|  |
| --- |
| Příloha 1.1.1 Technické specifikace: „Funkční a nefunkční požadavky částí plnění veřejné zakázky“ |
| **„****Modernizace a rozšíření bezpečnostní infrastruktury Kanceláře veřejného ochránce práv“** |
| **Dále též jen „Veřejná zakázka“** |
| **Zadavatel:** |
| **Kancelář veřejného ochránce práv**  Údolní 658/39  602 00, Brno |

**OBSAH:**

[1. Firewall 2](#_Toc173770077)

[2. NDR Systém 4](#_Toc173770078)

[3. EDR Systém 7](#_Toc173770079)

[4. Log Management Systém 12](#_Toc173770080)

[5. PAM Systém 13](#_Toc173770081)

[6. SIEM Systém 13](#_Toc173770082)

[7. Svolávací Systém SAIW (Systém Automatizace incidenčních workflow) 13](#_Toc173770083)

[8. SOC (Security Operation Centrum) 14](#_Toc173770084)

# Firewall

Zadavatel požaduje dodání nástroje Firewall, který nahradí stávající Firewall Kernun, který zadavatel v současnosti používá v provedení HW appliance, která je již za morální dobou udržitelnosti.

V rámci výběrového řízení požadujeme dodat řešení Firewall, které umožní snadný přechod ze stávajícího řešení Firewall Kernun zapojený v režimu HA (High Availability).

Budou dodány 2 centrální firewally, ve formě HW Appliance, které budou propojeny klastru dvou výkonných centrálních firewallů.

**Požadujeme dodat licence potřebné k provozu FW v HA režimu po dobu 5 let**

**Požadujeme dodání řešení vč. supportu/servisní podpory na dobu 5 let. Podpora musí zahrnovat všechny updaty i upgrady, telefonická nebo emailová podpora výrobce v rozsahu alespoň 8x5 (8-16 hod., po-pá).**

Řešení firewall zajistí tyto funkční a nefunkční požadavky:

| **ID** | **Název požadavku** | **Popis požadavku** |
| --- | --- | --- |
| FW01 | Základní funkce | 2 centrální firewally, ve formě HW Appliance umožní:   * poskytování HA (High Availability = vysoká dostupnost) * terminování zabezpečených spojení, * správu bezpečnostních politik, * správu MFA (multifaktorová autentizace) |
| FW02 | Základní požadavek na implementaci | Implementace vč. uvedení do pilotního provozu bude obsahovat tyto aktivity:   * Přenesení komplexních FW pravidel (bezpečnostních politik) a nastavení ze starých FW na nové FW; * Aktualizace dokumentace, školení uživatelů; * Vyhodnocení pilotního provozu a realizace nápravných opatření. |
| FW03 | Analýza síťového provozu | Firewall musí provádět analýzu síťového provozu v reálném čase k identifikaci potenciálních hrozeb a anomálií. |
| FW04 | Systém detekce útoků | Firewall musí obsahovat systém detekce útoků (IDS), který dokáže detekovat a zabránit neoprávněným pokusům o přístup. |
| FW05 | Filtrace na úrovni aplikace | Firewall musí být schopen filtrovat a řídit provoz na základě protokolů a atributů aplikací. |
| FW06 | Podpora virtuálních soukromých sítí (VPN) | Firewall musí podporovat připojení pomocí virtuálních soukromých sítí (VPN) pro bezpečný vzdálený přístup. |
| FW07 | Autentizace uživatelů | Firewall musí poskytovat mechanismy autentizace uživatelů, aby bylo zajištěno, že pouze autorizovaní uživatelé mají přístup do sítě. |
| FW08 | Filtrace obsahu | Firewall musí mít schopnost filtrovat obsah a blokovat přístup k nevhodným nebo škodlivým webovým stránkám. |
| FW09 | Řízení provozu | Firewall musí umožňovat řízení přístupu k webovým stránkám na základě příslušnosti přihlášeného uživatele koncové stanice do doménových skupin. |
| FW10 | Ochrana provozu | Firewall musí disponovat systémem detekce nebezpečných spojení s napojením na databázi známých a lokálně významných nebezpečných IP adres. |
| FW11 | Systém odchytávání útoků | Firewall musí disponovat systémem pro detekci podezřelých spojení (Honeypot) pomocí TCP handshaku na zvoleném seznamu portů a adres. |
| FW12 | Rozšiřitelnost | Firewall musí umožňovat propojení vícero rozhraní do jednoho (agregace) pro případ nutnosti navýšení propustnosti nebo zvýšení robustnosti. |
| FW13 | Vzdálený servisní zásah | Firewall musí poskytovat zabezpečený způsob připojení ze sítě dodavatele, nedostupný z veřejného internetu, pro případ nutnosti zásahu servisního týmu. |
| FW14 | Řízení adresace | Firewall musí poskytovat systém řízení adresace interní sítě pomocí DHCP serveru. |
| FW15 | Kontrola DNS | Firewall musí poskytovat systém překladu doménových jmen (DNS) pro poskytování klientům interní sítě. |
| FW16 | Doménová jména | Firewall musí podporovat zadávání pravidel provozu na webové servery pomocí doménových jmen. Firewall musí pro taková pravidla podporovat tzn. hvězdičkovou notaci (např. \*.google.com). |
| FW17 | Paralelní verze | Firewall musí umožňovat instalaci více verzí firmwaru zároveň s možností bezztrátového návratu k předchozí verzi firmware. |
| FW18 | Bezpečnostní komunita | Firewall musí být zapojen do komunitního systému ochrany dodavatele, který umožní sdílení informací o bezpečnostních hrozbách. |
| FW19 | Škálovatelnost | Firewall musí být snadno škálovatelný, aby se mohl přizpůsobit růstu sítě a zvýšenému provozu. |
| FW20 | Vyvažování zátěže | Firewall musí podporovat techniky vyvažování zátěže pro rovnoměrné rozložení síťového provozu a prevenci úzkých míst. |
| FW21 | Vysoká dostupnost | Firewall musí mít vysokou dostupnost, minimalizovat výpadky a zajišťovat nepřetržitou ochranu sítě. |
| FW22 | Tolerance vůči chybám | Firewall musí být navržen s mechanismy pro toleranci vůči chybám a minimalizaci dopadu hardwarových nebo softwarových poruch. |
| FW23 | Zálohování a obnova | Firewall musí poskytovat mechanismy pro pravidelné zálohování a obnovu pro ochranu konfigurace a dat. |
| FW24 | Šifrování dat | Firewall musí podporovat silné protokoly pro šifrování dat, aby ochránil citlivé informace při přenosu. |
| FW25 | Detekce proniknutí | Firewall musí mít schopnost detekovat a monitorovat potenciální pokusy o neoprávněný přístup. |
| FW26 | Auditování a záznamování | Firewall musí generovat audity a poskytovat komplexní funkcionalitu pro záznamování pro účely dodržování předpisů a forenzní analýzy. |
| FW27 | Ochrana proti přehřátí | Firewall musí zajistit ochranu proti přehřátí. Informovat o tomto stavu a zajistit ochranu proti vnitřnímu přehřátí. |
| FW28 | Snadná konfigurace | Firewall musí mít uživatelsky přívětivé rozhraní a intuitivní možnosti konfigurace pro snadné spravování a nastavení. |
| FW29 | Vzdálené monitorování a správa | Firewall musí podporovat možnosti vzdáleného monitorování a správy pro efektivní správu distribuovaných prostředí. |
| FW30 | Uživatelské rozhraní | Firewall musí mít dobře navržené a intuitivní uživatelské rozhraní pro efektivní monitorování a administraci. |
| FW31 | Integrace s existujícími systémy | Firewall musí bezproblémově integrovat s existující infrastrukturou sítě a bezpečnostními systémy. |
| FW32 | Podpora standardních protokolů | Firewall musí podporovat standardní síťové protokoly pro bezproblémovou komunikaci s dalšími zařízeními a systémy. |
| FW33 | Výkon | * Výkon IPS – min. 5 Gbps vč. logování * Výkon Threat Protection – min. 3 Gbps vč. logování * IPsec VPN výkon (512 bytů) - min. 5 Gbps vč. logování * SSL-VPN výkon - min. 2 Gbps vč. logování * Současná TCP spojení – min. 2 500 000 * Nová spojení za sekundu (TCP) – min. 200 000 |
| FW34 | HW požadavky | * Rozhraní – min. 10x1 GE RJ45, možnost rozšíření o min. 4x10 SFP+ další sítová rozhraní * Management rozhraní - min 1 Gbe RJ45 * Uložiště - integrovaný pevný disk, minimálně 480GB |
| FW35 | Jazyk | Uživatelské rozhraní firewallu musí být dostupné kompletně v Českém jazyce, a to včetně všech dokumentačních materiálů. |

# NDR Systém

Zadavatel požaduje dodání nástroje Netflow/NBAD, který nahradí stávající řešení Netflow /NBAD. Monitoring NetFlow a vyhodnocení anomálií v síti je v současnosti realizováno prostřednictvím nástroje od společnosti Flowmon. Je pořízena jedna sonda 4x1 GbE CU s vestavěným kolektorem a instalovaným Anomaly Detection Systémem:

Předmětem plnění v této části budou tyto základní komponenty a parametry:

* 1 ks Monitorovací sonda s kapacitou 1 x 10 Gbps Ethernet (rozhraní SFP+) ve formě hardware appliance (včetně transceiver modulu pro SFP+)
* 1ks Kolektor s diskovou kapacitou 1 TB a výkonem až 75 000 flows/s ve formě hardware appliance
* Systém ADS s výkonem 1 000 flows/s provozovaný v rámci kolektoru nebude tudíž zatěžovat server

**Požadujeme dodání řešení vč. supportu/servisní podpory na dobu 5 let. Podpora musí zahrnovat všechny updaty i upgrady, telefonická nebo emailová podpora v rozsahu alespoň 8x5 (8-16 hod., po-pá).**

Řešení NDR zajistí tyto funkční a nefunkční požadavky:

| **ID** | **Název požadavku** | **Popis požadavku** |
| --- | --- | --- |
| NDR01 | Shoda se standardy | * Podpora standardů NetFlow v5, NetFlow v9, IPFIX pro export i příjem statistik o síťovém provozu v souladu s příslušnými RFC pro dané standardy * Podpora pro spolehlivý a bezpečný přenos dat ve formátu IPFIX mezi sondami a kolektorem v souladu s RFC 7011 * Podpora pro nastavení času aktivní a neaktivní expirace toků (RFC 3954). * Události je možné automaticky exportovat do systémů typu log management nebo SIEM prostřednictvím protokolu syslog ve standardizovaném formátu CEF * Systém nabízí REST API, které pokrývá přístup k datům i konfiguraci. REST API je plnohodnotně dokumentované a oficiálně podporované výrobcem |
| NDR02 | Obecné požadavky na monitorování | * Monitorování v pasivním režimu (SPAN/TAP) a aktivním režimu (GRE/ERSPAN). * Monitorování MAC adres * Monitorování VLAN tagů. |
| NDR03 | Monitorování výkonnostních parametrů sítě: | * round trip time, * server response time, * TCP retransmise. |
| NDR04 | Monitorování odezvy aplikací | * Pro protokoly http, HTTPS * Pro MS SQL, Pstgre SQL a My SQL |
| NDR05 | Monitorování odezvy aplikací | V rámci monitorování odezvy aplikací jsou k dispozici následující metriky:   * network transport time (doba přenosu požadavku a odpovědi), * application response time (odezva aplikační transakce). |
| NDR06 | Monitorování výkonu a odezvy aplikací proti definovanému SLA | Systém umožní monitorovat skutečnou odezvu aplikací z pohledu uživatele, tj. monitorovat transakce jednotlivých uživatelů v reálném čase bez nutnosti instalovat softwarové agenty na servery nebo koncové stanice. Systém umožňuje pro každou aplikaci, resp. i její část definovat SLA pro dobu odezvy. Systém kontinuálně vyhodnocuje všechny uživatelské transakce a stanovuje celkový index výkonu aplikace na základě plnění SLA |
| NDR07 | Identifikace a extrakce metadat | * z aplikačního protokolu http * z aplikačního protokolu SSL/TLS vč. TLS 1.3. * z aplikačního protokolu DNS * aplikačního protokolu DHCP * aplikačního protokolu SMTP |
| NDR08 | Exporty statistik | Uživatelsky definované šablony pro export statistik o síťovém provozu ve formátu IPFIX |
| NDR09 | Vizualizace statistik | * Vizualizace statistik o provozu datové sítě v 5 minutových, 1 minutových nebo 30 sekundových intervalech, * Zobrazování výkonnostních metrik v grafech * Systém umožňuje zpracovávat dotazy na dlouhé časové intervaly s délkou minimálně 1 měsíc * Systém umožňuje agregovat síťové statistiky podle libovolných atributů a sumarizovat podle různých kritérií * Susystém poskytuje mu souhrnné informace o nejvýznamnějších událostech, nových incidentech (nebyly zaznamenány v předchozím období), rizikových stanicích a trendech. * Systém podporuje pokročilé dashboardy s libovolným počtem pohledů na data. Uživatel může sdílet dashboard s dalšími uživateli |
| NDR10 | Detekce útoků | Systém nabízí funkcionalitu detekce útoků, bezpečnostních incidentů a anomálií kombinací tradičního IDS pro identifikaci známých útoků a hrozeb základě signatur s moderní behaviorální analýzou pro detekci neznámých/nových útoků na základě analýzy chování. |
| NDR11 | Threat intelligence | Výrobce poskytuje automatické, pravidelné aktualizace databáze známých indikátorů kompromitace (tzv. threat intelligence) a databáze signatur. |
| NDR12 | Záchyt provozu | Na základě události je možné automaticky spustit záchyt provozu v plném rozsahu. Záchyt provozu je cílený |
| NDR13 | Reporting | Systém nabízí předdefinovanou sadu reportů s možností plné konfigurace uživatelem. Reporty jsou obsahově ekvivalentní s dashboardy a umožňují zobrazit veškeré informace, které je možné zobrazit na dashboardu. Reporty jsou dostupné prostřednictvím webového uživatelského rozhraní, ve formátu PDF nebo CSV |
| NDR14 | Autentizace uživatelů | Systém nabízí integraci LDAP/AD pro autentizaci a autorizaci uživatelů. V rámci konfigurace je možné prostřednictvím uživatelského rozhraní manuálně mapovat skupiny v rámci LDAP/AD na role v systému |
| NDR15 | Zálohování a obnova logů o aktivitě na síti | * K řešení je možné připojit standardizované datové úložiště (např. Samba, NFS, S3). * Objem zálohovaných dat není licenčně omezen a je limitován pouze kapacitou úložiště. * Data, která jsou předmětem zálohování je možné definovat pomocí libovolné kombinace atributů záznamů o síťovém provozu. Takových definic je možné vytvořit větší počet, bez explicitního omezení. * Zálohování dat probíhá pravidelně, minimálně jednou za 24 hodin. * Zálohovaná data je možné v případě potřeby obnovit tak, aby tato data bylo možné analyzovat standardními prostředky řešení identicky jako data, která jsou standardně v systému dostupná. |
| NDR16 | Podpora pro FlowLogs | Systém musí být připravený na monitoring datového provozu v prostředí AWS nebo Azure s využitím technologie tzv. FlowLogs. Požadována je nativní podpora pro VPC FlowLogs v případě AWS a NSG FlowLogs v případě Azure. |
| NDR17 | Pokročilé zpracování flow dat | Systém umožní přijímat data ve formátu NetFlow/IPFIX z vlastních senzorů. Tato data je následně možné předávat do systémů třetích stran včetně duplikace, filtrování a konverze formátu. |
| NDR18 | Modelování topologie | Systém umožní vytvářet libovolné logické nebo fyzické topologie a na tyto topologie mapovat síťový provoz, resp. libovolně filtrovaný síťový provoz. Účelem je modelovat a vizualizovat prostředí datové sítě, význačné systémy a zobrazovat jejich síťový provoz a vytížení |
| NDR19 | Záchyt provozu s krátkodobým bufferem | Nabízené řešení umožňuje selektivní záznam datového provozu v plném rozsahu ve formátu PCAP pro následnou analýzu. Zároveň je k dispozici krátkodobá paměť pro datový provoz, který bezprostředně předcházel spuštění záchytu provozu. Záchyt je integrován se systémem detekce anomálií a umožňuje v případě signifikantní detekce provoz automaticky zaznamenat |
| NDR20 | Automatická analýza záchytů provozu ve formátu PCAP | Nabízené řešení umožňuje automaticky analyzovat obsah záchytu provozu ve formátu PCAP s cílem identifikovat příčiny provozních a výkonnostních problémů bez nutnosti manuální analýzy v nástroji třetí strany a bez specifických znalostí v oblasti paketové analýzy |

# EDR Systém

Zadavatel požaduje nástroj který je určen pro detekcí pokročilých hrozeb a rozšiřuje nebo nahrazuje standardní antivirová řešení (AV), která tyto hrozby dnes plně nepokrývají. Detekuje pokročilé typy hrozeb na základě setrvalého monitoringu na koncových zařízeních. Vyhodnocuje nezvyklé chování a pokusy o napadení systému hackery prostřednictvím identifikátorů kompromitace. Dále umožňuje reagovat na vzniklé hrozby prostřednictvím automatizované reakce a zabránit útočníkovi v hlubším průniku do infrastruktury. V rámci provozního prostředí EDR zvýší schopnosti detekce hrozeb na koncových stanicích a serverech a reakce na ně.

jako součást řešení EDR je požadováno i řešení MFA autentizace uživatelů. Součástí řešení musí být i schopnosti detekce hrozeb na základě klasického antivirového skenování. Požaduje se tedy EDR + AV + MFA. EDR bude provozováno na virtuálních prostředcích zadavatele.

**Požadovaný počet licencí je minimálně 250.**

**Požadujeme dodání řešení vč. supportu/servisní podpory na dobu 5 let. Podpora musí zahrnovat všechny updaty i upgrady, telefonická nebo emailová podpora výrobce v rozsahu alespoň 8x5 (8-16 hod. po-pá).**

Řešení EDR zajistí tyto funkční a nefunkční požadavky:

## Požadavky na ANTIVIR

| **ID** | **Popis požadavku** | |
| --- | --- | --- |
| AV01 | Podporované klientské platformy | Podporované jsou min.: Windows, Linux, MacOS, Android, vše v českém jazyce |
| AV02 | Nativní podpora architektur pro platformy Windows a MacOS: | Podporované jsou x86, x84, ARM64 |
| AV03 | Rozsah funkcionalit | Antimalware, antiransomware, antispyware a anti-phishing pro aktivní ochranu před všemi typy hrozeb. Dále IPS, Application control, Device control, Security Memory (zabraňuje útokům na běžící aplikace), kontrola integrity systémových komponent. Dále ochrana proti pokročilým hrozbám (APT) a zero-day zranitelnostem |
| AV04 | Personální firewall | Součástí řešení je i personální firewall pro zabránění neautorizovanému přístupu k zařízení se schopností automatického přebrání pravidel z brány Windows Firewall. |
| AV05 | Ochrana operačního systému | Součástí řešení je i Modul pro ochranu operačního systému a eliminaci aktivit ohrožující bezpečnost zařízení s možností definovat pravidla pro systémové registry, procesy, aplikace a soubory. |
| AV06 | Implementované ochrany | Součástí řešení je i ochrana před neautorizovanou změnou nastavení / vyřazení z provozu / odinstalací antimalware řešení a kritických nastavení a souborů operačního systému. |
| AV07 | Heuristická analýza | Součástí řešení je i aktivní i pasivní heuristická analýza pro detekci dosud neznámých hrozeb. |
| AV08 | Ochrana proti zero-day zranitelnostem | Součástí řešení je i systém pro blokaci exploitů zneužívajících zero-day zranitelností, jenž pokrývá nejpoužívanější vektory útoku:   * síťové protokoly, * Flash Player, * Javu, * Microsoft Office, * webové prohlížeče, * e-mailové klienty, * PDF čtečky… * Systém pro detekci malwaru již na síťové úrovni poskytující ochranu i před zneužitím zranitelností na síťové vrstvě. * Kontrola šifrovaných spojení (SSL, TLS, HTTPS, IMAPS…). |
| AV09 | Anti-phishing | Součástí řešení je i anti-phishing se schopností detekce homoglyph útoků. |
| AV10 | Kontrola RAM paměti | Součástí řešení je i kontrola RAM paměti pro lepší detekci malwaru využívající silnou obfuskaci a šifrování. |
| AV11 | Kontrola souborů | Součástí řešení je i:   * Cloud kontrola souborů pro urychlení skenování fungující na základě reputace souborů. * Kontrola souborů v průběhu stahování pro snížení celkového času kontroly * Kontrola souborů při zapisování na disku a extrahování archivačních souborů |
| AV12 | Heuristická analýza | Součástí řešení je i detekce hrozeb a zranitelností s využitím strojového učení. |
| AV13 | Ochrana proti botnetu | Součástí řešení je i funkce ochrany proti zapojení do botnetu pracující s detekcí síťových signatur. |
| AV14 | Ochrana před síťovými útoky | Součástí řešení je i ochrana před síťovými útoky skenující síťovou komunikaci a blokující pokusy o zneužití zranitelností na síťové úrovni. |
| AV15 | Kontrola aplikací | Součástí řešení je i kontrola s podporou cloudu pro odesílání a online vyhodnocování neznámých a potenciálně škodlivých aplikací. |
| AV16 | Lokální sandbox | Součástí řešení je i lokální sandbox |
| AV17 | Behaviorální analýza | Součástí řešení je i modul behaviorální analýzy pro detekce chování nových typů ransomwaru. |
| AV18 | Systém reputace | Součástí řešení je i systém reputace pro získání informací o závadnosti souborů a URL adres. |
| AV19 | Detekce nového mallwaru | Součástí řešení je i cloudový systém pro detekci nového malwaru ještě nezaneseného v aktualizacích signatur |
| AV20 | Úvodní skenování | Součástí řešení je i skener firmwaru, BIOSu a UEFI |
| AV22 | Skenování souborů v cloudu OneDrive. | Součástí řešení je i skenování souborů v cloudu OneDrive. |
| AV23 | Funkcionalita pro klienty | * MS Windows – Antimalware, Antispyware, Personal Firewall * MacOS – Personal Firewall, Device control, autoupgrade. |
| AV24 | Bezpečnostní politiky | Součástí řešení je i možnost aplikování bezpečnostních politik i v offline režimu na základě definovaných podmínek. |
| AV25 | Automatické vytváření dump souborů | Součástí řešení je i podpora automatického vytváření dump souborů na stanici na základě nálezů. |
| AV26 | Okamžité blokování/mazání napadených souborů | Součástí řešení je i okamžité blokování/mazání napadených souborů na stanici (s možností stažení administrátorem k další analýze). |
| AV27 | Duální aktualizační profil | Součástí řešení je i Duální aktualizační profil pro možnost stahování aktualizací z mirroru v lokální síti a zároveň vzdálených serverů při nedostupnosti lokálního mirroru (pro cestující uživatele s notebooky). |
| AV28 | Spouštění web stránek v chráněném režimu | Součástí řešení je i možnost definovat webové stránky, které se spustí v chráněném režimu prohlížeče, pro bezpečnou práci s kritickými systémy nebo internetovým bankovnictví. |
| AV29 | Aktivní ochrany před útoky hrubou silou | Součástí řešení je i systém aktivní ochrany před útoky hrubou silou na protokol SMB a RDP. |
| AV30 | Blokování IP adres | Součástí řešení je i možnost zablokování konkrétní IP adresy po sérii neúspěšných pokusů o přihlášení pro protokoly SMB a RDP s možností výjimek ve vnitřních sítích. |
| AV31 | Automatické aktualizace | Součástí řešení jsou i automatické aktualizace bezpečnostního softwaru s možností odložení restartu stanice. |
| AV32 | „Zmražení“ na požadované verzi | Součástí řešení je i tzv. „Zmražení“ na požadované verzi – produkt je možné nakonfigurovat tak, aby nedocházelo k automatickému povyšování majoritních a minoritních verzí zejména na stanicích, kde se vyžaduje vysoká stabilita. |

## Požadavky na SANDBOX

| **ID** | **Popis požadavku** |
| --- | --- |
| SB01 | Funkce cloudového sandboxu je integrována do produktu pro koncové a serverové zařízení, tzn. Cloudový sandbox nemá vlastního agenta, nevyžaduje instalaci další komponenty ať už v rámci produktu nebo implementace HW prvku do sítě. |
| SB02 | Sandbox umožňující spuštění vzorků malwaru pro Windows a Linux. |
| SB03 | Možnost využití na koncových bodech a serverech pro aktivní detekci škodlivých souborů. |
| SB04 | Analýza neznámých vzorků v řádu jednotek minut. |
| SB05 | Optimalizace pro znemožnění obejití anti-sandbox mechanismy. |
| SB06 | Schopnost analýzy rootkitů a ransomwaru. |
| SB07 | Schopnost detekce a zastavení zneužití nebo pokusu o zneužití zero day zranitelnosti. |
| SB08 | Řešení pracuje s behaviorální analýzou. |
| SB09 | Kompletní výsledek o zanalyzovaném souboru včetně informace o nalezeném i nenalezeném škodlivém chování daného souboru. |
| SB10 | Manuální odeslání vzorku do sandboxu. |
| SB11 | Možnost proaktivní ochrany, kdy je potenciální hrozba blokována, dokud není znám výsledek analýzy ze sandboxu. |
| SB12 | Neomezené množství odesílaných souborů. |
| SB13 | Veškerá komunikace probíhá šifrovaným kanálem. |
| SB14 | Okamžité odstranění souboru po dokončení analýzy v cloudovém sandboxu. |
| SB15 | Možnost volby, jaké kategorie souborů do cloudového sandboxu budou odcházet (spustitelné soubory, archivy, skripty, pravděpodobný spam, dokumenty atp.) |
| SB16 | Velikost odeslaných souborů do cloudového sandboxu může dosahovat až 64MB. |
| SB17 | Výsledky analyzovaných souborů jsou dostupné a automatizovaně distribuované všem serverům a stanicím napříč organizací, tak aby nedocházelo k duplicitnímu testování. |

## Požadavky na vlastní EDR

| **ID** | **Popis požadavku** |
| --- | --- |
| EDR01 | Možnost provozu centrálního serveru on-premise na platformě Windows Server. |
| EDR02 | Webová konzole pro správu a vyhodnocení. |
| EDR03 | Možnost provozu s databázemi MS SQL a My SQL. |
| EDR04 | Možnost provozu v offline prostředí. |
| EDR05 | Autonomní chování se schopností vyhodnotit podezřelou/ škodlivou aktivitu a zareagovat na ni i bez aktuálně dostupného řídícího serveru nebo internetového připojení. |
| EDR06 | Logování činností administrátora (Audit Log). |
| EDR07 | Podpora EDR pro systémy Windows, Windows server, MacOS a Linux. |
| EDR08 | Možnost autentizace do managementu EDR pomocí 2FA. |
| EDR09 | Možnost řízení managementu EDR prostřednictvím API, a to jak pro přijímání informací z EDR serverů, tak i pro zasílání příkazů na EDR servery. |
| EDR10 | Integrovaný nástroj v EDR řešení pro vzdálené zasílání příkazů přímo z konzole. |
| EDR11 | Možnost izolace zařízení od sítě. |
| EDR12 | Možnost tvorby vlastních IoC. |
| EDR13 | Možnost škálování množství historických dat vyhodnocených v EDR:   * až 3 měsíce pro raw-data * až 3 roky pro detekované incidenty |
| EDR14 | Učící režim“ pro automatizované vytváření výjimek k detekčním pravidlům. |
| EDR15 | Indikátory útoku pracující s behaviorální detekcí. |
| EDR16 | Indikátory útoku pracující s reputací. |
| EDR17 | Řešení umožnuje analýzu vektorů útoku. |
| EDR18 | Schopnost detekce škodlivých spustitelných souborů:   * skriptů, * exploitů, * rootkitů, * síťových útoků, * zneužití WMI nástrojů, * bezsouborového malwaru * škodlivých systémových ovladačů / kernel modulů. * pokusů o dump přihlašovacích údajů uživatele |
| EDR19 | Schopnost detekovat laterální pohyb útočníka. |
| EDR20 | Analýza procesů, veškerých spustitelných souborů a DLL knihoven. |
| EDR21 | Náhled na spuštěné skripty použité při detekované události. |
| EDR22 | Možnost zabezpečeného vzdáleného spojení přes servery výrobce do konzole EDR. |
| EDR23 | Schopnost automatizovaného response úkonu pro jednotlivá detekční pravidla v podobě:   * izolace stanice, * blokace hash souboru, * blokace a vyčištění sítě od konkrétního souboru, * ukončení procesu, * restart počítače, * vypnutí počítače. |
| EDR24 | Podpora automatického vyřešení incidentu administrátorem. |
| EDR25 | Prioritizace vzniklých incidentů. |
| EDR26 | Možnost stažení spustitelných souborů ze stanic pro bližší analýzu ve formátu archivu opatřeným heslem. |
| EDR27 | Integrace a zobrazení detekcí provedených antimalware produktem. |
| EDR28 | Řešení je schopno generovat tzv. forest / full execution tree model. |
| EDR29 | Vyhledávání pomocí nově vytvořených IoC nad historickými daty. |
| EDR30 | Provázání s technikami popsanými v knowledge base MITRE ATT&CK. |
| EDR31 | Řešení obsahuje integrovaný vyhledávač VirusTotal s možnost rozšíření o vlastní vyhledávač. |

## Požadavky na management konzolí

| **ID** | **Popis požadavku** |
| --- | --- |
| MK01 | Management konzole pro správu všech řešení v rámci nabízeného balíku, Provedení webové konzole. Možnost instalace na Windows i Unix. |
| MK02 | Předpřipravená virtual appliance pro virtuální prostředí VMware, Microsoft Hyper-V a Microsoft Azure. |
| MK03 | Server/proxy architektura pro síťovou pružnost – snížení zátěže při stahování aktualizací detekčních modulů výrobce. |
| MK04 | Možnost probuzení klientů pomocí Wake On Lan. |
| MK05 | Vzdálené vypnutí, restart počítače nebo odhlášení všech uživatelů. |
| MK06 | Možnost konfigurace virtual appliance přes uživatelsky přívětivé webové rozhraní. |
| MK07 | Nezávislý management agent pro platformy Windows, Linux a MacOS. |
| MK08 | Management agent pro architektury na platformách Windows a MacOS:   * x86, * x64, * ARM64 |
| MK09 | Nezávislý agent (pracuje i offline) vzdálené správy pro zajištění komunikace a ovládání operačního systému klienta. |
| MK10 | Offline uplatňování politik a spouštění úloh při výskytu definované události (například: odpojení od sítě při nalezení škodlivého kódu). |
| MK11 | Administrace v nejpoužívanějších jazycích včetně češtiny. |
| MK12 | Široké možnosti konfigurace oprávnění administrátorů (například možnost správy pouze části infrastruktury, které konkrétnímu administrátorovi podléhá). |
| MK13 | Zabezpečení přístupu administrátorů do vzdálené správy pomocí 2FA. |
| MK14 | Podpora štítků/tagování pro snazší správu a vyhledávání. |
| MK15 | Správa karantény s možností vzdáleného vymazání / obnovení / obnovení a vyloučení objektu z detekce. |
| MK16 | Vzdálené získání zachyceného škodlivého souboru z klienta. |
| MK17 | Detekce nespravovaných (rizikových) počítačů komunikujících na síti. |
| MK18 | Podpora pro instalace a odinstalace aplikací 3. stran. |
| MK19 | Vyčítání informací o verzích softwaru 3. stran. |
| MK20 | Možnost vyčítat informace o hardwaru na spravovaných zařízeních (CPU, RAM, diskové jednotky, grafické karty…). |
| MK21 | Možnost vyčíst sériové číslo zařízení. |
| MK22 | Možnost vyčíst volné místo na disku. |
| MK23 | Detekce aktivního šifrování BitLocker na spravované stanici. |
| MK24 | Zobrazení časové informace o posledním bootu stanice. |
| MK25 | Odeslání zprávy na počítač / mobilní zařízení, které se následně zobrazí uživateli na obrazovce. |
| MK26 | Vzdálená odinstalace antivirového řešení 3. strany. |
| MK27 | Vzdálené spuštění jakéhokoli příkazu na cílové stanici pomocí Příkazového řádku. |
| MK28 | Dynamické skupiny pro možnost definování podmínek, za kterých dojde k automatickému zařazení klienta do požadované skupiny a automatickému uplatnění klientské úlohy. |
| MK29 | Automatické zasílání upozornění při dosažení definovaného počtu nebo procent ovlivněných klientů (například: 5 % všech počítačů / 50 klientů hlásí problémy). |
| MK30 | Podpora SNMP Trap, Syslogu a qRadar SIEM. |
| MK31 | Podpora formátů pro Syslog zprávy:   * CEF * JSON * LEEF |
| MK32 | Podpora instalace skriptem – např. \*.bat, \*.sh, \*.ini (GPO, SSCM…). |
| MK33 | Rychlé připojení na klienta pomocí RDP z konzole pro vzdálenou správu. |
| MK34 | Reportování stavu klientů chráněných jinými bezpečnostními programy. |
| MK35 | Schopnost zaslat reporty a upozornění na e-mail. |
| MK36 | Konzole podporuje multidoménové prostředí (schopnost pracovat s více AD strukturami). |
| MK37 | Konzole podporuje multitenantní prostředí (schopnost v jedné konzoli spravovat více počítačových struktur). |
| MK38 | Podpora VDI prostředí (Citrix, VMware, SCCM, apod.) |
| MK39 | Podpora klonovaní počítačů za pomocí golden image. |
| MK40 | Podpora instančních klonů. |
| MK41 | Podpora obnovy identity počítače pro VDI prostředí na základě FQDN. |
| MK42 | Možnost definovat vícero jmenných vzorů klonovaných počítačů pro VDI prostředí. |
| MK43 | Přidání zařízení do vzdálené správy pomocí:   * synchronizace s Active Directory, * ruční přidání pomocí dle IP adresy nebo názvu zařízení, * pomocí síťového skenu nechráněných zařízení v síti * Import skrze csv soubor. |

## Požadavky na MFA

| **ID** | **Název požadavku** | **Popis požadavku** |
| --- | --- | --- |
| MFA01 | Způsoby doručení OTP (One Time Password): | OTP lze doručit:   * aplikací v mobilním zařízení, * e-mailem, * bezpečnostním tokenem, * SMS zprávou, (poznámka: Včetně možnosti konfigurace vlastní SMS brány pro doručení OTP kódu) * vlastní aplikací. |
| MFA02 | Další možnosti ověření | Další možnosti ověření jsou:   * FIDO * Push Authnetication |
| MFA03 | Existence aplikace výrobce s podporou Push-Notifications | Existence aplikace výrobce s podporou Push-Notifications pro platformy:   * iOS * Android * watchOS, wear OS |
| MFA04 | Požadavky na aplikaci výrobce (aplikace podporující push notifikace) | Požadavky na aplikaci výrobce (aplikace podporující push notifikace)   * Mobilní aplikace v hlavních jazykových lokalizacích včetně češtiny * Přístup do mobilní aplikace ochráněn PINem / biometrikou * Možnost generovat OTP v off-line prostředí (bez internetové připojení, bez GSM spojení) |
| MFA05 | Podporovaná zařízení | Řešení MFA musí podporovat:   * Hardwarové tokeny HOTP splňující standard OATH * Hardwarové tokeny certifikované výrobcem * Kompletně softwarové řešení – bez nutnosti nákupu dalšího hardwaru * Podpora time based hardwarových tokenů (PSKC) * Self-enrollment uživatelů |
| MFA06 | Chráněné služby | Požadují se tyto chráněné služby:   * Příhlášení do webových aplikací společnosti Microsoft (OWA, SharePoint…), * Přihlášení přes RDP, * Exchange Control Panel & Exchange Administrator Center, * VMware Horizon View, * VPN služby využívajících protokol RADIUS (Cisco, Citrix, Fortinet, Juniper, Microsoft, OpenVPN…), * cloudové služby Office 365, G Suite, identity providerů (podpora SAML protokolu, podpora AD FS) * Lokálního přihlášení do Windows, Linux, macOS účtů * Vyžádání 2FA v nouzovém režimu Windows * Vyžádání 2FA při vyvolání UAC dialogu ve Windows * Vyžádání 2FA při uzamčeném účtu |
| MFA07 | Správa řešení | Požadavky na správu řešení:   * Webové konzole * Přístup do konzole lze chránit 2FA ověřením * Podpora multitenantního provozu (možnost spravovat vícero uživatelských struktur v jedné konzoli) * Podpora synchronizace uživatelských účtů z Active Directory * Možnost tvorby výjimek pro vnitřní sítě, kde není 2FA vyžadováno * Umožnit uživatelům přihlášení bez použití 2FA pro vybrané služby * Konzole umožňuje generovat Master recovery klíče pro konkrétní chráněné služby * Centrální správa a přidělování hardwarových tokenů jednotlivým uživatelům * Možnost reportování o úspěšných/ neúspěšných přihlášení uživatelů, způsobu použité autentizace (SMS, Push, OTP) |
| MFA08 | Podpora integrace systémů třetích stran | Požaduj se podpora integrace systémů třetích stran prostřednictvím:   * API * SDK výrobce (Java, PHP, .NET, Windows Script Host) |
| MFA09 | Shoda se standardy | Soulad se standardem ISO027001. |
| MFA10 | Limitace počtu offline přihlášení | - Možnost definovat maximální počet offline přihlášení |

# Log Management (LM) Systém

V současnosti je provozován stávající LM ve formě HW BOXU, který je již morálně zastaralý. Vzhledech k aktuálnímu směru rozvoze požadujeme dodání moderního LM ve formě virtuálním appliance. Aktuálně LM provádí sběr a vyhodnocení logových informací z jednotlivých prvků infrastruktury, jejich centralizaci a archivaci v jednom místě. V rámci organizace bude i nadále zajišťovat schopnost vyhodnocení logových informací z jednotlivých prvků infrastruktury. Centrální LM bude provozován v novém virtuálním prostředí, které zajistí požadovaný výkon.

Požaduje se řešení, které umožňuje seskupovat provozní záznamy HW zařízení, OS a aplikací na jednom místě, ve sjednoceném formátu, se zachováním jejich dostupnosti, důvěrnosti a integrity. Díky přehlednému rozhraní pro vyhledávání, přizpůsobitelným reportům a statistikám, bude Log Management umožňovat snazší práci s logy při analýze, a to jak za účelem auditu, tak i pro zajištění každodenního provozu.

**Požaduje se licence na min. 250 IP nebo min. 1000 EPS.**

**Požadujeme dodání řešení vč. supportu/servisní podpory na dobu 5 let. Podpora musí zahrnovat všechny updaty i upgrady, telefonická nebo emailová podpora výrobce v rozsahu alespoň 8x5 (8-16 hod. po-pá).**

Řešení LM zajistí tyto funkční a nefunkční požadavky:

| **ID** | **Název požadavku** | **Popis požadavku** |
| --- | --- | --- |
| LM01 | Konfigurovatelnost přes GUI | Řešení musí být konfigurovatelné a ovládané přes webové GUI rozhraní. |
| LM02 | Podpora HA | Řešení musí podporovat zapojení pro High Availability, tj. vysokou dostupnost. |
| LM03 | Podpora vstupních protokolů | Požaduje se podpora vstupních protokolů (sources ~ zdrojů log záznamů) a přenosu dat:   * SNMP * syslog:   + UDP (dle RFC 3164)   + TCP   + IETF (RFC 5424) + TLS * Aktivní sběr logů z databází (přes ODBC). * Agent/Client pro sběr log záznamů jak pro prostředí Windows, tak i pro prostředí Linux/Unix (HP-UX, Solaris, …)/AIX:   + sběr Windows EVT záznamů i z kontejnerů Windows Server.   + sběr AIX/Solaris/HP-UX/IRIX auditních OS záznamů.   + sběr textových logů ze souborů.   + přenos log dat (tj. forward přes syslog) šifrovaným kanálem.   Podpora RELAY funkce (tj. přeposílací servery, např. pro infrastrukturu v DMZ) |
| LM04 | Podpora BUFFER/CACHE | Požaduje se podpora BUFFER/CACHE na výstupu jak u Agenta, tak pro RELAY, a také pro Server/Appliance |
| LM05 | Výstupní protokoly | Požaduje se podpora výstupních protokolů (destinations ~ umístění log záznamů):   * syslog (UDP, TCP, IETF). * zápis logových dat napřímo do databází (ODBC). * zápis logových dat do JSON formátu. * SNMP Trap. |
| LM06 | Pokročilé filtrování | Požaduje se možnost konfigurace pokročilého filtrování logových záznamů (jakýkoli vstup logových dat prochází libovolnou sadou filtrů na libovolný výstup). |
| LM07 | Ukládání log dat: | Požaduje se ukládání log dat:   * Textové úložiště v originálním (RAW) formátu. * Šifrované úložiště (logspace) s podporou šifrování privátním klíčem/certifikátem a TSA podpisem, pro zajištění právních potřeb forenzního šetření. * Podpora indexace logových dat pro rychlé vyhledávání údajů i v nestrukturovaných v datech (položka message u syslog protokolu). * Podpora komprimace jako součást daného úložiště. |
| LM08 | Řízení přístupů (AAA) | Požaduje se řešení řízení přístupů k LM:   * řízení přístupu na úrovni jednotlivých úložišť (logspace). * podpora GROUP managementu. * podpora autentizace přes RADIUS. * Podpora lokální /externí databáze uživatelů – LDAP |
| LM09 | Zálohování, Archivace, Export, Sdílení log dat | Součástí řešení LM bude i Zálohování, Archivace, Export, Sdílení log dat:   * nezávislé zálohovací politiky jak pro konfiguraci, tak pro jednotlivá úložiště (logspace). * nezávislé archivační (data retention) politiky pro jednotlivá úložiště log dat. * podpora exportu/sdílení log dat v originálním i ve strukturovaném tvaru |
| LM10 | Alerting | Součástí řešení LM bude alerting:   * RATE alerting (detekce změn „nestandardního chování zdrojů logových záznamů“ pro nastavené limitní hladiny datových přenosů v čase). * Výskyt definovaného slova/znaku v logu (Např. „error“, „fail“ nebo „alert“). * Artificial Ignorance – funkcionalita, která identifikuje, co je informačně nezajímavé a potlačuje eskalaci. Nebo identifikuje, co informačně systém Log managementu ještě nikdy neviděl a eskaluje anomálii. |
| LM11 | Nezávislost na SIEM | Řešení je koncipováno jako čistý Log Management, nejedná se tedy o Event Management – pro plnou funkci není potřeba tvorby parserů. Řešení není provázáno na SIEM a je plně nezávislé jak fyzicky tak logicky na SIEM řešeních. Nejedná se tedy o ALL-IN-ONE řešení, s konfigurací pro Log Management. |
| LM12 | Vyhledávání a Reporting: | * Rychlé vyhledávání na základě fulltext indexace (vyhledávaní bez nutnosti tvorby parserů), tedy velké objemy dat se neprohledávají formou „grep like“ prohledávání po řádcích. * Umožnění vytváření vlastních analytických pohledů. * Dashboardy/Statistiky Log management infrastruktury. * Uživatelsky konfigurovatelný reporting strukturovaných dat (timestamp, facility, priority, tag, program, hostname, atd.). * Definice vlastních vyhledávacích filtrů a „pohledů“. * Podpora přístupů pro pohledy (co pohled to jiná skupina uživatelů). |
| LM16 | Peering | Požaduje se peering:   * Možnost přepojit více Log Management serverů a vyhledávání nad nimi přes jedno rozhraní. * Definice vyhledávacích filtrů a „pohledů“ nad „peeringovými“ servery. * Podpora přístupů pro pohledy (co pohled to jiná skupina uživatelů). |
| LM14 | API rozhraní | Řešení bude umožňovat vyhledávání přes REST API rozhraní |

# PAM Systém

Požadujeme dodání nástroje PAM, který nahradí stávající HW appliance, která je již za morální dobou udržitelnosti. Požadujeme dodat PAM, který umožní snadný přechod ze stávajícího řešení, které je koncipováno jako transparentní proxy a neovlivňuje pracovníky návyky uživatelů a dodavatelů. Zároveň požadujeme převedení stávající konfigurace ze současného řešení v co největší míře. Celé nové řešení požadujeme postavit jako virtuální appliance pro VMWARE ESX prostředí, které nevyžaduje instalaci agentů na dohledované systémy a která bude opět plně transparentní.

Požadujeme systém řízení privilegovaných účtů = účtů, které má vysoké oprávnění, tj. účty typu root v Linux/UNIX systémech, účty typu Administrátor ve Windows systémech, systémové účty používané aplikacemi nebo sdílené účty, které nejsou vázané na fyzickou osobu. S těmito účty pracují privilegovaní uživatelé, tedy fyzické osoby, která používají privilegované účty (mají možnost změny jak konfigurace, tak i dat). Jedná se o pracovníky provozu, dodavatele, nebo vývojáře.

PAM zaznamenává činnost systémového administrátora, který přistupuje k citlivým datům anebo provádí konfigurační činnost. Systém vytváří auditní stopu. Auditní záznamy mohou být přehrávány jako video, takže je možné sledovat události přesně tak, jak se ve skutečnosti odehrály.

PAM monitoruje tzv. Session = spojení od privilegovaného uživatele k cílovému serveru / systému, které je řízené a monitorované. Cílovým systém je systém, na který se privilegovaný uživatel připojuje prostřednictvím privilegovaných účtů. Činnost uživatele je ve formě jeho „session“ auditována/nahrávána tak, aby nebylo možné tento záznam pozměnit a ani otevřít neoprávněným uživatelem.

**Požadujeme licence na min. 25 koncových systémů bez omezení počtu uživatelů.**

**Požadujeme dodání řešení vč. supportu/servisní podpory na dobu 5 let. Podpora musí zahrnovat všechny updaty i upgrady, telefonická nebo emailová podpora výrobce v rozsahu alespoň 8x5 (8-16 hod., po-pá).**

Řešení PAM zajistí tyto funkční a nefunkční požadavky:

| **ID** | **Popis požadavku** |
| --- | --- |
| PAM01 | Řešení musí podporovat zapojení pro High Availability, tj. vysoká dostupnost. |
| PAM02 | Řešení musí být konfigurovatelné a ovládané přes webové GUI rozhraní. |
| PAM03 | Řešení musí být bezagentové. |
| PAM04 | Řešení musí být nezávislé na verzi OS cílových serverů. |
| PAM05 | Řešení musí podporovat práci přes tyto protokoly:   * Microsoft RDP * Citrix ICA * SSH * VNC i z SSL * TELNET i z SSL * HTTP/S * MS-SQL * SUDO log |
| PAM06 | Podpora aktualizace systému přes rozhraní produktu |
| PAM07 | Pravidelně vydávané aktualizace výrobcem. Minimálně 2x ročně. |
| PAM08 | Řešení v rámci daných protokolů rozlišuje jejich kanály (např. CLIPBOARD, REMOTE PRINTER, REMOTE DISK, atd.), u kterých je možné definovat:   * Časové okna * Uživatelské skupiny * Rozsahy IP adres * Blokaci |
| PAM0910 | Řešení musí být schopné detekovat pokusy o spuštění aplikace/příkazu a ukončit spojení uživatele. |
| PAM11 | Řešení musí být schopné zaznamenat použité příkazy, titulky oken a použité aplikace |
| PAM12 | Řešení musí být schopné analyzovat stisknuté klávesy a provádět behaviorální analýzu s cílem odhalit zneužití uživatelského účtu |
| PAM13 | Řešení musí být schopné detekovat použití neautorizovaných skriptů |
| PAM14 | Řešení má vestavěny mechanismus pro automatické skórování potencionálně rizikového chování privilegovaného uživatele (použití neobvyklé sekvence příkazů, odlišné chování při použití klávesnice a myši) |
| PAM15 | Řešení musí umožňovat tvorbu black listů a white listů |
| PAM16 | Požadavky na vlastnosti Auditní stopy:   * Přehráváni jako video s přesnou časovou stopou ze signalizací „hluchých míst“ kde se nic neděje. * Šifrování auditní stopy. * TSA časové razítko. * Možnost přehrání online i offilne * Možnost exportu dat v originální formátu |
| PAM17 | Řízení přístupů „sessions“:   * Řešení musí být schopné řídit přístupy v rámci „session“ dle ověření vůči LDAP/RADIUS. * Řešení podporuje možnost dvoufaktorové autentizace pro „session“. * Řešení podporuje režim „čtyř očí“. * Řešení podporuje integraci s externími programy typu ERPM, IDM. * API pro integraci s HelpDesk/ServiceDesk systémy. |
| PAM18 | Logování jak interních akcí, tak informací o „sessions“ pomocí syslog protokolu, podpora TLS nad syslog protokolem. |
| PAM19 | Zálohování, Archivace, Export, Sdílení log dat:   * nezávislé zálohovací politiky jak pro konfiguraci/interní databázi, tak pro jednotlivé „sessions“. * nezávislé archivační (data retention) politiky pro jednotlivé úložiště auditních dat. * podpora exportu auditních stop a exportu strukturovaných metadat. * podpora archivace na externí úložiště * podpora automatizovaného zálohování dat |
| PAM20 | Řešení musí poskytovat indexaci pro rychlé vyhledávaní nejen informací o získaných „session“ dat, ale taky o jejich obsahu (taky nazývané content, nebo OCR indexace). |
| PAM21 | Přístupy k samotnému systému:   * podpora GROUP managementu. * podpora autentizace přes RADIUS. * Podpora lokální /externí databáze uživatelů – LDAP. |
| PAM22 | Reporting bude zahrnovat:   * Dashboardy/Statistiky o „sessions“. * Uživatelsky konfigurovatelný reporting strukturovaných dat. * Možnost tvorby vlastních reportů nad content informacemi formou tvorby SQL QUERY dotazů. * API pro reporting do externích SW. * Řešení umožňuje Full text search. |

# SIEM Systém

Aktuálně je využívám SIEM ve formě hardware appliance, která je technicky i morálně zastaralá. Z tohoto důvodu požadujeme dodání moderního nástroje SIEM, který bude provozován na virtuálních prostředcích organizace. Požadujeme moderní nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí známý pod zkratkou SIEM (Security Information and Event Management), který provádí management bezpečnostních informací a událostí.

Nový SIEM nahradí stávající řešení, které se používá jako analytický nástroj vytvářející závěry o bezpečnostní situaci v reálném čase. Musí tedy velmi rychle analyzovat získaná log data o následcích s informacemi o možných příčinách. Aby SIEM plnil svoji úlohu, je nutné zajistit základní kontrolu a monitoring bezpečnosti dané infrastruktury, integrovat vhodné zdroje Log informací – vazba na Log Management. Samotný SIEM pouze identifikuje bezpečnostní události a incidenty na základě poskytnutých informací z bezpečnostní infrastruktury.

Řešení SIEM bude umožňovat integraci s dalšími komponentami bezpečnostní infrastruktury tak, aby byl při maximální efektivitě zajištěn sběr všech potřebných informací pro detekci bezpečnostních incidentů.

**Požaduje se dodání virtuální appliance SIEM. Komponenta SIEM musí mít garantovanou licenci pro zpracování min. 1000 událostí za sekundu (dále jen „EPS“) v rámci celodenního průměru, která musí být rozšiřitelná na 5000 EPS v celodenním průměru bez nutnosti upgradu HW, jen pomocí aktivace rozšiřující či nové licence.**

**Systém SIEM musí podporovat současnou práci min. 10 uživatelů.**

**Řešení, respektive licence musí obsahovat možnost minimálně 1000 sběrných konektorů, včetně vlastních custom logů (možnost doplnit další lokality, zdroje událostí, apod.).**

**Řešení, respektive licence dále musí obsahovat možnost sbírat všechny typy výrobcem podporovaných zdrojů událostí a vlastních custom logů.**

**Požadujeme dodání řešení vč. supportu/servisní podpory na dobu 5 let. Podpora musí zahrnovat všechny updaty i upgrady, telefonická nebo emailová podpora výrobce v rozsahu alespoň 8x5 (8-16 hod. po-pá).**

Řešení SIEM zajistí tyto funkční a nefunkční požadavky:

| **ID** | **Popis požadavku** |
| --- | --- |
| SIEM01 | Všechny potřebné komponenty musí být součástí dodaného systému SIEM, včetně databáze. |
| SIEM02 | Log Management je fyzicky i logicky nezávislý na SIEMu. Při nedostupnosti SIEMu je Log Management plně funkční a obsahuje všechny logy v RAW formátu. Při nedostupnosti Log Managementu je SIEM plně funkční a obsahuje všechny potřebné logy v normalizovaném formátu. Vrstva zajištující sběr je fyzicky i logicky nezávislá na LM a SIEM. Při nedostupnosti jak SIEM, tak LM, vrstva nadále funguje nezávisle a zajištuje jak sběr logů tak je možné ji konfigurovat. |
| SIEM03 | Rozhraní všech komponent systému SIEM je dostupné v českém nebo anglickém jazyce. Dokumentace skutečného provedení je k dispozici v českém jazyce, ostatní buď v jazyce českém anebo anglickém. |
| SIEM04 | Všechny požadované funkce se spravují a využívají přes společnou řídící konzoli (dále jen „Centrální správa“), která je rovněž přístupná přes webové rozhraní z fyzického i virtuálního PC s využitím Microsoft Edge a novějších, nebo jiným podobným způsobem. Prezentace dat musí být provedena v grafické podobě, prezentační rozhraní musí být multiplatformní nebo platformě nezávislé a plně funkční na platformách Windows, Linux, Apple OS.X. |
| SIEM05 | Centrální správa systému SIEM musí podporovat GUI (Grafické uživatelské rozhraní), a skriptovací nástroje. |
| SIEM06 | Veškerá konfigurace, definice zdrojů logů, definice korelačních pravidel, tvorba reportů, atd., musí probíhat z grafického rozhraní systému SIEM. |
| SIEM07 | Správa uživatelů systému SIEM musí být integrovatelná s Microsoft Active Directory a RADIUS, tj. systém k přihlášení využívá doménové účty s využitím SSO. |
| SIEM08 | Systém SIEM musí rovněž umožňovat přihlašování pomocí lokálních účtů pro případ neaktivního propojení s AD. |
| SIEM09 | Řešení musí umožnit přístup více uživatelů současně, a to jak na úrovni přístupu ke vstupním/zdrojovým datům systému, tak i k incidentům. Přístup uživatelů musí být založen na volně definovaných, oddělených rolích s možností granulárního přidělování práv v rámci každé role, dle zdrojových dat, identifikace monitorovaných zařízení, skupin zařízení a serverů, typu vstupních dat, apod. Role nesmí být vázány na AD, musí být spravovány interně. |
| SIEM10 | Řešení musí podporovat nebo být rozšiřitelné pro kompletní oddělení skupin uživatelů k odlišným datům a konfiguracím, kdy jednotlivé instance mohou mít možnost vlastní konfigurace a správy (multi-tenant přístup). Požaduje se řešení pro min. 10 tenantů |
| SIEM11 | Systém SIEM musí vyhledávat dle klíčových slov (řetězců) v názvech zdrojů, v korelačních pravidlech v uložených log záznamech a v auditních log záznamech systému (tedy vyhledávání v konfiguračních položkách a v „contentu“). |
| SIEM12 | Systém SIEM musí zaznamenávat vlastní auditní logy po nastavitelnou dobu a tyto musí být chráněny proti modifikaci. |
| SIEM13 | Řešení musí nativně podporovat protokoly IPv4, IPv6, jak při normalizaci vstupních dat, tak i při komunikaci se zdroji dat. |
| SIEM14 | Systém umožňuje exportovat/importovat své nastavení do/ze souboru (definice dashboardů, reportů a korelačních pravidel – tedy „contentu“). |
| SIEM15 | Systém musí obsahovat plně integrovaný nástroj pro řízení celého životní cyklu incidentu (ticketing). |
| SIEM16 | Systém SIEM musí mít srozumitelně a prokazatelně deklarováno vedení licenční politiky, a to včetně uvedení funkcionalit, které nejsou součástí základní licence a zda a za jakých podmínek je možné je dokupovat. |
| SIEM17 | Systém SIEM nesmí být licenčně omezen na počet generujících zařízení/zdrojů logů, na počtu evidovaných aktiv a na počtu uživatelů/konzolí. |
| SIEM18 | Komponenta SIEM musí být schopna nárazově (minimálně po dobu 72h) zpracovat 7500 EPS, bez jakýchkoliv výkonnostních nebo licenčních omezení, včetně zachování plné funkcionality u všech komponent (bez ztráty logů), přičemž dodané řešení musí zajistit zpracování logů nejpozději v minutách od jejich vzniku. |
| SIEM19 | Systém SIEM nesmí technicky limitovat počet událostí (například při překročení licence nebo výkonu zakoupeného řešení) za určité časové období, aby nedošlo k jejich zahození. |
| SIEM20 | Kapacita interního úložného prostoru systému SIEM musí umožnit interně uchovat normalizované log záznamy po dobu min. 4 měsíců. |
| SIEM21 | Systém dále musí umožnit uchovávání obou formátu logů formou záloh (archivace), a zejména musí umožnit obnovení vybraných částí logů a jejich zpřístupnění přes Centrální správu SIEM. |
| SIEM22 | Výkonnost systému musí být dostatečná nejen pro sběr a korelaci logů, ale i pro přípravu reportů a alertů. Alert musí být zaslán nejpozději do 3 minut od vzniku, report obsahující 1000 řádek musí být vytvořen do 10 minut od začátku generování. |
| SIEM23 | SIEM musí umožňovat používání regulárních výrazů na straně agentů (pokud budou využity) i serveru systému SIEM. |
| SIEM24 | SIEM musí umožňovat Normalizaci/Parsování bezpečnostních událostí v systému SIEM do jednotného formátu (centrální logy musí mít stejný formát ze všech zdrojů) a doplnění o další detailní informace (např. doplnění jména uživatele na základě uživatelského účtu, doplnění jména stanice na základě IP adresy apod.). |
| SIEM25 | SIEM musí umožňovat kategorizaci logů, kterou poskytuje univerzální taxonomii nezávislou na výrobci zdroje události, aby bylo možné homogenně vyhledávat, reportovat nebo porovnávat události z různých zařízení bez nutnosti detailní znalosti konkrétního logu. |
| SIEM26 | SIEM musí umožňovat vyhodnocovat i vlastní provozní logy |
| SIEM27 | SIEM musí umožňovat zobrazení a změnu nasazených korelačních pravidel, včetně pravidel dodaných výrobcem. |
| SIEM28 | SIEM musí umožňovat export a import pravidel i parserů. |
| SIEM29 | SIEM musí umožňovat definování / přidávání vlastních korelačních pravidel a log parserů bez nutnosti spolupráce s dodavatelem nebo výrobcem, např. pomocí wizardu nebo regulárních výrazů. |
| SIEM30 | SIEM musí umožňovat real-time korelaci a korelaci v časovém okně několika hodin mezi událostmi z různých zdrojů (libovolných a nezávislých zdrojů předávajících data do systému). |
| SIEM31 | SIEM musí umožňovat korelaci událostí dávkově importovaných do systému SIEM, tj. korelaci událostí, které nejsou zařazovány real-time, ale např. prostřednictvím importů logů 1x denně (scheduler correlations). SIEM umožní ověření nového korelačního pravidla proti historickým datům. |
| SIEM32 | SIEM musí umožňovat automatické stanovení závažnosti událostí např. na základě předchozí činnosti zdroje / cíle nebo jiných dostupných informací. |
| SIEM33 | SIEM musí umožňovat vyhledávání anomálií v událostech (např. nárůst počtu neúspěšných pokusů o přihlášení v určitém čase, neúspěšné pokusy o přihlášení v mimopracovní době apod.) nebo datových tocích (např. neobvyklé toky dat). |
| SIEM34 | SIEM musí umožňovat ukládání logů v systému SIEM ve tvaru, ve kterém je možné jejich prohledávání, tj. minimálně musí poskytovat vyhledávání na základě regulárních nebo logických výrazů podle času a klíčových slov (např. jmen uživatelů, čísel /jmen událostí apod.). |
| SIEM35 | SIEM musí umožňovat vyhledávání logů/eventů na základě „full-text“ indexace. |
| SIEM36 | SIEM musí umožňovat na jakoukoliv událost navázat automatickou akci:   * notifikaci přes mail s možností definovat pravidla pro zasílání na různé adresy podle kritičnosti, zdroje apod. * spuštění externího skriptu. |
| SIEM37 | SIEM musí poskytovat zabudovanou "security knowledge" tj. předdefinovaná pravidla rozpoznávání a zpracování událostí a jejich pravidelné aktualizace od výrobce, min 4x ročně. Musí obsahovat minimálně:   * Generické politiky * Generická korelační pravidla * Generické předdefinované reporty, pokud budou k dispozici |
| SIEM38 | SIEM musí obsahovat komplexní sadu funkcionalit a přednastavených korelačních pravidel, které řeší klasické hrozby a bezpečnostní rizika i sofistikované bezpečnostní problémy z různých oblastí:   * útoky robotů, červů a virů (včetně chyb antivirů); * neoprávněný přístup k aplikacím (ověřování uživatelů, změny administrace a konfigurace); * chyby a změny v sítích (chyby a stavy síťových zařízení); * monitorování serverů a desktopů (administrace privilegovaných uživatelů, přístupy a změny konfigurace, odmítnutá připojení, úspěšné a chybné přihlašovací aktivity, varování systémů IPS/IDS a využívání šíře pásma); * uchvácení šíře pásma a porušení platných zásad (úspěšná a chybná přihlášení do systému, změny hesla, změny konfigurace); * masivní šifrování dat (ransomware); * vědomá snaha nebo neuvědomělá činnost vedoucí k odcizení nebo znehodnocení důvěrných dat (porušení logů SIEM, DLP události, porušení časových razítek apod.); * a další. |
| SIEM39 | Řešení SIEM musí umět porovnat neobvyklý počet určitých událostí oproti jinému období z minulosti – base line analýza. |
| SIEM40 | Systém SIEM musí být schopen provázat několik přístupových záznamů tak, aby byl schopen rozpoznat "admin hopping" = přihlášení z bodu A do D přes prostředníky B a C, za předpokladu, že přímý prostup není dovolen. |
| SIEM41 | Reportovací nástroj musí podporovat trendový reporting nad velkými objemy dat ve velkém časovém období (1 rok) a tvorbu vlastních agregačních (sumarizačních) tabulek s možností nastavit různé sumarizační časové rámce (minimálně hodiny, dny). |
| SIEM42 | Systém SIEM musí poskytovat reporty i ve formě grafů a tabulek. |
| SIEM43 | Systém SIEM musí vytvářet reporty ve formátech PDF, HTML a CSV, popř. dalších. |
| SIEM44 | Systém SIEM musí umožňovat export dat ve formátu XML nebo CSV. |
| SIEM45 | Systém SIEM musí obsahovat analytické nástroje umožňující např. reportování, forenzní analýzu, analýzu změn, statistické reporty nad aktuálními i historickými daty. |
| SIEM46 | Systém SIEM musí poskytovat pro každého uživatele vlastní personalizovaný dashboard. |
| SIEM47 | Systém SIEM musí poskytovat Drill-down analýzu v GUI tj. od obecnějších informací vedou linky na konkrétnější informace (např. z reportu o počtu bezpečnostních událostí podle jednotlivých typů OS je možné na jeden klik dostat report o počtu bezpečnostních událostí na jednotlivých hostech s daným OS a dále pokračovat na report o počtu bezpečnostních událostí v jednotlivých aplikacích / lozích / zdrojích na daném hostu apod.). |
| SIEM48 | Systém musí podporovat automatické spouštění definovaných reportů (měsíčně, týdně, denně, nebo v definovaném čase), ukládání na síťové úložiště a jejich zasílání e-mailem přímo ze systému. |
| SIEM49 | Autentizace musí být oddělená od autorizace. Tj. Při autentizaci vůči AD je autorizace řízená uvnitř SIEM pomocí rolí a ne pomocí skupin v AD. |
| SIEM50 | Systém musí podporovat režim vysoké dostupnosti HA (High availability). Jak v řežimu active-active, tak active-passive. |
| SIEM51 | Součástí SIEM nástroje je i komplexní řešení SOAR bez omezení na počet akcí nebo uživatelů. |
| SIEM52 | Řešení musí poskytovat out-of-the box pracovní toky (Workflows) na automatizaci standardních toků incidentů (Incident flows) pro různí kategorie incidentů jako DDoS, Phishing, Malware... |
| SIEM53 | Řešení musí poskytovat možnost graficky vytvářet pracovní toky (Workflow) anebo aktivity. |
| SIEM54 | Řešení musí podporovat sdružení aktivit Incident Response podle fází a schopnost stanovit pořadí aktivit, které se mají dokončit. |
| SIEM55 | Řešení musí podporovat automatizované specifikování reakčních aktivit nebo aktivity na základě a/nebo podmínek |
| SIEM56 | Řešení musí, byť schopné notifikovat zainteresovaných lidí (Tvůrce incidentu, Analytik...) o průběhu incidentu (např. při aktualizaci, označení v časti incidentu, přiřazení aktivity na dokončení) |
| SIEM57 | Řešení musí nabízet produktové a konfigurovatelné funkce Reportingu a Dashboardy. |
| SIEM58 | Řešení musí poskytovat obohacení založené na typických interních údajích společnosti (např. Informace o aktivitách, uživatelích, odděleních, rolích). |
| SIEM59 | Řešení musí integrovat informace od interních a externích poskytovatelů (např. Threat Intelligence Feeds, nástroje SIEM, Endpoint). |
| SIEM60 | Řešení musí nabízet plně zdokumentované REST API. |

# Svolávací Systém SAIW (Systém Automatizace incidenčních workflow)

Předmětem dodávky bude dále implementace Systému pro Automatizaci Incidenčních Workflow (SAIW). Jedná se o komunikační nadstavbu bezpečnostních komponent, která umožní automatizaci komunikace v rámci řešení incidentů vzniklých na dodaných bezpečnostních prvcích

**Požaduje se licence plně pokrývající všechny požadavky SAIW01-SAIW13.**

**Požadujeme dodání řešení vč. supportu/servisní podpory na dobu 5 let. Podpora musí zahrnovat všechny updaty i upgrady, telefonická nebo emailová podpora výrobce v rozsahu alespoň 8x5 (8-16 hod., po-pá).**

| **ID** | **Popis požadavku** |
| --- | --- |
| SAIW01 | Systém bude poskytovat funkce pro efektivní komunikaci a spolupráci mezi osobami odpovědnými za řešení incidentů a zúčastněnými stranami. Komunikace bude zajištěna v rozsahu:   * Mailové notifikace * Rozesílání SMS * Automatizované hlasové volání |
| SAIW02 | Možnost rozšíření komunikačních kanálů o whatsapp – existující funkcionalita |
| SAIW03 | Systém bude poskytovat klienta pro mobilní zařízení typu Android, iOS. Systém bude umožňovat v chytrých telefonech umožňovat přijetí nebo zamítnutí výzvy, náhled do historie oslovení a scénářů, výběr stavu (připraven, mimo službu atd.), změnu hesla, reportování polohy. Chytrým telefonem se rozumí mobilní telefon, který používá mobilní operační systém Android nebo iOS, |
| SAIW04 | Systém bude umět zakládat bezpečnostní komunikační scénáře = předpisy komunikačních kroků/úkonů (sestavení hlasového volání, odeslání SMS, příjem odpovědní SMS, odeslání PUSH notifikace, bude obsahovat funkci odeslání zprávy ve WhatsApp, příjem zprávy z WhatsApp) a pracovat se zpětnou vazbou (přijímám úkol / nepřijímám úkol) |
| SAIW05 | Systém by měl umět nabírat a vyhodnocovat zpětnou vazbu k zaslaným bezpečnostním incidentům čímž realizuje funkci rozhodovacího uzlu (ano/ne, resp. úspěch/neúspěch). Komunikační kroky lze provádět sekvenčně (jeden po druhém) či paralelně (současně na určitou množinu osob), následující komunikační kroky je možno definovat pro oba výsledky rozhodovacího uzlu a dále je možné podmínit je požadovanými parametry (odbornost, operační stav, dosažení potřebného skóre = situace, kdy výzvu přijme potřebný počet pracovníků. |
| SAIW06 | Systém bude mít možnost spustit bezpečnostní komunikační scénář automaticky (bez zásahu lidské obsluhy) v případě mailového notifikačního alertu generovaného ze systémů NGFW neboLog Manager či SIEM. Událost či incident zaslaný z uvedených systémů automaticky spustí nadefinované bezpečnostní komunikační scénáře |
| SAIW07 | Možnost spouštění předem nadefinovaných bezpečnostních komunikačních scénářů lidskou obsluhou odkudkoliv z webového prohlížeče, z mobilního telefonu:   * Spuštěním zcela předpřipraveného bezpečnostní scénáře – ke spuštění stačí jeden klik * Doplněním proměnných v operačním dashboardu a následným spuštěním bezpečnostního komunikačních scénáře – dashboard lze ovládat jak z dotykové obrazovky, tak i z pracovní stanice |
| SAIW08 | Systém bude mít možnost využití následujících komunikačních kanálů:   * Mailové notifikace, * SMS zprávy s možností požadování odpovědní SMS * telefonický hovor s funkcí TTS (Text To Speech) s možností požadování odpovědi interaktivní DTMF volbou * Automatické zasílání varovných zpráv na PC stanice, vybavené samostatnou aplikací (tlustý klient), která umožňuje akustickou a optickou vizualizaci varovného hlášení na PC stanici |
| SAIW09 | Real-timový přehled o aktuálním stavu odpovědí, průběhu převzetí informace o incidentech včetně zachování evidence a záznamu historie (kompletní přehled o průběhu a historii informování) |
| SAIW10 | Tvorba reportů obsahujících veškeré dostupné informace o komunikaci, vyrozumění a průběhu scénářů. Součástí reportu je i detailní historie odpovědí účastníků. Výběr z několika předdefinovaných reportů. |
| SAIW11 | Možnost automatického vkládání dynamických informací do textu zprávy (datum a čas spuštění/jméno uživatele, který scénář spustil/druh a typ bezpečnostního incidentu …) |
| SAIW12 | Možnost a podpora zadávání operačního stavu informované osoby („připraven / nepřipraven“; respektive „ve službě / mimo službu“ nebo respektive „v pohotovosti/ mimo pohotovost“ |
| SAIW13 | Systém automatizace komunikace SAIW bude provozován v režimu on-premis. Systém tedy bude umístěn v infrastruktuře zákazníka. Nicméně komunikační služby SMS konektor a SIP trunk budou provozovány formou služby a systém automatizace komunikace na ně bude napojen. Součástí řešení je i volná měsíční kapacita 100 SMS a 30 min volání zdarma. |

# SOC (Security Operation Centrum)

V rámci projektu bude pro zajištění monitoringu kybernetické bezpečnosti využito služeb bezpečnostního dohledového centra. Služba zajistí monitoring nad stávajícími informačními systémy a nově dodanými technologiemi a tím eliminuje rizika spojená s nedostatečnou personální kapacitou na úrovni oddělení bezpečnosti a IT. V rámci služeb SOC dojde k napojení současných IS do dohledového centra a zajištění dohledu v režimu technický monitoring v režimu 24x7, operátor v režimu on line 8x5 a v režimu pohotovosti 24x7.

**Součástí ceny SOC musím být všechny potřebné technologie a licence pro poskytování služby.**

**Služba bude dostupná 99,9 % času z režimu 24x7.**

**Výkonový rozsah licence pro LM/SIEM na straně SOC musí být v rozsahu viz požadované parametry jednotlivých technologii výše (viz kapitoly 2 až 6)**

**Požadovaný čas ukládání dát pro ONLINE vyhledávaní je minimálně 100 dní.**

**Požadovaný čas ukládaní dát pro OFFLINE archive je minimálně dalších 200 dní.**

| **ID** | **Popis požadavku** |
| --- | --- |
| SOC01 | Řešení je plnohodnotné – tedy služba, která obsahuje všechny potřebné technologie, procesy, znalosti a obsluhu. |
| SOC02 | Řešení SOC obsahuje z pohledu technologií LM, SIEM, Security Ticketing, Security Dashboard a SOAR. |
| SOC03 | SOC bude poskytovaný jako externí outsourcovaná služba – všechny technologie jsou provozované v prostředí zadavatele, dodavatel potřebné logy / data z těchto technologiích vyhodnocuje ve svém prostředí. Zadavatel připouští alert forwarding směrem k SOC dodavatele. |
| SOC04 | Všechna data budou přenášena do SOC-u v zabezpečené zašifrované formě a musí být chráně vůči neoprávněným změnám/zásahům. |
| SOC05 | Provozu SOCu L1 je zajišťován v režimu 8x5. |
| SOC06 | SoučástíSOC jsou služby certifikovaného CSIRT. CSIRT je certifikovaný minimálně na stupeň "Accredited". |
| SOC07 | Je požadovaná vysoká dostupnost služby SOC provozovaná minimálně ve 2 geograficky oddělených lokalitách pro vykrytí případného výpadku. |
| SOC08 | Provozovatel SOC je certifikovaný na ISO 27000. |
| SOC09 | Všechny aktivity specialistů SOCu jsou auditované na úrovni detailních aktivit (pohyby myší, práce s klávesnicí, obsah obrazovky), které vůči zadavateli vykonávají. Daný nástroj na zajištěni této auditní stopy je součástí technického řešení dodavatele. |
| SOC10 | Řešení SOCu jako služby musí být v souladu se zákonem 181/2014 Sb o kybernetické bezpečnosti (ZoKB). |
| SOC11 | Součástí řešení bude real-time provozní monitoring dostupnosti informačních systémů, kritických aplikaci a síťových prvků s cílem zjistit výpadky procesů a funkčnosti systémů, narušení dostupnosti, včasného identifikovaní bezpečnostních incidentů, resp. omezení účinnosti bezpečnostních opatření. |
| SOC12 | Řešení musí vědět zpracovat i dočasné zvýšený přenos dat (peak) na síti bez jeho zahození/ignorováni. |
| SOC13 | Řešení musí umožňovat rozšíření výkonnosti anebo připojeni monitorovaných zdrojů jen licenčním vypořádáním (škálovatelnost). |
| SOC14 | Řešení je postavené jako otevřené pro zadavatele, zadavatel má přístup do všech častí/technologie minimálně v rozsahu READ ONLY. |
| SOC15 | Součástí služby jsou specialisté bezpečnostního monitoringu v rozsahu L1, L2, L3. |
| SOC16 | Součástí SOC jsou pravidelné schůzky/status meetingy aspoň 1x do měsíčně. |
| SOC17 | Součástí SOC je tvorba Knowledge Base a tvorba RUNBOOKS pro efektivní řešeni bezpečnostních událostí. |
| SOC18 | Součástí SOCu je specializovaný portál, kde jsou dostupné všechny informace na jednom místě v podobě DASHBOARDU. Tento portál poskytuje dashboardy na míru (možnost konfigurace specialisty dodavatele), kde je možné zobrazit informace ze všech komponent SOCu. |
| SOC20 | Řešení bude schopné monitorovat, analyzovat a vyhodnocovat bezpečnostní události, hrozby, útoky a anomálie na základě netflow, pomoci přímého monitoringu v reálném čase a to aj na aplikační vrstvě ISO/OSI, resp. TCP/IP. Technologicky řešení monitoringu netflow zajistí zadavatel. Po provozovateli SOC požaduje jeho napojení do dohledu a konzultace speciality certifikovaného na tuto technologii. |
| SOC21 | Řešení musí umět identifikovat zero-day útoky (např. na základě behaviorální analýzy). |
| SOC22 | Řešení musí umožňovat automatické korelování událostí z vícerých zdrojů, vyhodnoceni incidentů a následné generovaní alertů, a to všechno v reálném čase. |
| SOC24 | Řešení musí primárně využívat bez-agentový sběr logů. Ten typ sběru je preferovaný. Instalace agenta bude umožněna jen v odůvodněných případech Např. pokud není technologicky možné zajistit sběr logů jiným způsobem. |
| SOC25 | Databáze musí být zabezpečená proti manipulaci, tak aby nebylo možné narušit integritu uložených záznamů. |
| SOC26 | Řešení bude podporovat napojeni různých zdrojů obohacujících informací (DNS, IDM, LDAP, ap.). |
| SOC27 | Řešení nesmí způsobit omezení funkcionality, kvality a narušení bezpečnosti jakýchkoliv jiných zařízení / systémů v síti. |
| SOC28 | Řešení bude podporovat možnosti vícenásobné notifikace jednoho alertu. |
| SOC29 | Řešení musí podporovat filtraci a agregaci už na úrovni sběru logů v prostředí zadavatele. |
| SOC30 | Řešení zabezpečí normalizaci logů z různých zdrojů a formátů do jednotného formátu. |
| SOC31 | Řešení bude schopné zaznamenávat a vyhodnocovat minimálně následující detaily bezpečnostních událostí: typ nebo akce, datum a čas, ID systému, který událost zaznamenal, ID systému, kde k události došlo a ID uživatele nebo systému, který akci vyvolal. |
| SOC32 | Řešení SOC využívá SOAR techniky a procesy pro orchestraci a zrychlení threat detection a incident response. |
| SOC33 | Řešení je na úrovni Alertingu provázané s technikami popsanými v knowledge base MITRE ATT&CK. |
| SOC34 | Součástí služby SOCu je měsíčný KPI reporting na míru zákazníka. |
| SOC35 | Samotný poskytovatel SOCu musí nabízet RestAPI (nebo podobné API) rozhraní pro výměnu informací o svých aktivitách, minimálně na úrovni ticketing nástroje. |
| SOC36 | Služba SOCu musí obsahovat funkcionalitu THREATS EXCHANGE, minimálně na úrovni MISP. |