## Technická specifikace – software dohledového centra (SOC)

Tento dokument je souhrnem všech požadovaných systémů a činností, které musí být součástí poptávaného softwaru a jsou blíže specifikovány v jednotlivých částech této technické specifikace.

Software dohledového centra pro analýzu síťového provozu a bezpečnostní monitoring, který okamžitě identifikuje bezpečnostní rizika a události a který splňuje klíčové požadavky uvedené níže.

Při definici technických požadavků jsou všechny uvedené požadavky závazné. Je-li definice požadavku „umožňuje, lze, je možné, možnost, …“ je uvedený parametr závazný a požadovaná funkcionalita musí být v rámci produktu a jeho podpůrných systémů dodána a případně licencována. Tyto technické požadavky jsou minimálně možné, účastník zadávacího řízení (dále jen „Účastník“) může nabídnout charakteristiky (funkce) lepší.

Řešení musí splňovat **VŠECHNY** níže uvedené požadavky:

Popis nabízených komponent musí účastník zadávacího řízení zpracovat podle následujících podmínek:

* 1. Ve 2. sloupci následujících tabulek v každém řádku účastník zadávacího řízení potvrdí, že splňuje požadované technické podmínky uvedené v 1. sloupci tabulky slovem „ANO“ či jiným slovem např. „SPLŇUJE“ apod., a uvede konkrétní technickou hodnotu stěžejního nabízeného parametru a popis způsobu splnění technického požadavku, který je součástí nabízeného řešení. Z vyjádření v posledním sloupci u každého řádku musí být zřejmé, že účastník zadávacího řízení splňuje anebo překračuje požadované technické podmínky.
  2. Údaje stanovené zadavatelem v 1. sloupci tabulky nesmí být měněny, vynechány nebo jinak přeskupeny.

Pokud komentář k některému z řádků v tabulce přesáhne možnosti 2. sloupce tabulky, pak účastník zadávacího řízení uvede v příslušném řádku tabulky jen základní anotaci odpovědi a uvede zde odkaz na konkrétní číslo kapitoly a strany své nabídky obsahující podrobnější údaje.

Security Operations Center (zkráceně SOC) je specializované pracoviště, které se zabývá monitorováním a řešením bezpečnostních incidentů v reálném čase. SOC je obvykle součástí organizace a jeho hlavním cílem je zajistit bezpečnost IT infrastruktury a ochránit organizaci před různými bezpečnostními hrozbami. SOC monitoruje všechny příchozí a odchozí datové toky v organizaci, aby identifikoval potenciální bezpečnostní incidenty. Tento proces zahrnuje sběr a analýzu bezpečnostních dat z různých zdrojů, včetně firewalů, antivirových programů, IDS/IPS systémů, bezpečnostních kamer a dalších. Pokud SOC detekuje nějaký bezpečnostní incident, okamžitě se zaměří na jeho identifikaci a analýzu. Cílem je určit typ a rozsah incidentu, zdroj hrozby a jak nejlépe řešit situaci. Díky SOC je možné připravit postupy a plány pro rychlou a efektivní reakci na bezpečnostní incidenty. Tyto postupy stanovují, jak zastavit nebezpečí a minimalizovat škody.

**Hlavní role dohledového centra (SOC)**

|  |  |
| --- | --- |
| **Požadované role** | **Nabízené řešení splňuje/ nesplňuje (doplní účastník)**  **Včetně vysvětlení, jak je zadání splněno.**  **U specifikací, které mají vazbu na hodnotící kritéria dbejte na kvalitní popis požadovaných aspektů, aby bylo možno relevantně ohodnotit dodávaný produkt ve vztahu k hodnotícím kritériím uvedeným v Zadávací dokumentaci v bodě 8.1.4** |
| **Sítový dohled**  Zajištění centralizované správy, ukládání a vyhodnocování komunikačních spojení a výkonnostních parametrů datové sítě |  |
| **Bezpečnostní dohled**  zajištění správy a provozu |  |
| **Incident management**  zajištění Operátorské činnosti, Incident handling, Incident Response. |  |
| **Analýza incidentů**  zajištění odborné činnosti v detekci a lokalizaci příčin incidentů Analytikem incidentů ze strany Poskytovatele služby. |  |
| **Návrhy systematických opatření**  Sestavení opatření v organizační a technické úrovni pro posouzení Zadavatelem. |  |
| **Návrhy řešení incidentů**  zajištění odborné činnosti pro kategorizaci na interní a externí příčiny incidentů a k nim příslušných opatření. |  |
| **Reporting a analýza stavů, událostí a incidentů**  zajištění odborné činnosti pro doložení úrovně bezpečnosti vůči interním kontrolním procesům nebo pro doložení vůči externím kontrolním autoritám. |  |
| **Notifikace/Eskalace**  Informování IT techniků o vzniku bezpečnostního incidentu v reálném čase za pomocí základních komunikačních nástrojů (mail / SMS). |  |
| **Vulnerability management**  Software musí zajistit kontinuální skenování aktiv definovaných danou sítí/sítěmi a zranitelnostmi relevantními pro daná aktiva. V pravidelných intervalech. |  |
| **Technologie sběru dat**  Software kybernetického centra umožní sběr a vyhodnocení síťového provozu jako základních zdrojů dat a bude s nimi komunikovat průmyslově standardními protokoly.  Požadované řešení služby:   * zajištuje sběr, přenos a uložení logů a jejich vyhodnocování a korelaci v rámci nástroje kybernetického centra nasazeným v infrastruktuře. |  |
| **Base line analýza**  Software umožňuje porovnání neobvyklých počtů určitých událostí oproti jinému období z minulosti. |  |
| **Monitoringu a detekce**   * Real-time sledování provozu prostředí zadavatele. * Real-time analýza situace v napojených nástrojích podle skupin, kategorií zařízení a podle kontextu log záznamů nebo událostí. |  |

|  |  |
| --- | --- |
| **Požadované funkcionality/ vlastnosti** | **Nabízené řešení splňuje/ nesplňuje (doplní účastník)**  **Včetně vysvětlení jak je zadání splněno** |
| **Základní funkce**  Integrovaný systém zpracování logů a událostí z definovaných zdrojů napříč výrobci aplikací, operačních systémů a síťového hardware a sledování síťových toků a detekce anomálií |  |
| **Ovládání**  Uživatelsky přívětivý přístup ke všem komponentám systému z jednotného grafického uživatelského rozhraní (GUI). Konfigurace, definice zdrojů logů, definice korelačních pravidel, tvorba reportů, řešení událostí a další běžné operace musí probíhat z jediné řídící konzole s jednotným GUI. |  |
| **Správa prvků**  Automatické jednorázové i plánovatelné vyhledávání i ruční přidávání Prvků a detekce jejich typů a vlastností. Prvkem se rozumí hw i sw (např. OS) s IP adresou. Prvky jsou typicky zdroji dat - logů a událostí. |  |
| **Skupiny prvků**  Podpora zařazování Prvků do skupin/kategorií dle vlastností (typ, operační systém, dostupné služby, síť apod.) i metadat (umístění, hodnota apod.) |  |
| **Metadata prvků**  Možnost konfigurace metadat Prvků - min. hodnota, priorita a spolehlivost (věrohodnost) událostí |  |
| **Monitorování prvků**  Automatické monitorování stavu Prvků - min. dostupnost poskytované služby a základní dostupnost (odezva na ping) |  |
| **Vyhledávání prvků**  Víceparametrové vyhledávání a filtrování Prvků podle vlastností i metadat, export do souboru v běžném strojově zpracovatelném formátu (např. csv, pdf apod.) |  |
| **Detekce zranitelností**  Automatická ruční i plánovaná detekce zranitelností Prvků (i nezařazených) - porovnání stavu Prvků s databází známých zranitelností průběžně aktualizovanou výrobcem |  |
| **Profily zranitelností**  Vestavěné i uživatelsky definované profily detekce zranitelností - definice typů zranitelností, které mají být kontrolovány. |  |
| **Autentizované detekce zranitelnosti**  Podpora detekce zranitelností s přihlášení (autentizací) ke kontrolovanému Prvku. |  |
| **Detekce průniku**  Víceúrovňová detekce průniku (intrusion detection) - min. na úrovni sledování síťového provozu a na úrovni Prvků. |  |
| **Detekce průniku – Aktiva**  Monitoring a analýza uživatelských aktivit, logů, integrity souborů a registrů, rootkitů či obdobného škodlivého kódu. |  |
| **Detekce průniku – Síť**  Analýza monitorovaných síťových toků a detekce anomálií indikující možné narušení bezpečností politiky (NBA - Network Behavior Analysis) |  |
| **Detekce prolomení hesel**  Testování prolomení uživatelských a administrátorských hesel v pravidelných intervalech. |  |
| **Síťové toky – Hypervisor**  Podpora sledování síťových toků (netflow či kompatibilní) virtuálních síťových přepínačů Hyper-V |  |
| **Viditelnost síťového provozu**  zobrazení, prohledávání, filtrování síťových toků včetně historie. |  |
| **IP reputace**  Integrovaná služba aktualizovaná výrobcem ohodnocující reputaci a spolehlivost veřejné IP adresy s možností změny priorit událostí, alarmů apod. Reputace založena na detekovaných aktivitách IP adresy (spam, skenování, phishing, distribuce malware, botnet apod.) |  |
| **Ukládání logů**  Bezpečné ukládání logů s řízeným přístupem v nezměněné (nefiltrované) podobě (tzv. raw logy) |  |
| **Zpracování logů**  Centrální zpracování logů, jejich normalizace, korelaci, grafická interpretace a archivace, včetně logů generovaných samotným řešením. |  |
| **Prohledávání logů**  Pokročilé prohledávání a filtrování raw logů, podpora indexování pro zrychlení hledání. |  |
| **Expirace logů**  Podpora automatické rotace raw logů s nastavením doby expirace. |  |
| **Zálohování logů**  Podpora zálohování logů na dodané externí síťové úložiště „on-premise“ i cloud. |  |
| **Ochrana logů**  Zajištění integrity raw logů aplikací digitální podpisu. Možnost jednoduchého uživatelského ověření integrity. |  |
| **Centralizace logů**  Konsolidace logů na jednom centrálním místě. |  |
| **Geolokace**  Automatické doplňování geolokačních informací k událostem a jejich grafické znázornění na mapě. |  |
| **Doplňování názvů**  Automatické doplňování reverzních DNS a hostname záznamů k IP adresám. |  |
| **Grafy událostí**  Grafické znázornění událostí - četnost, typ, časová osa. |  |
| **Parsery**  Možnost vytváření uživatelských parserů bez nutnosti externí spolupráce. |  |
| **Standardizace logů**  Standardizace přijatých logů do jednotného formátu, parsování parametrů do předepsaných polí. |  |
| **Dashboardy**  Předpřipravené pohledy a podpora vytváření vlastních pohledů na data uživateli a jejich ukládání pro pozdější využití a zpracování dat. Včetně grafické reprezentace dat - grafy, mapy apod. |  |
| **Reporty**  Integrovaný reportovací nástroj s přednastavenými reporty (uživatelská aktivita, konfigurační změny, přístupy, bezpečnostní události) a možností vlastních úprav a vytvoření nových reportů. Včetně grafické reprezentace dat - grafy, mapy apod. Reporty bude možno generovat jak na základě manuálního spuštění, tak automatizovaně. |  |
| **Upozornění**  Zasílání uživatelsky vytvořených upozornění podle uživatelsky definovaných podmínek. Možnost zahrnutí přijatých rozparsovaných dat do upozornění. |  |
| **Správa uživatelů**  Správa uživatelů systému musí být integrovatelná s MS Active Directory/LDAP nebo AAD. Systém musí umožňovat i přihlašování pomocí lokálních účtů. Podpora granulárního (lokálního) nastavení uživatelských oprávnění. |  |
| **Politiky**  Podpora vestavěných a tvorby vlastních komplexních politik zpracování událostí. Politiky musí umožnit spustit minimálně následující akce: odeslání emailu, odeslání sms, spuštění skriptu. |  |
| **Korelace**  Podpora korelací události na základě definovaných parametrů bez závislosti na typu zdroje. Vestavěné a výrobcem aktualizované korelace (v řádech tisíců), podpora vytváření vlastních. |  |
| **Rozšířené korelace**  Systém musí umožňovat tvorbu korelací nejen napříč zdroji, ale také napříč daty z interních subsystémů (např. detekce zranitelnosti, průniků, IP reputace). V závislosti na datech interních subsystémů je případně upravena vážnost incidentu (oproti standardní korelaci). |  |
| **Vyhledávání**  Fulltextové vyhledávání minimálně nad archivními daty. |  |
| **Škálovatelnost**  Možnost zvýšení výkonu doplněním dalších appliance pro sběr dat a vykovávání funkcí systémů, popřípadě rozdělením systému na více serverů. |  |
| **Integrace**  Možnost komunikace se systémy třetích stran např. - standardizované API, podpora skriptování. |  |

## Požadavky na funkcionality systému kybernetického centra

|  |  |
| --- | --- |
| **Systém pro sběr, analýzu a korelaci**  Systém pro sběr, analýzu a korelaci logů napříč všemi monitorovanými zdroji s možností napojit přímo i nepodporovaný zdroj pomoci standartních protokolů. |  |
| **Skenování zařízení**  Aktivní a pasivní skenování zařízení v definovaných IP rozsazích pro zjišťování nových a neznámých zařízení v sítí (asset discovery) |  |
| **Operační systémy**  Systém musí umožňovat skenování zranitelností u podporovaných zdrojů (minimálně Windows/Linux). |  |
| **Network IDS**  Systém musí obsahovat Network IDS (Výkon min. 100 Mbps), Host IDS a dále také File Integrity Monitoring. |  |
| **Základní analýza datových toků**  Musí umožňovat základní analýzu datových toků podporovaných síťových zařízení. |  |
| **Kontrola dostupnosti**  Systém musí obsahovat kontrolu dostupnosti služeb u podporovaných operačních systémů (minimálně windows/linux) |  |
| **Notifikace**  Systém musí umožňovat na základě vytvořených korelačních událostí vytvářet:   * alerty * mailové notifikace * spouštět skripty * sms notifikace |  |
| **Jednotná konzole**  Všechny uvedené funkce musí být přístupné a spravovatelné z jedné konzole |  |
| **Provoz řešení**  Řešení musí zahrnovat v ceně dodávky veškeré náklady spojené s provozem celého řešení. |  |
| **Možnost automatizovaného reportingu**  Možnost vytváření automatizovaných manažerských reportů o stavu kybernetické bezpečnosti z pohledu zprávy kybernetických incidentů ideálně dle oblastí jejich vzniků (např.: doména, web, email apod.).  Je požadováno vytváření reportů v českém jazyce. |  |

|  |  |
| --- | --- |
| **Ukládání a vyhledávání aplikačních metadat**  Systém musí být schopen ukládat a následně vyhledávat aplikační metadata (vždy dotaz i odpověď všech transakcí v toku) minimálně z následujících protokolů, které jsou nebo mohou být využívány ve vnitřní síti organizace: FTP, FTP-DATA, TFTP, TFTP-DATA, SSH, Telnet, SMTP, SMTPS, DNS, DHCP, HTTP, HTTPS, NTP, SMB, SNMP, LDAP, NFS, MS-SQL, SIP, Kerberos, SSL/TLS, ARP, MODBUS.  V rámci metadat u HTTP, SMTP, SMB a NFS je požadováno ukládání informací o po síti přenášených souborech alespoň v rozsahu:   * název souboru, * velikost souboru,   HASH souboru. |  |
| **Monitoring výkonu aplikací a sítě**  Systém v celé monitorované síti, mezi všemi zařízeními a na všech službách měří a vytváří automaticky (bez nutnosti nastavovat manuálně limitní hodnoty nebo jiné parametry) model normálního chování pro výkonnostní parametry minimálně:   * přenosová rychlost sítě, * rychlost odezvy aplikace, * odezva systému z pohledu uživatele, * informace o retransmission a out of order paketech.   Výkonnostní anomálie na jednotlivých zařízeních a jejich službách jsou reportovány uživateli. |  |
| **Zaznamenávání a ukládání plného provozu**  Je požadováno volitelné nahrávání plného síťového provozu (full packet capture) na všech dodaných zařízeních minimálně na základě parametrů: cílová a zdrojová IP/MAC adresa, podsíť, využitý protokol, IPv4 nebo IPv6. |  |
| **Jednotné grafické rozhraní**  Systém musí poskytovat jednotné grafické uživatelské rozhraní pro veškerou práci uživatelů, včetně všech detekcí, analýzy síťových statistik, nastavení systému, konfiguraci alertů, reportů a dashboardů. |  |

|  |  |
| --- | --- |
| **Monitorování zařízení, segmentů sítě a využívaných síťových služeb**  Dodaný systém musí identifikovat všechna zařízení připojená do sítě včetně koncových zařízení, serverů, IoT zařízení apod. Zároveň musí být systém schopen identifikovat změny v síti – minimálně:   * změna IP/MAC adresy hosta, * duplicitní IP/MAC adresa, * změna VLAN, * vytvoření nové podsítě, * připojení nového zařízení, * použití nové služby, * nedostupnost dříve dostupné a komunikující služby nebo dříve dostupného a komunikujícího zařízení, * přístup nového zařízení ke službě či zařízení.   Systém musí uživateli umožnit pomocí těchto detekčních metod nastavovat bezpečnostní politiky pro různé segmenty sítě a pro různá zařízení a na porušení těchto politik reagovat upozorněním. |  |
| **Detekce síťových služeb**  Systém musí být schopen detekovat síťové služby na základě síťových metadat získaných prostřednictvím DPI (Deep Packet Inspection), nikoliv pouze čísla portu. |  |
| **Samostatné učení behaviorálních aktivit a detekce anomálií**  Systém musí používat matematické metody samostatného učení pro analýzu síťové aktivity, musí vytvářet a v čase automaticky modifikovat modely chování na základě běžného chování jednotlivých zařízení a na nich provozovaných služeb v rámci celé organizace.  Systém musí mít schopnost na základě modelu daného zařízení a jeho služeb identifikovat nestandardní síťové chování, a to zejména:   * odchylku od modelu pro přenos dat, toků a paketů, * odchylku od modelu pro počet komunikačních partnerů a entropie na komunikačních portech, * odchylku od modelu pro počet síťových toků a využitých síťových služeb, * odchylku od modelu výkonnosti sítě (rychlost přenosu) a aplikací (doba odezvy).   Samostatné učení je požadováno na všech síťových zařízeních a na nich provozovaných službách (port číslo 0 až 65535 u TCP i UDP) na IPv4 a IPv6 a dalších protokolech L3 a L4 síťové vrstvy. |  |
| **Identifikace neznámých hrozeb, podezřelých chování na síti a porušení politik**  Systém musí být schopen detekovat neznámé hrozby, které nelze identifikovat prostřednictvím detekčních signatur, jako jsou trojské koně, botnety apod.  Zejména musí být identifikovány tyto příznaky potenciálně škodlivého chování:   * průzkumné aktivity v síti, * potenciální úniky dat, * detekce podezřelého strojového chování, které nevytvářejí lidští uživatelé sítě, * detekce repetitivních vzorců chování na síti, * detekce botnetů a ovládání kompromitované stanice, * detekce příznaků těžení kryptoměn, * útoky hrubou silou a enumerace dat, * rozpoznání tunelovaného síťového provozu – alespoň IPv4 prostřednictvím IPv6 a DNS tunely. |  |
| **Detekce na základě databáze známých hrozeb (signaturní detekce)**  Systém musí být schopen identifikovat a reportovat události na základě detekční databáze malware, známých útoků a zranitelností, porušení bezpečnostních pravidel a „best practices“ a dalších rizik. Tato databáze musí být aktualizovaná minimálně na hodinové bázi. Nesmí se jednat o volně dostupnou/open-source databázi, ale musí se jednat o komerční databázi renomovaného výrobce nebo poskytovatele těchto služeb.  Databáze detekčních pravidel (signatur) musí být založena na pokročilých regulárních výrazech pro zpracování řetězců, které dokáží provádět inspekci veškeré síťové komunikace od L2 (Ethernet apod.) po L7.  Systém musí využívat tuto signaturní detekci pro veškerý monitorovaný provoz (na perimetru i v interní síti mezi všemi segmenty), nikoliv pouze pro omezený segment nebo podmnožinu celkové komunikace.  Systém musí detekovat události na základě vysokého počtu signaturních pravidel (minimálně několik desítek tisíc).  Uživatel musí být schopen přidávat vlastní detekční pravidla v praktickém a obecně využívaném formátu. |  |
| **Analýza šifrované komunikace**  Vedle samostatného učení musí systém používat další metody pro analýzu šifrované komunikace, minimálně TLS fingerprinting a s ní spojenou detekci známých hrozeb. |  |
| **Kontrola platnosti certifikátů**  Ověřování platnosti interních certifikátu pro validní TLS šifrování u HTTPS a upozornění před datem jejich vypršení. |  |
| **Asistované učení a korelace událostí**  Systémmusí být schopen korelace jakýchkoliv detekovaných událostí ze všech detekčních metod a úpravy samostatného učení a dalších detekčních metod tak, aby byly v maximální míře eliminovány falešné alarmy. Systém musí být schopen eliminovat falešné alarmy i pro události detekované v historii.  Systém musí být schopen zobrazovat zařízení podle souhrnné kritičnosti identifikovaných událostí – minimálně v rozsahu kritické, důležité a střední. |  |
| **Aktuální databáze blacklistů**  Systém musí být schopen hodnotit IP adresy, se kterými komunikují vnitřní hosté v sítí prostřednictvím minimálně denně aktualizovaných reputačních databází. Uživatel musí být schopen importovat vlastní reputační databáze. |  |