škodlivým kódem i bez nutnosti být v tu chvíli připojen k internetu či interní síti. | |
| 19 | Dodávaný systém brání spuštění škodlivých procesů, stejně jako činnosti, která je vyhodnocena jako škodlivá až v průběhu běhu procesu. | |
| 20 | Dodávaný systém brání škodlivému chování, které je způsobeno legitimními procesy. | |
| 21 | Dodávaný systém poskytuje ochranu před bezsouborovými útoky. | |
| 22 | Dodávaný systém provádí dynamickou analýzu chování běžících procesů. | |
| 23 | Dodávaný systém obsahuje funkci dynamické analýzy v sandboxu, umožňující analýzu souborů minimálně do velikosti 100MB. | |
| 24 | Dodávaný systém poskytuje dynamickou analýzu v sandboxu minimálně souborů typu apk, flash, java, office, PE, pdf, mac OS X files, linux ELF, archivy rar, 7-zip, skripty bat, shell. | |
| 25 | Dodávaný systém poskytuje dynamickou analýzu dat v sandboxu, jak s využitím virtuálního, tak bare-metal prostředí pro zabránění evazivnímu chování škodlivého kódu. | |
| 26 | Dodávaný systém dokáže zastavit spuštění neznámého souboru, dokud nezíská verdikt z dynamické analýzy sandboxu. | |
| 27 | Dodávaný systém umožňuje manuální změnu verdiktu poskytnutého dynamickou analýzou. | |
| 28 | Dodávaný systém odesílá vzorky k analýze do sandboxu na základě hash hodnot. Jeden identický soubor tak nebude analyzován zbytečně vícekrát, byť má rozdílný název. | |
| 29 | Dodávaný systém dokáže provést whitelisting/blacklisting spustitelných procesů na základě hash hodnoty, umístění a digitálního podpisu souboru. | |

| | | |
|---|---|---|
| 30 | Dodávaný systém obsahuje funkci lokální analýzy, využívající prvky strojového učení. | |
| 31 | Dodávaný systém umožňuje vytvoření pravidel/zásad, které zamezí konkrétním scénářům spuštění škodlivého kódu. | |
| 32 | Dodávaný systém poskytuje ochranu před útokem pomocí manipulace s pamětí a spuštěním kódu z datové oblasti (techniky DEP, JIT, ROP). | |
| 33 | Dodávaný systém umožňuje blokaci útočných technik jakými je například vkládání kódu. | |
| 34 | Dodávaný systém umožňuje blokaci DLL knihoven s nebezpečným umístěním. | |
| 35 | Dodávaný systém umožňuje blokaci útočných technik manipulujících s obsahem (heap spray, buffer overflow). | |
| | | |
| | **Parametry agenta koncových zařízení** | **Ano/Ne** |
| 36 | Agent instalovaný na koncové zařízení má nízké HW nároky (instalační soubor maximálně 100 MB, nízká zátěž CPU při zapnutí všech funkcionalit, nízké obsazení RAM) | |
| 37 | Dodávaný systém zajišťuje správu koncových zařízení i za účelem identifikace cizích zařízení. | |
| 38 | Dodávaný systém poskytuje možnost skenování koncových stanic za účelem nalezení malware dle plánu či na vyžádání. | |
| 39 | Dodávaný systém umožňuje vynucení a kontrolu pravidel lokálního Windows a macOS firewallu na koncovém zařízení. | |
| 40 | Dodávaný systém umožňuje vynucení a kontrolu politik šifrování disku pomocí technologie BitLocker (Windows), respektive FileVault (macOS). | |
| 41 | Dodávaný systém umožňuje vynucení zákazu přístupu k mobilním médiím (USB, DVD) a řízení spouštění procesů z těchto médií, stejně jako ze síťových umístění. | |
| 42 | Agent nainstalovaný na koncovém zařízení žádným způsobem nenarušuje činnost VPN agentů Anyconnect a GlobalProtect používaných zákazníkem. | |
| 43 | Dodávaný systém zaručuje, že koncoví uživatelé nejsou schopni obejít bezpečnostní pravidla, i když mají práva místních správců. | |
| 44 | Dodávaný systém zaručuje, že agenta není z koncového zařízení možné odinstalovat/odstranit bez znalosti hesla definovaného v managementu systému. | |
| 45 | Dodávaný systém zaručuje, že ani lokální adminstrátoři nemohou zastavit agenta nebo související služby. | |
| 46 | Dodávaný systém zaručuje, že ani lokální adminstrátoři nemohou upravit součásti systému ochrany koncových zařízení, programové složky a záznamy v registru, které jsou potřebné pro plnohodnotnou ochranu. | |
| 47 | Dodávaný systém zaručuje, že agenta je možno aktualizovat z prostředí centrálního managementu. | |
| 48 | Dodávaný systém zaručuje podporu provozu v non-persistentním VDI prostředí | |

| | | |
|---|---|---|
| 49 | Agent je možno nainstalovat minimálně na následující platformy a OS:<br>Všechny aktuálně podporované verze Microsoft Windows (32-bit, 64-bit)<br>Všechny aktuálně podporované verze Microsoft Windows Server (32-bit, 64-bit)<br>Všechny enterprise distribuce Linux (Debian, Ubuntu, Red Hat, SuSE Linux Enterprise server, CentOS)<br>Všechny aktuálně podporované verze Apple MAC OS a MAC OS X – min. High Sierra a novější včetně Big Sur<br>Android OS 6 a novější<br>Citrix XenDesktop RDS + VDI, XenApp<br>VMware Horizon View, Appvolumes, ThinApp | |
| 50 | Dodávaný systém je plnohodnotnou náhradou antivirového řešení a systém Microsoft Windows ho tak ve svém system centru zobrazuje. | |
| | | |
| | **Sběr dat pro účely analýzy** | **Ano/Ne** |
| 51 | Dodávaný systém získává pro analýzu uživatelská data (doménové jméno, organizační složka, email adresa, typické koncové zařízení, uživatel spouštějící proces) napojením na interní adresářovou službu. | |
| 52 | Dodávaný systém získává pro analýzu informace o koncovém zařízení (IP adresa, MAC adresa, název a doména, informace o OS, informace o instalovaném FW) prostřednictvím agenta nainstalovaného na koncovém zařízení. | |
| 53 | Dodávaný systém získává pro analýzu informace o procesu (časové razítko, cesta a jméno, ID procesu, hash MD5 nebo SHA-256, parametry) spouštěném na koncovém zařízení, pomocí agenta, který je na koncovém zařízení nainstalován. | |
| 54 | Dodávaný systém získává pro analýzu informace o souborech (časové razítko, cesta a jméno, historie umístění a jména, hash MD5 nebo SHA-256) a práci s nimi (vytvoření, smazání, přejmenování, přesun, zkopírování) prostřednictvím agenta nainstalovaného na koncovém zařízení. | |
| 55 | Dodávaný systém musí umožnit volitelné rozšíření umožňující získání informace pro analýzu ze síťových prvků (časové razítko, zdrojová a cílová IP adresa i port, přenesený objem dat, protokol, geolokační data, integrace s aplikačním firewallem pro kompletní analýzu layer 7 včetně jména aplikace, doba spojení, rozšířená data o klíčových protokolech - DNS, HTTP, DHCP, RPC, ICMP, ARP). K tomu musí být schopen použít stávající síťová zařízení instalovaná v síti zákazníka. Podpora minimálně firewallů nové generace výrobců Cisco, Fortinet, Checkpoint, Palo Alto Networks. | |
| 56 | Dodávaný systém musí umožnit volitelné rozšíření o funkci pro získávání informace pro analýzu o registrech systémů Windows (časové razítko, název zápisu, jeho hodnota a typ, historie změn) prostřednictvím agenta nainstalovaného na koncovém zařízení. | |
| 57 | Dodávaný systém získává pro analýzu informace o systémových událostech, jako je zejména, nikoliv však výlučně přihlášení a odhlášení uživatele prostřednictvím agenta nainstalovaného na koncovém zařízení. | |
| 58 | Dodávaný systém musí umožnit volitelné rozšíření pro analýzu bezpečnostní události, navštěvovaná URL, incidenty z firewallů nové generace minimálně od výrobců Cisco, Fortinet, Checkpoint, Palo Alto Networks. | |
| | | |
| | **Detekce pokročilých hrozeb (APT)** | **Ano/Ne** |
| 59 | Dodávaný systém používá k detekci hrozeb vytvoření standardního chování síťového provozu, uživatelů, i konkrétních koncových zařízení (tzv. baseline) a sleduje odchylky zachycené systémem strojového učení. | |
| 60 | Dodávaný systém provádí detekci hrozeb na základě pravidel definovaných výrobcem, založených na indikátorech kompromitace (IOC) a behaviorálních indikátorech | |

| | | |
|---|---|---|
| | kompromitace (BIOC). | |
| 61 | Dodávaný systém umožňuje tvorbu uživatelských IOC na základě zadání celé cesty umístění souboru, jména souboru, navštěvované domény, IP adresy, hashe souboru, nebo pokročilé behaviorální IOC skládající se z řetězce událostí jako je např. vytváření souborů, spouštění specifických procesů, úprav registrů, iniciace síťové komunikace. | |
| 62 | Dodávaný systém umožňuje přebírání informací o nových hrozbách ze zdrojů třetích stran ve formátu JSON a CSV. | |
| 63 | Dodávaný systém umožňuje vytváření IOC pomocí API, včetně možností importu více IOC najednou a importu IOC z CSV souboru v konzoli pro správu. | |
| 64 | Dodávaný systém umožňuje nastavit pro jednotlivé IOC hodnotu závažnosti. | |
| 65 | **Dodávaný systém detekuje minimálně následující události:** | |
| 66 | Nestandardní síťová komunikace, jako je neúspěšná komunikace, změna v objemu z pohledu množství dat, nebo relací, první úspěšné přihlášení z nové země, přihlášení jedním účtem z více zemí v krátkém časovém úseku, administrátorská komunikace ze stanice, která byla dříve pouze uživatelskou, neočekávaná SMTP a SSH spojení. | |
| 67 | Spuštění nové služby, která neodpovídá charakteru koncového zařízení. | |
| 68 | Nestandardní uživatelské chování, které je v rozporu s charakterem ostatních typových koncových zařízení, nestandardní komunikace známých procesů, spuštění známých zneužitelných procesů např. z dokumentů MS Office. | |
| 69 | Nestandardní práce s uživatelskými účty, jako jsou výjimečná přihlášení výchozími účty, snaha o přihlášení zablokovaným účtem, nebo účtem, který nebyl dlouho použit, neúspěšná snaha o přihlášení stejným účtem na více koncových zařízeních, snaha o získání uložených přihlašovacích údajů (mimikatz, cmdkey) | |
| 70 | Dodávaný systém musí umožnit volitelné rozšíření o detekci nestandardního DNS chování, jako je DNS tunneling, více neúspěšných DNS dotazů. | |
| 71 | Nestandardní práce se soubory, jako je např. zpožděné smazání, závislé na ověření konkrétní komunikace. | |
| 72 | Skenování okolních počítačů, ať již pomocí standardních port či sweep skenů, nebo použití WMIC. | |
| 73 | Snaha o prolomení hesel, jako je bruteforce útok. | |
| 74 | Chování, odpovídající známé útočné technice | |
| | | |
| | **Reakce na hrozby** | **Ano/Ne** |
| 75 | Dodávaný systém umožňuje zabezpečený a logovaný terminálový přístup na koncovou stanici. | |
| 76 | Dodávaný systém umožňuje v reakci na zaznamenanou hrozbu, nebo i manuálně spustit skript či příkaz v prostředí Windows (CMD, PowerShell, Python) a skripty typu bash a Python v prostředí MacOSX a Linux. | |
| 77 | Dodávaný systém umožňuje spuštění Python skriptu na více koncových zařízeních nezávisle na jejich OS (Windows, macOS, Linux) a bez nutnosti instalovat prostředí Python. Skript je interpretován součástí agenta nainstalovaného na koncovém zařízení. | |
| 78 | Dodávaný systém obsahuje předdefinovanou sadu skriptů pro snadný sběr dat, jejich analýzu a vyhodnocení, stejně jako pro servisní zásahy okamžitě blokující útok probíhající na koncovém zařízení. | |

| | | |
|---|---|---|
| 79 | Dodávaný systém umožňuje automaticky izolovat jedno či více nakažených koncových zařízení tak, že koncové zařízení má možnost komunikovat pouze s managementem dodávaného systému. | |
| 80 | Dodávaný systém musí umožnit volitelné rozšíření o funkci pro vzdálené smazání podezřelého či škodlivého souboru z jednoho či více koncových zařízení najednou pomocí grafického rozhraní i pomocí skriptu. | |
| 81 | Dodávaný systém bude dodavatelem integrován s používanými firewally (Palo Alto Networks) tak, aby byly firewally automaticky a okamžitě po získání informace schopny blokovat IP adresy či domény označené dodávaným systémem jako nevhodné. | |
| 82 | Dodávaný systém umožňuje integraci se SOAR řešením pro analýzu incidentů. | |
| 83 | Dodávaný systém umožňuje integraci s používaným SIEM řešením (IBM Qradar). | |
| | | |
| | **Analýza incidentů** | **Ano/Ne** |
| 84 | Dodávaný systém poskytuje automatizovanou analýzu hlavní příčiny jakéhokoliv incidentu, včetně nástrojů a dat pro detailní forenzní analýzu. | |
| 85 | Dodávaný systém provádí vizualizaci jednotlivých kroků tvořících incident, včetně možnosti přehledně sledovat jejich časovou posloupnost, včetně současného výskytu na dalších koncových zařízeních. | |
| 86 | Dodávaný systém poskytuje nástroj pro vyhledávání ve všech nasbíraných datech pomocí plnohodnotného dotazovacího jazyka. Tento nástroj zajistí možnost vyhledat jakoukoliv uloženou informaci. | |
| 87 | Dodávaný systém poskytuje uživatelsky přívětivý nástroj pro vyhledávání v nasbíraných datech pomocí grafického rozhraní správcovské konzole. | |
| 88 | Dodávaný systém v rámci incidentu automaticky propojí a přehledně prezentuje informace ze všech zdrojů dat, vztahující se k detekovanému incidentu. | |
| 89 | Dodávaný systém prezentuje všechny akce a incidenty na časové ose. | |
| 90 | Dodávaný systém prezentuje informaci o tom, jestli byla škodlivá činnost blokována agentem na koncovém bodu, firewallem, nebo jinou preventivní technologií. | |
| 91 | Dodávaný systém poskytuje pouze relevantní informace a potlačuje šum, např. odstranění bezvýznamných binárních souborů a DLL knihoven z řetězce událostí. Tyto potlačené informace, které nejsou relevantní k vyšetřování incidentu je však stále možno dohledat. | |
| 92 | Dodávaný systém umožňuje vyhledávat indikátory kompromitace napříč jednotlivými koncovými zařízeními, např. v případě výskytu škodlivého souboru na jednom z koncových zařízení je možné automaticky prohledat, jestli se tento soubor nevyskytuje i na dalších spravovaných koncových zařízeních, nebo při výskytu škodlivé komunikace je možno vyhledat, která koncová zařízení (i ta bez nainstalovaného agenta) komunikovala obdobně. | |
| 93 | Dodávaný systém poskytuje funkci zpětného vyhledávání v historických datech. Ve chvíli, kdy je vytvořen či výrobcem doplněn nový IOC nebo BIOC, je systém schopen prohledat dostupná historická data a vytvořit incidenty, ke kterým došlo v minulosti, kdy ještě konkrétní způsob útoku nebyl známý. | |
| 94 | Dodávaný systém poskytuje funkci řízeného vyhledávání hrozeb na základě IOC pro snadné a rychlé prověření celého prostředí. | |
| 95 | Dodávaný systém zobrazuje u každé části incidentu její návaznosti na standardizovaný framework MITRE ATT&CK. | |

| | | |
|---|---|---|
| 96 | Dodávaný systém obsahuje integrovanou MITRE ATT&CK matici s vyznačenými technikami, které daná část útoku používá. | |
| 97 | Dodávaný systém umožňuje tvorbu vlastních pravidel, které definují skóre jednotlivých incidentů pro účely jejich prioritizace. | |
| | | |
| | **Správa incidentů** | **Ano/Ne** |
| 98 | Dodávaný systém udržuje životní cyklus incidentu, jako je jeho otevření, přiřazení, vyšetření, uzavření. | |
| 99 | Dodávaný systém umožňuje manuální přepsání závažnosti incidentu. | |
| 100 | Dodávaný systém poskytuje informaci o všech uživatelích, zařízení, souborech a doménách zapojených do konkrétního incidentu. | |
| 101 | Dodávaný systém umožňuje manuální sloučení incidentů. | |
| 102 | Dodávaný systém umožňuje přiřadit incident konkrétnímu řešiteli, včetně zaslání notifikace. | |
| 103 | Dodávaný systém umožňuje přiřadit incidentu komentáře. | |
| 104 | Dodávaný systém umožňuje exportovat informací o incidentu do nástrojů třetích stran. | |
| | | |
| | **Reference** | **Ano/Ne** |
| 105 | Dodavatel poskytne alespoň dvě referenční dodávky totožného řešení v ČR, každá alespoň v počtu 1000 koncových zařízení, včetně možnosti ukázky prostředí. | |
| | | |
| | **Centrální management** | **Ano/Ne** |
| 106 | Řešení musí obsahovat **virtuální** platformu pro centrální správu všech dodaných firewallů do **VMware ESXi** prostředí | |
| 107 | Součástí dodávky musí být licence pro centrální správu, tak aby bylo možné centrálně spravovat alespoň 20 HW appliance | |
| 108 | Centrální management musí podporovat sběr logových záznamů, analýzu logových záznamů, správu veškerých bezpečnostních a síťových konfigurací, korelaci logových záznamů, analýzu hrozeb a korelaci hrozeb v jediné instanci | |
| 109 | Centrální management musí podporovat sběr 20 000 logových záznamů za vteřinu | |
| 110 | Administrátor musí mít možnost úpravy veškeré síťové a bezpečnostní konfigurace přímo na grafickém rozhraní FW a zároveň přes grafické rozhraní centrálního managementu | |
| 111 | Administrátor musí mít možnost importovat FW konfiguraci do centrálního managementu | |
| 112 | Grafické rozhraní a způsob konfigurace na centrálním managementu se musí shodovat se grafickým rozhraním a způsobem konfigurace FW nasazených u zadavatele kvůli konzistenci a jednoduchosti přechodu mezi platformami | |
| | | |
| | **Licence a podpora** | **Ano/Ne** |
| 113 | Požadovaná délka podpory a platnosti licencí je 3 roky od nasazení zařízení do sítě objednatele. | |
| 114 | Systém bude licenčně pokrývat minimálně 1900 koncových stanic. | |

**Na všechny parametry musí uchazeč odpovědět „ANO“**