ÚVN
ÚSTŘEDNÍ VOJENSKÁ NEMOCNICE
Vojenská fakultní nemocnice Praha

Technická specifikace

POPIS STÁVAJICÍHO STAVU:

Ústřední vojenská nemocnice (ÚVN) disponuje základním rámcem kybernetické bezpečnosti, který odpovídá současným požadavkům na provoz zdravotnického zařízení s vysokým stupněm dostupnosti a důvěrnosti dat. Kybernetická bezpečnost je zajišťována kombinací technických, organizačních a personálních opatření a vychází z platné legislativy a interních směrnic Ministerstva obrany ČR.

Základní monitoring provozu ICT infrastruktury je zajištěn vybranými nástroji a pravidelně vyhodnocován. Řízení incidentů probíhá ve spolupráci mezi IT oddělením a odborníky na informační bezpečnost. V provozu jsou klíčové bezpečnostní technologie na úrovni perimetru, koncových zařízení i vnitřní infrastruktury, které chrání před nejběžnějšími typy hrozeb. Zásady řízení přístupových práv a správy identit jsou zavedeny a postupně rozvíjeny.

V oblasti uživatelské bezpečnosti je kladen důraz na osvětu a prevenci – zaměstnanci jsou seznamováni s bezpečnostními zásadami a riziky, zejména ve vztahu k e-mailové komunikaci, přístupům do systémů a ochraně citlivých údajů.

Z pohledu strategického řízení kybernetické bezpečnosti si ÚVN uvědomuje nutnost dalšího rozvoje v oblasti bezpečnostní architektury, posílení detekčních a analytických schopností, zajištění kontinuálního rozvoje kompetencí a přípravy na nové legislativní požadavky, zejména v souvislosti s transpozicí směrnice NIS2 a novelizací zákona o kybernetické bezpečnosti. Prvky bezpečnosti jsou postupně systematizovány a slaďovány s celkovou IT architekturou nemocnice.

SPECIFIKACE POŽADOVANÉHO PLNĚNÍ:

Zadavatel požaduje, aby vybraný dodavatel zajistil předmět plnění na svůj náklad a nebezpečí, řádně a včas v následujícím rozsahu:

Dodávka řešení pro kybernetickou bezpečnost - SABRA, Logmanagement a síťový dohled, Software pro klasifikaci dat, Software pro skenování zranitelností **(část č. 1, 2, 3 a 4 VZ).**

Předmětem dodávky je komplexní zajištění kybernetické bezpečnosti prostřednictvím dodávky a implementace moderních nástrojů a platforem pro pokročilý bezpečnostní dohled, detekci a reakci. Zakázka zahrnuje systém SABRA, logmanagement, monitoring síťových toků, software pro klasifikaci dat a nástroj pro skenování zranitelností. Cílem je posílit ochranu IT prostředí nemocnice v souladu s legislativou (včetně směrnice NIS2), zvýšit efektivitu správy a zajistit rychlou, auditovatelnou a automatizovanou reakci na bezpečnostní incidenty. Integrované řešení přináší technologickou provázanost, provozní efektivitu a minimalizuje rizika spojená s implementací.

Další požadavky na předmět plnění je uveden v Příloze č. 5 Verifikační tabulky, kde je dodavatel povinen vyplnit hodnoty nabízeného předmětu plnění.

Splnění min. technických požadavků je pro plnění předmětné zakázky závazné. V případě, že se prokáže nesplnění jakéhokoliv technického požadavku, bude tato skutečnost důvodem pro vyloučení účastníka ze zadávacího řízení.

POŽADAVKY NA JEDNOTLIVÉ ČÁSTI:

ÚVN-VoFN Praha - kybernetická bezpečnost monitoring - nákup - software - část 1 SABRA

Zadavatel požaduje dodání integrované bezpečnostní platformy nové generace, která konsoliduje klíčové bezpečnostní schopnosti v rámci jednoho prostředí. Řešení musí zahrnovat funkcionalitu pro pokročilou detekci a reakci na hrozby, automatizaci a orchestraci bezpečnostních procesů a využívání zdrojů threat intelligence pro obohacování detekovaných bezpečnostních událostí. Cílem je zajistit rychlou a efektivní detekci, vyšetřování a řešení bezpečnostních incidentů na základě centralizovaného sběru dat, pokročilé analytiky, korelace událostí a automatizovaných zásahů napříč různými bezpečnostními nástroji a IT prostředími. Důraz je kladen na jednotnou architekturu, datové propojení jednotlivých komponent, vizuální správu automatizačních scénářů a podporu rozhodování na základě aktuálních hrozeb, indikátorů kompromitace a MITRE ATT&CK rámce.

Předmětem plnění této smlouvy je závazek poskytovatele k poskytování po stanovenou dobu bezpečnostního systému XDR (extended detection and response) určeného k ochraně 2000 ks koncových stanic vč. vyhodnocování až 100 GB denního přírůstku dat z třetích zdrojů a souvisejících nástrojů pro automatizaci, orchestraci a reakci na bezpečnostní incidenty v datové síti objednatele, včetně závazku poskytovat servisní a rozvojové služby, a to za bližších podmínek vymezených smlouvou a verifikační tabulkou.

V případě pochybností o vlastnostech nabízeného systému si vyhrazujeme právo vyžádat si funkční vzorek nabízeného řešení pro ověření funkčních vlastností a provést ověřovací testy ještě před ukončením výběrového řízení. **V tomto případě je dodavatel povinen dodat funkční vzorek do 1 týdne od výzvy zadavatele a poskytnout součinnost s testováním.**

Ověření funkčních vlastností a všech požadavků z verifikační tabulky nabízeného systému bude provádět zadavatel, vycházeje z dokumentace k nabízenému systému. V případě nejasností zadavatel vyzve k účasti zástupce dodavatele/uchazeče, který mu poskytne potřebnou součinnost, a to maximálně do 3 pracovních dnů po doručení výzvy uchazeči. Testy budou provedeny v prostředí zadavatele. Po ukončení testování budou funkční vzorky uchazeči vráceny (uchazeč si vyzvedne vzorky na vlastní náklady v místě plnění).

Ověřování bude zakončeno vyhotovením zápisu. V případě, že testovaný systém neprojde úspěšným ověřením funkčních vlastností, neuzavře zadavatel s takovým uchazečem smlouvu a vyzve k dodání testovacích vzorků uchazeče, který se v hodnocení nabídek umístil jako další v pořadí.

Kompletní technická specifikace je definována v Příloze č. 5 pro danou část.

ÚVN-VoFN Praha - kybernetická bezpečnost monitoring - nákup - software - část 2 Logmanagement a síťový dohled

Zadavatel poptává:

1. **Hardware pro centralizované ukládání a správu logů z libovolných zdrojů včetně podpory výrobce v délce trvání minimálně 60 měsíců**

2. **Implementační služby**

- Analýza – účastník provede v rámci realizace díla vstupní analýzu a vytvoří „Implementační plán projektu". Součástí tohoto plánu projektu bude technický popis řešení, vč. finální podoby implementace (nastavení) dodávaného řešení, testovacího scénáře, harmonogramu realizace projektu, potřebných instalačních postupů a požadavků na zajištění součinnosti.
- Instalace – účastník zrealizuje dodávané řešení do prostředí Zadavatele ve shodě s Implementačním plánem projektu a s ohledem na infrastrukturu Zadavatele.
    - Nedílnou součástí instalačních prací musí být zejména:
        - ✓ Instalace zařízení pro ukládání logů do infrastruktury Zadavatele

- ✓ Konzultace při nastavení infrastruktury Zadavatele tak, aby zasílala logy do logovacího nástroje
- ✓ Nastavení všech parametrů o síťové infrastruktuře do logovacího systému (DNS, DHCP atd.)

- Implementace – dodavatel provede potřebnou konfiguraci a nastavení všech modulů – dashboardů, integrovaných parserů, alertů
- Testování – účastník zajistí řádné otestování řešení dle navržených Zadavatelem schválených testovacích scénářů v Implementačním plánu projektu
- Dokumentace – dokumentace bude sepsána výhradně v českém jazyce a je vyžadována v následujícím rozsahu:
  - Implementační plán projektu, vč. popisu architektury řešení a finální konfigurace
  - Produktová dokumentace výrobce ke všem dodávaným modulům
  - Instalační dokumentace (předpis pro prvotní instalaci a instalační postupy pro údržbu a rozvoj dodávaného řešení) a dokumentace k integrovaným systémům
  - Administrátorské a uživatelské příručky (manuály)
- Zaškolení správců – v prostorách Zadavatele a v českém jazyce

3. Servisní a konzultační služby

Zadavatel požaduje specializovanou správu, údržbu a servisní podporu centrálního úložiště logů pro plně automatizovaný sběr provozních událostí z provozních systémů požadovanou přes Helpdesk uchazeče (technická úroveň podpory L2/L3) zahrnující: změny konfigurací, aktualizace, servisních zásahy, konzultace k auditní a bezpečnostní problematice v níže uvedeném rozsahu po dobu 60 měsíců.

Předmět zakázky:

Navrhnout, dodat a implementovat centrální úložiště pro sběr a analýzu logů (SEM/SIEM řešení) s možností následné analýzy a řešení bezpečnostních událostí/incidentů z kritických systémů a aplikací. Navržený systém musí zachovávat originál logů za účelem bezpečnostního auditu a umožňovat splnění legislativních norem a požadavků, zejména pak doložením souladu nabízeného systému s požadavky ISO/ČSN 27001:2013 pro pořizování auditních záznamů. Systém musí být schopen shromáždit provozní data ze všech důležitých systémů na jednom místě a dlouhodobě je uchovávat. Tímto operátor IT/Bezpečnosti dostane možnost zjistit informace o bezpečnostních incidentech, provozních stavech a případných závadách v IT v reálném čase i v pohledu do minulosti nejméně jeden rok zpět. Toto úložiště musí být schopné generovat reporty o aktivitách systémů i uživatelů, včetně auditních reportů na vyžádání, nebo se stanovenou periodicitou s definovatelným obsahem, a to bez nutnosti používat SQL syntaxi pro vytváření reportů.

Součástí dodávky musí být úplná a podrobná dokumentace systému v češtině. Není přípustné předložit českou dokumentaci, která bude odkazovat do dokumentace, která bude v jiném jazyce, než je čeština. Dodaný systém plánujeme provozovat vlastními lidskými zdroji, proto by nabízený systém měl umožňovat našim pracovníkům IT provádět základní i středně pokročilé konfigurace bez nutnosti konzultovat dodavatele nebo výrobce. Nabízený systém proto musí splňovat očekávané parametry uživatelské přívětivosti a integrity uživatelského rozhraní a vyhnout se nutnosti používaní skriptů, maker, konfigurací v příkazové řádce nebo terminálu. Dále by dokumentace měla poskytnout jednoznačné návody, jak konfigurovat nejčastější zdrojová zařízení pro spolupráci s nabízeným systémem.

V případě pochybností o vlastnostech nabízeného systému si vyhrazujeme právo vyžádat si funkční vzorek nabízeného řešení pro ověření funkčních vlastností a provést ověřovací testy ještě před ukončením výběrového řízení. **V tomto případě je dodavatel povinen dodat funkční vzorek do 1 týdne od výzvy zadavatele a poskytnout součinnost s testováním.**

Zadavatel v rámci testovacího provozu na dodaném testovacím vzorku, **vycházeje z dodané dokumentace k nabízenému systému**, provede tyto práce a vytvoří záznam o jednotlivých činnostech a jejich výsledcích. Jedná se zejména tyto testy:

- Základní nastavení systému a jeho konfigurace tak, aby mohl pracovat v prostředí zadavatele, včetně vytvoření uživatelů s rozdílným systémovým i databázovým oprávněním, a to v jednotném webovém rozhraní nabízeného systému

- Zapojení pěti vybraných zdrojových systémů logů odesílajících logy prostřednictvím Syslog protokolu přes UDP/TCP/TLS z prostředí zadavatele a otestování následujících vlastností:
    - Nastavení klasifikace zdrojů
    - Nastavení značek (tagů) pro vybrané zdrojové systémy
    - Filtrování událostí
    - Úprava normalizace existujícího zdroje v grafickém rozhraní nástroje
    - Vytvoření reportů a exportu logů a vybraných údajů z logů
- Konfiguraci pěti vybraných systémů Microsoft Windows tak, aby posílaly EVTx a textové logy do testovaného systému, s konfigurací pouze v jednotném grafickém rozhraní nabízeného systému
- Ověření funkčních a výkonových parametrů Windows agenta a jeho centralizované správy v nabízeném systému – viz Technická specifikace, všechny body z odstavce „Sběr událostí z Microsoft prostředí"
- Konfiguraci kolektoru logů z prostředí Microsoft Office365 s licencí E3 zadavatele v jednotném webovém rozhraní nabízeného systému bez nutnosti instalovat produkty třetích stran
- Konfigurace kolektoru logů z jedné databáze z prostředí zadavatele v jednotném webovém rozhraní nabízeného systému bez nutnosti instalovat na databázový server další produkty třetích stran
- Oprava ze záloh po simulovaném úplném selhání nabízeného systému v následujících krocích:
    - Provedení zálohy konfigurace a dat na externí systém
    - Vytažení dvou libovolných disků za běhu systému
    - Nastavení systému do továrního nastavení
    - Obnovení konfigurace a všech dat z vytvořených záloh
    - Kontrola úplnosti obnovené konfigurace a dat ze záloh
- Navýšení a ponížení software nabízeného systému v grafickém rozhraní a provedení kontroly, že v případě ponížení nedojde ke ztrátě dříve shromážděných dat
- Kontrola, jakým způsobem se nastavuje systém ve vysoké dostupnosti (vytvoření clusteru) v jednotném webovém rozhraní systému a úplnost dokumentace k možným havarijním scénářům
- **Kontrola výkonu systému v běžné zátěži** – generátorem logů se odešle vzorek originálních dat sesbíraných během předchozích testů. A to rychlostí odpovídající nabízenému systému, po dobu minimálně 30 minut. Sledované hodnoty budou: přijetí všech logů a jejich správné zařazení do databáze s časovým razítkem odpovídajícím skutečné době přijetí logu. Dále bude provedena kontrola, zda nedošlo během zpracování logů k jejich poškození nebo ztrátě. Logy musejí být kompletně zpracovány bez ztráty dat, se správným časovým razítkem uloženy v databázi, normalizovány a doplněny o rozšiřující informace typu metadata, DNS-PTR a geolokace
- **Kontrola výkonu systému v krátkodobém přetížení** – generátorem logů se odešle vzorek originálních dat sesbíraných během předchozích testů. A to rychlostí odpovídající dvojnásobku výkonu nabízeného systému po dobu 10 minut. Sledované hodnoty budou: přijetí všech logů a jejich správné zařazení do databáze s časovým razítkem odpovídajícím době přijetí logu systémem. Dále kontrola, zda nedošlo během zpracování logů k jejich poškození nebo ztrátě. Logy musí být kompletně zpracovány bez ztráty dat, se správným časovým razítkem uloženy v databázi, normalizovány a doplněny o rozšiřující informace typu metadata, DNS-PTR, číslo a jméno ASN a geolokace
- Kontrola kompletnosti dokumentace pro nabízený systém v českém jazyce
- Součástí ověření funkčních vlastností může být i ověření požadované funkcionality a parametrů dodaného funkčního vzorku systému dle Technické specifikace tohoto zadání.

Ověření funkčních vlastností nabízeného systému bude provádět zadavatel, vycházeje z dokumentace k nabízenému systému. V případě nejasností zadavatel vyzve k účasti zástupce dodavatele/uchazeče, který mu poskytne potřebnou součinnost, a to maximálně do 3 pracovních dnů po doručení výzvy uchazeči. Testy budou provedeny v prostředí zadavatele. Po ukončení testování budou funkční vzorky uchazeči vráceny (uchazeč si vyzvedne vzorky na vlastní náklady v místě plnění).

Ověřování bude zakončeno vyhotovením zápisu. V případě, že testovaný systém neprojde úspěšným ověřením funkčních vlastností, neuzavře zadavatel s takovým uchazečem smlouvu a vyzve k dodání testovacích vzorků uchazeče, který se v hodnocení nabídek umístil jako další v pořadí.

Monitoring síťových toků

Zadavatel poptává:

1) **Hardware a software pro monitoring sítě včetně úložiště pro dlouhodobé uchování informací o síti a podpory výrobce v délce trvání minimálně 60 měsíců**

2) **Implementační služby**
   - Analýza – účastník provede v rámci realizace díla vstupní analýzu a vytvoří „Implementační plán projektu". Součástí tohoto plánu projektu bude technický popis řešení, vč. finální podoby implementace (nastavení) dodávaného řešení, testovacího scénáře, harmonogramu realizace projektu, potřebných instalačních postupů a požadavků na zajištění součinnosti.
   - Instalace – účastník zrealizuje dodávané řešení do prostředí Zadavatele ve shodě s Implementačním plánem projektu a s ohledem na infrastrukturu Zadavatele.
     - Nedílnou součástí instalačních prací musí být zejména:
       - ✓ Instalace sondy a úložiště do infrastruktury Zadavatele
       - ✓ Konzultace při nastavení síťové infrastruktury Zadavatele tak, aby zasílala data do sond
       - ✓ Nastavení všech potřebných modulů na hardwarovém úložišti
       - ✓ Nastavení všech parametrů o síťové infrastruktuře do monitorovacího systému (DNS, DHCP atd.)
   - Implementace – dodavatel provede potřebnou konfiguraci, nastavení a odladění všech modulů – tj. pro behaviorální analýzu, vč. odladění základních fals positive, nastavení základních dashboardů v součinnosti se Zadavatelem, nastavení modulu pro automatickou analýzu zachyceného provozu a interpretaci dat z paketů.
   - Testování – účastník zajistí řádné otestování řešení dle navržených zadavatelem schválených testovacích scénářů v Implementačním plánu projektu
   - Dokumentace – dokumentace bude sepsána výhradně v českém jazyce a je vyžadována v následujícím rozsahu:
     - Implementační plán projektu, vč. popisu architektury řešení a finální konfigurace
     - Produktová dokumentace výrobce ke všem dodávaným modulům
     - Instalační dokumentace (předpis pro prvotní instalaci a instalační postupy pro údržbu a rozvoj modulů) a dokumentace k integrovaným systémům
     - Administrátorské a uživatelské příručky (manuály)
   - Zaškolení správců – v prostorách Zadavatele a v českém jazyce

Níže jsou uvedeny požadavky na celé řešení rozdělené do následujících kategorií:
- Obecné požadavky na monitorovací systém
- Požadavky na sondu
- Požadavky na kolektor
- Požadavky na modul monitoringu anomálií
- Požadavky na modul záchytu síťového provozu
- Požadavky na záruční podporu výrobce

Souhrn poptávaného řešení	***Splněno: ANO/NE***
Minimální požadavak: 2 ks hardwarového monitorovacího zařízení (sondy) 2x10Gb ethernet monitorovací port (včetně SPF+ modulu)	
Minimální požadavek: 1ks hardwarového úložiště s kapacitou 12 TB, které bude sloužit pro vyhodnocování a analýzu z monitorovacího zařízení	
Modul monitoringu anomálií – minimálně až pro 5000 toků/s a 5 zdrojů dat	

Souhrn poptávaného řešení	*Splněno: ANO/NE*
Modul pro záchyt síťového provozu s licencí pro 2 sondy	

Monitorovací systém:

Monitorovací systém musí umožňovat dlouhodobé detailní monitorování veškerého provozu na počítačové síti. Získané statistiky o provozu datové sítě musí umožnit v reálném čase sledovat a vyhodnocovat objemy a strukturu provozu, analyzovat příčiny provozních nebo výkonnostních problémů a odhalovat bezpečnostní hrozby. Je nezbytné, aby monitorovací systém byl zcela nezávislý na použité síťové infrastruktuře a svou funkcí monitorovanou síť neovlivňoval. Ze strany sledované sítě nesmí být monitorovací systém detekovatelný.

Uložení a zpracování statistik musí být redundantní na k tomu určených specializovaných zařízeních – kolektorech. Ty musí být vybaveny SW nebo HW RAIDem, případně s možností provozu na virtualizované infrastruktuře. Kolektory musí poskytovat grafické uživatelské rozhraní a analytické nástroje pro práci se síťovými statistikami bez nutnosti instalovat jakýkoliv software na klientské stanice a dále pak poskytovat automatizované reporty i notifikace na nestandardní situace. Ukládání dat probíhá kontinuálně s dostupností bez jakékoliv ztrátové agregace po dobu několika měsíců. Samozřejmostí je plná customizace způsobu prezentace dat a reportů na základě cílového prostředí.

Systém musí pracovat s technologií datových toků (NetFlow/IPFIX/jFlow/NetStream/cflow) a s moderními cloudovými FlowLog daty. Tato technologie představuje nejmodernější prostředek pro monitorování sítí včetně hybridních sítí a oproti konkurenčním technologiím nabízí výhody zpracování všech paketů bez vzorkování, imunitu vůči šifrovanému provozu, škálovatelnost i pro vysokorychlostní sítě nebo specializovaná prostředí průmyslových, tj. non IT sítí.

Požadavky na sondu:

Zdroje flow (NetFlow/IPFIX) dat (sondy) jsou výkonná autonomní zařízení, která monitorují síťový provoz, vytváří o něm statistiky v podobě IP toků (NetFlow/IPFIX data) a zasílají tyto statistiky na kolektor pro uložení a další zpracování. NetFlow/IPFIX data obsahují informace o tom, kdo komunikoval s kým, jak dlouho, jakým protokolem, kolik přenesl dat a další informace ze síťové (L3) a transportní (L4) vrstvy OSI modelu. Sondy musí umožňovat analýzu aplikační vrstvy (L7), identifikaci aplikací (NBAR2) a podrobný monitoring hlavních aplikačních protokolů (např. HTTP, DNS, DHCP). Mimo objemových charakteristik provozu musí sondy poskytovat rovněž výkonové parametry datové sítě (např. RTT, SRT, jitter) pro analýzu zpoždění na síti. Díky tomu přináší sonda komplexní přehled a detailní informace o dění v síti a usnadňuje tak řešení síťových problémů, správu a optimalizaci sítě a zvyšuje její bezpečnost.

Sondy musí být nezávislé na použité síťové infrastruktuře a svou funkcí nijak neovlivňují sledovanou síť. K síti musí být připojeny pasivně prostřednictvím SPAN/mirroring portu nebo pomocí TAPu. Ze strany monitorovacích rozhraní připojených do sledované sítě nesmí být zařízení detekovatelné. Sonda musí být vybavená vlastní kolektorovou aplikací umožňující lokální ukládání a analýzu vlastních NetFlow/IPFIX dat.

Požadavky na kolektor:

Kolektor musí splňovat následující požadavky: Kolektory je zařízení (datové úložiště) s vysokou diskovou kapacitou určená pro uložení, vizualizaci a vyhodnocení síťových statistik exportovaných NetFlow/IPFIX dat. Kolektor musí podporovat flow data ve formátech jFlow, sFlow, NetStream a další kompatibilní s NetFlow, a tudíž je na něj možné exportovat flow data z různých zdrojů (routery, switche, firewally apod.). Kolektor musí být připraven pro hybridní sítě a podporuje sběr nativních cloudových VPC flow logů. Zobrazení uložených flow dat a jejich analýza (vyhledávání, agregace, výpisy aj.) musí probíhat na kolektoru prostřednictvím zabezpečeného webového rozhraní. Uložená data a výsledky analýz musí být dostupné ve formě dlouhodobých grafů a top statistik s možností zobrazení dat až na úrovni jednotlivých komunikací (jednotlivé NetFlow/IPFIX záznamy). Kolektor musí poskytovat funkce reportování statistik o síťovém provozu a systém notifikací v případě výskytu definované

události/anomálie. Kolektor tak přináší kompletní přehled o dění v síti a umožňuje operátorům přesně, rychle a efektivně řešit problémy v síti, zvýšit jejich bezpečnost díky detekci analýze provozu, optimalizovat síť, plánovat budoucí rozvoj a kapacitní požadavky a snížit provozní náklady.

Funkčnost kolektoru musí být možné dále rozšířit o systémy pro automatické vyhodnocování NetFlow/IPFIX dat, záchyt síťového provozu.

Modul pro detekci anomálií

Systém pro automatické vyhodnocování IP toků musí umožňovat automatickou detekci bezpečnostních nebo provozních anomálií datové sítě a jejich hlášení formou událostí. Systém musí být založen na pokročilých metodách tzv. behaviorální analýzy a umožňovat tak odhalovat hrozby a incidenty, které překonaly zabezpečení na perimetru nebo bezpečnostních ochranu koncových stanic, a pro které dosud není dostupná signatura. Jedná se tak o systém včasné detekce a reakce na bezpečností incidenty, který vhodným způsobem doplňuje stávající nástroje pro předcházení kybernetickým bezpečnostním incidentům. Detekované události musí být možné dále analyzovat, vizualizovat nebo automaticky reportovat, případně integrovat s dohledovými systémy, incident handling systémy a systémy typu SIEM. Automatická detekce bezpečnostních incidentů, anomálií provozu sítě a konfiguračních problémů musí výrazně zjednodušovat správu datové sítě, zvyšuje její bezpečnost a umožňuje proaktivně identifikovat příčiny problémů.

Modul pro záchyt síťového provozu

Systém na záchyt a analýzu síťového provozu umožňuje záznam datového provozu včetně jeho obsahu a jeho následnou analýzu, díky čemuž pomáhá s řešením provozních problémů na síti. Na základě zadaných filtračních kritérií systém provede záchyt síťového provozu. Záchyt lze následně automaticky analyzovat a interpretovat zachycené komunikace srozumitelnou formou. V případě detekce nestandardních či chybových stavů je uživateli prezentován detailní popis nastalé situace společně s doporučením jejího řešení. Systém tak významně rozšiřuje možnosti v oblasti identifikace a řešení příčin provozních a komunikačních problémů, které jdou za hranici analytických možností IP toků.

Další technická specifikace je definována v Příloze č. 5 pro danou část.

ÚVN-VoFN Praha - kybernetická bezpečnost_monitoring - nákup - software - část 3 Software pro klasifikaci dat

Specifikace funkcionalit bezpečnostní platformy pro ochranu dat
Počet uživatelů v Active Directory: 3501
Počet uživatelů pro sdílené souborové systémy, automatickou klasifikaci, alertování a automatické opravy je 2501

Přehled funkcionalit

a. Obousměrná viditelnost oprávnění
   - Podporované platformy:
     - Windows File Systém
     - SMB a NAS uložiště
     - M365 (Sharepoint Online, OneDrive, Exchange Online, MS Teams) – pouze jako možnost budoucího rošíření
   - Zobrazení uživatelů a skupin s oprávněním k určité složce.
   - Naopak zobrazení složek přístupných určitému uživateli nebo skupině.
   - Systém zobrazuje u uživatele všechny skupiny a podskupiny ve kterých se nachází.
   - V systému je na první pohled jasné, zdali daný učet je v AD, Entra ID „enable“ či „disable“.

b. Auditní záznamy (Logy)
   - Podporované platformy a potřebné moduly:
     - Active Directory
     - SMB
       - Windows File Systém
       - NetApp
       - Dell/EMC
       - HPE
       - IBM
     - M365 (Sharepoint Online, OneDrive, Exchange Online, MS Teams, Entra ID) – případné rozsíření
     - VPN, DNS, Proxy – případné rozšíření
   - Systém pro sledované servery pořizuje o každé operaci prováděné nad datovým objektem auditní záznam.
   - Systém audituje operace prováděné v samotném bezpečnostním SW. Tento údaj obsahuje informace o dané události, a především identitu účtu, který operaci vykonal.
   - V auditních záznamech nad dokumenty jsou viditelné záznamy, zdali se jedná o klasifikovaný soubor s informací o klasifikačním pravidle. Např.: dokument obsahuje rodné číslo, datum narození atp.
   - Nad auditními záznamy je možno provádět vyhledávání, filtrování a třídění.
   - Sběr dat má minimální dopad na výkonnost serveru.
   - Sběr dat je prováděn skrze agenty/služby nainstalované na jednotlivých informačních systémech nebo skrze čtení/odesílání logů.
   - Pro sběr logů z AD musí být podporováno bezagentové řešení.

c. Systém doporučení a automatické politiky pro sjednání nápravy
   - Odebírání anonymních odkazů na složky/soubory obsahující citlivé údaje.
   - Odebírání přístupových oprávnění pro celou organizaci, např. Domain Users, Everyone, Authenticated Users, …
   - Oprava nekonzistentních oprávnění na složkách.
   - Odebírání členství ve skupinách/oprávnění pro disabled uživatele.
   - Disablování nepoužívaných účtů (možnost definování doby neaktivity účtu).
   - Odebrání nepoužívaných přímých oprávnění.

   V rámci automatických politik je možnost defintovat tato nastavení:
   - Definovat rozsah (např. složka, organizační jednotka, datový zdroj, …)
   - Možnost zcela automatické nápravy nebo možnost schvalování navrhovaných oprav.
   - Možnost zobrazení navrhovaných oprav.
   - Možnost kontinuálního běhu nebo periodického spouštění oprav.
   - Možnost vrácení změn provedených automatickou opravou.

d. Centrální správa systému
   - Systém umožnuje veškerou funkcionalitu v rámci jednoho webového rozhraní.
   - Systém přehledů a sestav pro management, provozní administrátory a bezpečnostní oddělení, interní audit, compliance, DPO.
   - Možnost vytváření šablon přehledů a sestav.
   - Export vyhledávaných a filtrovaných dat.
   - Vysoce škálovatelné prostředí.
   - Centrální management disponuje možností rozdělení oprávnění pro samotné administrátory či jednotlivé role v rámci organizace. Např.: Administrátoři, auditoři, helpdesk, Data Protection Officer, Security IT atp.
   - Systém nevyžaduje dodatečné komerční licence třetích stran, např. MSSQL.

e. Identifikace vlastníků informací
   - Systém umožňuje nastavení vlastníků/garantů pro jednotlivé složky. Tyto vlastníci jsou vedeni pouze v bezpečnostním softwaru a nemají žádný dopad na vlastnictví složek z pohledu základního systému např.: Microsoft File System.
   - Složky či zdroje umožňují více vlastníků.
   - Systém umožňuje rozesílání reportů na jednotlivé vlastníky. Tím je myšleno, že systém vyhledá nad zdroji jednotlivé vlastníky, následně vygeneruje jednotlivé reporty a ty jim rozešle. Z pohledu administrace se jedná o nastavení jednoho reportu, který bude automaticky distribuován na jednotlivé vlastníky.

f. Klasifikace informací
   - Podporované platformy:
     - Windows File Systém, SMB
     - OneDrive, Sharepoint Online, MS Teams, Exchange Online
   - Systém umožňuje automaticky prohledávat nestrukturovaná data skrze regulární výrazy a textové řetězce s možností využití slovníků.
   - Systém umožňuje validaci těchto nálezů skrze matematický algoritmus např.: české rodné číslo identifikuje skrze regulární výraz. Po shodě formátu čísla provede jeho ověření skrze matematickou funkci. Tímto je zamezeno identifikování falešných rodných čísel a systém maximálně identifikuje osobní údaje.
   - Systém umožňuje kategorizaci dat na základě jejich metadat, např.: identifikace dat dle jejich formátu *.pdf, *.doc, *.cad a veškeré multimediální soubory.
   - Systém na základě klasifikování metadat umožňuje klasifikování souborů, které jsou starší než např.: 180 dní a mají velikost větší než xx a žádný uživatel s nimi nepracuje.
   - Systém umožňuje nastavení na citlivá a necitlivá klasifikační pravidla z důvodu nezkreslování výsledných reportů při klasifikaci multimediálních a starých souborů.
   - Systém umožňuje sledovat a vyhodnocovat nesrovnalosti s politikami řízení přístupu k elektronickým informacím dle jejich klasifikace. Tím je myšleno např.: Pokud jsou klasifikována personální data zaměstnanců, systém upozorňuje na nakládání s těmito daty pracovníky, kteří nejsou z personálního oddělení. Toto tzv. křížení rolí je možné individuálně nastavovat.
   - Možnost vytvářet vlastní slovníky, které budou použity při prohledávání dat.
   - Systém umožňuje nastavení negativních klíčových slov.
   - Systém umožňuje nastavení výjimek k regulárním výrazům.
   - Klasifikace dat není prováděna na zdrojových uložištích (nezatěžuje datový zdroj).
   - Výsledky klasifikace jsou zobrazeny v centrálním managementu přímo u daných složek/souborů a také u událostí v logu, tak aby na první pohled bylo zřejmé, jaké data konkrétní složka obsahuje.
   - Klasifikace umožňuje napojení na MS Sensitive Labels
   - Systém pracuje ve standardu MS Sensitive Labels.
   - Zobrazení labelů u jednotlivých souborů.
   - Možnost labely zachovat nebo soubor přelabelovat v případě nesouladu.

g. Detekce hrozeb a možnost integrace se SW třetích stran
   - Alerty umožňují reakci na zalogované události, např. změny přístupových oprávnění včetně práce s klasifikovanými dokumenty.
   - Alertní systém může být integrovaný s produkty třetích stran např. SIEM.
   - Alertní systém umožňuje vykonat akce:
     - Zaslání emailu
     - SYSLOG message
     - Event Log
     - SNMP Trap
     - Spuštění aplikace nebo skriptu

- Systém má definovatelnou strukturu výše uvedených akcí
- Systém již obsahuje předdefinovaná best practise pravidla, např.
    - Identifikace generických hrozeb typu RANSOMWARE
    - Práce s citlivými daty.
    - Nakládání s administrátorskými a dalšími privilegovanými účty.
    - Systém automaticky rozpoznává privilegované účty.
    - Hlášení anomálií chování uživatele založené na strojovém učení, vyhodnocování z pohledu jednotlivých účtů (UEBA).

h. Monitorování Microsoft Copilot – umělé inteligence (pouze rozšíření)

- Systém je napojený na korporátní AI platformu Microsoft Copilot
    - Systém zobrazuje počet komerčních licencí v rámci organizace
- Systém loguje veškeré dotazy od jednotlivých uživatelů, v rámci tohoto logu je vidět přesná otázka od uživatele a kompletní odpověď od Copilotu.
- Systém eviduje veškeré dokumenty, na které v rámci svých odpovědí odkazuje uživatele. Tím jsou myšleny dokumenty v rámci datových zdrojů.
- Systém v rámci těchto dokumentů zobrazuje informaci o jejich obsahu, tedy zobrazuje jednotlivá klasifikační pravidla.
- Systém graficky zobrazuje, které složky a soubory jsou pod rizikem vyhledávání Copilotem, zejména se jedná o citlivé informace, které jsou přístupné všem účtům v MS Active Directory či Entra ID skrze plošné skupiny.

Další technická specifikace je definována v Příloze č. 5 pro danou část.

ÚVN-VoFN Praha - kybernetická bezpečnost_monitoring - nákup - software - část 4 Software pro monitoring zranitelností

Kompletní technická specifikace je definována v Příloze č. 5 pro danou část.

Potvrzuji splnění všech technických požadavků pro ÚVN-VoFN Praha - kybernetická bezpečnost_monitoring - nákup - software - část 1 SABRA.

Ing. Irena Hýsková
Digitálně podepsal Ing. Irena Hýsková
Datum: 2025.09.09 08:22:00 +02'00'

Michal Polesný
Digitálně podepsal Michal Polesný
Datum: 2025.09.08 22:54:03 +02'00'