**Technická specifikace pro část 2 - Nástroj pro analýzu datových toků v síti**

Technologie bezpečnostního monitoringu interní sítě OU

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

Nabízená technologie musí být určená pro český trh. SW licence a jejich PN (produktové číselné označení) musí být dostupné přímo v oficiálním ceníku výrobce pro český trh. Podpora na licence ve všech úrovních musí být zajištěna přímo jejich výrobcem, kterého může Objednatel (dále také „zadavatel“) přímo kontaktovat.

|  |  |
| --- | --- |
| **Konkrétní specifikace nabízeného zboží\*** | |
| * **Model – typové/výrobní označení:** |  |
| * **Výrobce:** |  |

*\* Vyplní účastník zadávacího řízení*

Při definici technických požadavků jsou všechny uvedené požadavky závazné. Tyto technické požadavky jsou minimální možné, Poskytovatel (dále také „dodavatel“) může nabídnout charakteristiky (funkce) lepší.

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

**Obecné požadavky**

|  |  |  |
| --- | --- | --- |
| **Požadované funkcionality/vlastnosti** | **Minimální požadavky** | **Splňuje ANO/nabízená hodnota\*** |
| **Systém pro analýzu síťového provozu** | |  |
| Systém musí monitorovat síťovou aktivitu v reálném čase a identifikovat potenciální kybernetické hrozby, bezpečnostní rizika a anomální chování a musí o nich v reálném čase vytvářet upozornění. | **Ano** |  |
| Systém musí monitorovat síťovou aktivitu v reálném čase a identifikovat potenciální kybernetické hrozby, bezpečnostní rizika a anomální chování a musí o nich v reálném čase vytvářet upozornění. | **Ano** |  |
| Dodaný systém musí analyzovat síť na základě zrcadleného síťového provozu ze SPAN portů nebo TAPů (nikoliv jen na základě statistických protokolů typu NetFlow) a zároveň bez potřeby nasazovat agenty na koncové stanice nebo další zařízení v síti. | **Ano** |  |
| Systém musí analyzovat obsah datových paketů v reálném čase a detekovat protokol nebo aplikaci na základě obsahu provozu prostřednictvím DPI (Deep Packet Inspection), nikoli pouze čísla portu. | **Ano** |  |
| Dodaný systém musí být schopen analyzovat síť také na základě zpracování statistických protokolů typu NetFlow, IPFIX, NetStream, Cisco NSEL a případně dalších. | **Ano** |  |
| Systém musí být plně funkční v offline prostředí objednatele bez využití cloudového prostředí pro sběr, ukládání a zpracování dat a veškeré konfigurace a reporting jsou k dispozici přímo v systému. | **Ano** |  |
| Aktualizace systému musí být možné provádět uživatelsky v offline režimu. | **Ano** |  |
| **Zpracování a ukládání síťových toků** | |  |
| Systém ukládá síťové toky ve formátu, který umožní analýzu síťové komunikace na úrovni jednotlivých toků, včetně dohledání informací o aplikačních transakcích a jejich metadatech z L2 až L7, obsažených v daném síťovém toku. | **Ano** |  |
| Požadované protokoly pro ukládání aplikačních metadat z jednotlivých transakcí jsou: DHCP, DNS, SMB, HTTP, HTTPS, SMTP, SMTPS, POP3, IMAP, SSH, LDAP, LDAPS, KERBEROS, SNMP, CIFS, MSSQL, RDP, SIP, TELNET, FTP, FTP-DATA, TFTP, TFTP-DATA, NFS, ARP, SSL/TLS zapouzdření. | **Ano** |  |
| Je požadováno využití vysokorychlostní úložiště pro uchování historie datových toků na dobu minimálně 6 měsíců složené z SSD disků. | **Ano** |  |
| **Analýza aplikačních a systémových logů** | | |
| Systém musí být schopen sbírat a analyzovat aplikační a systémové logy ve formátu syslog z dohledovaných zařízení a identifikovat nebezpečné nebo potenciálně škodlivé aktivity. | **Ano** |  |
| **Uživatelské 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. | **Ano** |  |
| Systém musí být schopen vytváření profilů a skupin uživatelů pro omezení funkcionality produktu a viditelnosti uložených dat s podporou minimálně: |  |  |
| * granulárního nastavení přístupu k analytickým i konfiguračním/administrativním komponentám systému s definovanými úrovněmi přístupu (alespoň read, write, execute), | **Ano** |  |
| * granulárního nastavení přístupu k datům z různých segmentů sítě organizace s definovanými úrovněmi přístupu (alespoň read, write, execute), | **Ano** |  |
| * vytváření vlastních filtrů veškerých dat a jejich sdílení mezi uživateli a skupinami uživatelů, | **Ano** |  |
| * vytváření vlastních uživatelských pohledů, reportů, dashboardů apod. | **Ano** |  |
| **Automatické hlášení (alerty) a reporting** | |  |
| Systém musí být schopen upozorňovat uživatele prostřednictvím minimálně emailu a logu o všech identifikovaných událostech a dále o událostech filtrovaných minimálně dle IP a MAC adresy, podsítě, závažnosti události, kategorie události, země, uživatele, síťové služby, čísla portu, provozu do/z internetu. | **Ano** |  |
| Tyto alerty musí být systém schopen dodávat i ve strojově čitelném formátu pro vyžití v nástrojích typu SIEM a musí obsahovat minimálně kompletní informace o detekované události včetně URL odkazu na danou událost v reportovaném období do grafického rozhraní systému. | **Ano** |  |
| Systém musí mít možnost vytváření automatizovaných manažerských reportů o stavu kybernetické bezpečnosti z pohledu zprávy kybernetických incidentů ideálně dle oblastí jejich vzniků (např.: doména, web, email apod.). | **Ano** |  |
| Je požadováno vytváření automatizovaných reportů v českém jazyce. | **Ano** |  |

*\* Vyplní účastník zadávacího řízení*

**Požadavky na architekturu nasazení**

|  |  |  |
| --- | --- | --- |
| **Požadované funkcionality/vlastnosti** | **Minimální požadavky** | **Splňuje ANO/nabízená hodnota\*** |
| **Požadavky pro pokrytí IT prostředí** | |  |
| V síti je předpokládáno cca 8000 aktivních IP adres s průměrným celkový průtokem max. 2Gbps. | **Ano** |  |
| Je požadován 1x SW/VA datový kolektor/sensor o celkové propustnosti minimálně 2Gbps s podporou monitorovacích rozhraní 4x 1GE, 2x10GE, 2x 25GE a 2x40GE.  Na zařízení je požadována dostupná historie dat minimálně 6 měsíců zpětně, uložená na rychlém úložišti typu SSD. | **Ano** |  |
| Je požadován 1x SW/VA datový sensor o celkové propustnosti minimálně 1000Mbps. | **Ano** |  |

*\* Vyplní účastník zadávacího řízení*

**Požadavky na schopnost detekce bezpečnostních událostí**

|  |  |  |
| --- | --- | --- |
| **Požadované funkcionality/vlastnosti** | **Minimální požadavky** | **Splňuje ANO/nabízená hodnota** |
| **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, | **Ano** |  |
| * duplicitní IP/MAC adresa, | **Ano** |  |
| * změna VLAN, | **Ano** |  |
| * vytvoření nové podsítě, | **Ano** |  |
| * připojení nového zařízení, | **Ano** |  |
| * použití nebo vznik nové služby, | **Ano** |  |
| * nedostupnost dříve dostupné a komunikující služby nebo dříve dostupného a komunikujícího zařízení, | **Ano** |  |
| * přístup nového zařízení ke službě či zařízení | **Ano** |  |
| * ověřování platnosti interních certifikátu pro validní TLS šifrování u HTTPS a upozornění před datem jejich vypršení. | **Ano** |  |
| 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. | **Ano** |  |
| **Samostatné učení behaviorálních aktivit a detekce anomálií** | |  |
| Systém musí používat matematické metody samostatného učení pro analýzu síťové aktivity, vytvářet a v čase automaticky modifikovat modely chování na základě běžného chování jednotlivých zařízení a na nich provozovaných služeb v rámci celé organizace. | **Ano** |  |
| Systém musí mít schopnost na základě matematického modelu daného zařízení a jeho služeb identifikovat nestandardní síťové chování, a to zejména odchylky od modelu normálního chování pro: |  |  |
| * odchylku od modelu pro přenos dat, toků a paketů, | **Ano** |  |
| * odchylku od modelu pro počet komunikačních partnerů, | **Ano** |  |
| * odchylku od modelu entropie na komunikačních portech, | **Ano** |  |
| * odchylku od modelu pro počet síťových toků a využitých síťových služeb, | **Ano** |  |
| * odchylku od modelu výkonnosti sítě (rychlost přenosu) a aplikací (doba odezvy). | **Ano** |  |
| 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. | **Ano** |  |
| **Identifikace neznámých hrozeb a podezřelých chování** | |  |
| 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, | **Ano** |  |
| * detekce podezřelého strojového chování, které nevytvářejí lidští uživatelé sítě, | **Ano** |  |
| * detekce repetitivních vzorců chování na síti, | **Ano** |  |
| * detekce botnetů a ovládání kompromitované stanice, | **Ano** |  |
| * detekce příznaků těžení kryptoměn, | **Ano** |  |
| * útoky hrubou silou a enumerace dat, | **Ano** |  |
| * rozpoznání tunelovaného síťového provozu – alespoň IPv4 prostřednictvím IPv6 a DNS tunely. | **Ano** |  |
| **Detekce na základě databáze známých hrozeb** | |  |
| Systém musí být schopen identifikovat hrozby a reportovat události na základě |  |  |
| * detekční databáze známých hrozeb, tj. malware (trojské koně, viry, červy, rootkity, apod.), známých útoků (exploity) a zranitelností, porušení bezpečnostních pravidel a „best practices“ a dalších rizik, | **Ano** |  |
| * reputační databáze známých škodlivých IP adres, TLS certifikátů, záznamů DNS a hostname, URL adres a hashů souborů. | **Ano** |  |
| Tyto databáze musí být aktualizované minimálně na hodinové bázi. Nesmí se jednat pouze o volně dostupné/open-source databáze, ale musí se jednat o komerční databázi renomovaného vendora nebo poskytovatele těchto služeb. | **Ano** |  |
| Uživatel musí být schopen importovat vlastní záznamy. | **Ano** |  |
| Systém musí využívat tuto detekci pro veškerý monitorovaný provoz (na perimetru i v interní síti mezi všemi segmenty), nikoliv pouze pro omezený segment nebo podmnožinu celkové komunikace. | **Ano** |  |
| 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 detekovat události na základě vysokého počtu signaturních pravidel (minimálně několik desítek tisíc). | **Ano** |  |
| Uživatel musí být schopen přidávat vlastní detekční pravidla v praktickém a obecně využívaném formátu.  Příklad možné syntaxe detekčního pravidla:  *alert tcp $HOME\_NET any -> any any (msg:”Command Shell Access”; content:”C:\\Users\\Administrator\\Desktop\\hfs2.3b”; sid:1000001; rev:1;)* | **Ano** |  |
| **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. | **Ano** |  |
| **Asistované učení** | |  |
| Je požadován uživatelsky přívětivý proces vytváření pravidel pro zpřesnění detekce a eliminaci falešně pozitivní detekce, a to na základě minimálně následujících parametrů: |  |  |
| * IP adresa, | **Ano** |  |
| * MAC adresa, | **Ano** |  |
| * hostname, | **Ano** |  |
| * segment sítě / podsíť, | **Ano** |  |
| * lokalita – ASN, země, apod. | **Ano** |  |
| * směr komunikace – určení klienta, nebo serveru, | **Ano** |  |
| * detekovaná událost – kategorie, název apod. | **Ano** |  |
| * použité služby, protokolu, portu, | **Ano** |  |
| * libovolné kombinaci výše popsaných. | **Ano** |  |
| Systém musí být schopen eliminovat falešné alarmy i pro události detekované v historii. | **Ano** |  |

*\* Vyplní účastník zadávacího řízení*

**Požadavky na zajištění síťové viditelnosti**

|  |  |  |
| --- | --- | --- |
| **Požadované funkcionality/vlastnosti** | **Minimální požadavky** | **Splňuje ANO/nabízená hodnota** |
| **Vyhledávání, filtrování a vizualizace dat** | | |
| Systém musí být schopen okamžitého (v řádu vteřin) vyhledávání a vizualizace pro forenzní analýzu a podporu threat hunting bez zvláštního dotazovacího jazyka. | **Ano** |  |
| Jedná se o možnost okamžitě filtrovat a vyhledávat v plné historii všech uložených dat, tj. bezpečnostních událostí, síťových toků a agregovaných síťových statistikách (tabulky a grafy), a to minimálně: |  |  |
| * podle parametrů IP a MAC adresa, hostname, username (identita uživatele), příchozí a odchozí provoz, síťová služba, lokální nebo vzdálená služba (služba z pohledu klient nebo server), číslo portu, VLAN, země, ASN, | **Ano** |  |
| * prostřednictvím full-textového vyhledávání v datech a vyhledávání na základě definice směru (zdroj, cíl) a logických výrazů and, or, not. | **Ano** |  |
| Systém musí pro vyhledávání poskytovat již předpočítané hodnoty výkonnostních a behaviorálních charakteristik pro každé zařízení v síti a pro všechny na něm provozované služby, bez nutnosti zpracování surových dat ze síťových logů. | **Ano** |  |
| Systém musí být schopen filtrovat a vizualizovat výsledky v grafech, výčtových tabulkách s možností řazení a TOP N statistikách. | **Ano** |  |
| 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, RDP, ARP, MS-SQL, SIP, Kerberos, SSL/TLS. | **Ano** |  |
| Systém umožnuje provádět uživatelsky jednoduché a okamžité vizualizace síťových prostupů mezi zařízeními a podsítěmi. Využitím uživatelského datového filtru lze vizualizační pohledy libovolně modifikovat. | **Ano** |  |
| **Kontextuální informace** | | |
| Systém musí být schopen pro každé zařízení získávat, vizualizovat a v jednom grafickém pohledu zobrazovat kontextuální informace: |  |  |
| * jméno uživatele a další jeho parametry z doménového řadiče (MS Active Directory), včetně její historie | **Ano** |  |
| * hostname zařízení a jeho historie na základě zpracování relevantních dat z DNS a DHCP provozu | **Ano** |  |
| * IP geolokace | **Ano** |  |
| * IP reputace, vč. údaje, jestli je IP adresa na blacklistu nebo podezřelá | **Ano** |  |
| * historie použitých MAC adresa a výrobce zařízení | **Ano** |  |
| * operační systém a jeho historie na zařízení | **Ano** |  |
| * uživatelem zadané poznámky a informace k zařízení | **Ano** |  |
| * automaticky přiřazené značky/tagy zařízení, které popisují jejich účel a chování – alespoň server doménového řadiče, webový server, poštovní server, server DNS, server SSH, databázový server, tiskárna, administrátorské zařízení, datové úložiště, aktivní dohledy, skenery zranitelností a technologické systémy. | **Ano** |  |
| **Zaznamenávání a ukládání plného provozu** | | |
| Je požadováno volitelné nahrávání plného síťového provozu (full packet capture) ve formátu PCAP na všech dodaných zařízeních minimálně na základě parametrů: cílová a zdrojová IP/MAC adresa, podsíť, využitý protokol, IPv4 nebo IPv6. Zaznamenávání je možno zapínat automaticky dle detekovaných událostí, nebo uživatelskou aktivací. | **Ano** |  |

*\* Vyplní účastník zadávacího řízení*

**Další požadované oblasti využití**

|  |  |  |
| --- | --- | --- |
| **Požadované funkcionality/vlastnosti** | **Minimální požadavky** | **Splňuje ANO/nabízená hodnota** |
| **Monitorování politik kybernetické bezpečnosti** | | |
| Systém musí umožňovat vytváření komplexních komunikačních a bezpečnostních politik, a to minimálně: |  |  |
| * monitorovat definovanou komunikační matici a detekovat, kdy jsou tyto matice porušeny – alespoň jaké zařízení smí komunikovat s jakým zařízením, přes jaký protokol, v jakém čase. | **Ano** |  |
| * detekce změn v síti – přinejmenším nové komunikační vektory, nová nebo změněná zařízení a podsítě, obcházení perimetru. | **Ano** |  |
| Pro účely monitorování politik kybernetické bezpečnosti musí systém poskytovat uživatelský rámec pro definování pravidel pomocí: |  |  |
| * uživatelem definované podsítě na základě rozsahů IP adres | **Ano** |  |
| * uživatelsky libovolně definovaných skupin zařízení | **Ano** |  |
| * automaticky přiřazené značky/tagy zařízení, které popisují jejich účel a chování – alespoň server doménového řadiče, webový server, poštovní server, server DNS, server SSH, databázový server, tiskárna, administrátorské zařízení, datové úložiště, aktivní dohledy, skenery zranitelností a technologické systémy. | **Ano** |  |
| **Detekce úniku dat** | |  |
| Systém musí být schopen detekovat přenosy citlivých souborů a dat definovaných pomocí jejich názvů, hashů, specifického binárního obsahu (vodoznaku) nebo regulárních výrazů (např. rodné číslo). | **Ano** |  |
| Systém musí být schopen detekovat přenosy citlivých souborů a dat alespoň u následujících protokolů: HTTP, FTP, SMTP, SMB, NFS. | **Ano** |  |
| V rámci historických metadat u HTTP, FTP, SMTP, SMB a NFS je požadováno ukládání informací o všech po síti přenášených souborech alespoň v rozsahu: |  |  |
| * název souboru, | **Ano** |  |
| * velikost souboru, | **Ano** |  |
| * HASH souboru. | **Ano** |  |
| **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) model normálního chování pro výkonnostní parametry minimálně: |  |  |
| * přenosová rychlost sítě, | **Ano** |  |
| * rychlost odezvy aplikace, | **Ano** |  |
| * odezva systému z pohledu uživatele. | **Ano** |  |
| Výpočet uvedených výkonnostních parametrů a automatická a detekce anomálií na základě odchylky od modelu normálního chování musí být prováděna pro: |  |  |
| * všechny porty a služby TCP, | **Ano** |  |
| * pro všechny kombinace služeb a zařízení. | **Ano** |  |
| Systém musí v celé monitorované síti, mezi všemi zařízeními a na všech službách měřit informace o retransmission paketech, out of order paketech, TTL, QoS a komunikaci blokované firewally. | **Ano** |  |
| **Monitoring cloudových služeb** | |  |
| Systém musí být schopen monitorovat přístupy zařízení a uživatelů ke cloudovým službám, a to minimálně Google Workspace a Microsoft Office 365, vč. monitoringu operací se soubory, změn oprávnění a nastavení a neúspěšných přístupů. | **Ano** |  |
| Systém musí být schopen tyto informace autonomně a průběžně získávat z aplikačních rozhraní těchto cloudových služeb bez nutnosti využití řešení třetích stran. | **Ano** |  |

*\* Vyplní účastník zadávacího řízení*

**Implementační služby**

Všechna dodavatelem instalovaná zařízení nebo komponenty musí být dodavatelem profesionálně nainstalovány a zprovozněny, vč. prokázání, že tato zařízení plní všechny požadované a výkonnostní parametry.

Všechna dodavatelem instalovaná zařízení budou zabezpečena a nebudou obsahovat zjevná rizika a zranitelnosti, a to po celou dobu provozu služby.

Řešení musí splňovat bezpečnostní kritéria podle Zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů, a nebude v rozporu s požadavky Národního úřadu pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“) pro provoz významných informačních systémů;

Zadavatel je povinen dle §5 Vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), ve znění pozdějších předpisů, provádět analýzu rizik a identifikovaná rizika řídit. Současně je zadavatel povinen zabývat se všemi hrozbami, které prostřednictvím varování vydává NÚKIB a zohlednit je v analýze rizik. Zadavatel proto provedl, s přihlédnutím k vydanému "varování" NÚKIB, analýzu rizik a v hodnocení se řídil pokyny uvedenými v dokumentu NÚKIB "Metodika k varování ze dne 17. prosince 2018". Veškerá bezpečnostní opatření, která bude nutné u dodaného řešení na základě výsledků analýzy rizik přijmout, nesmí pro zadavatele znamenat žádné další náklady.

**Produktová podpora výrobce**

Dodavatel musí zajistit:

* softwarovou produktovou podporu řešení v délce 12 měsíců od podepsání akceptačního protokolu po předáním monitorovacího systému.

**Administrátorské školení**

V rámci realizace je požadováno administrátorské školení pro zaměstnance zadavatele v rozsahu nezbytném pro kvalifikovanou obsluhu.

**Akceptační podmínky**

Předpokladem pro předání řešení do provozu bude splnění následujících akceptačních testů.

* Veškeré komponenty systému jsou řádně licencované.
* Byly dodány SW licence dle požadované technické specifikace.
* Všechny SW komponenty systému jsou nainstalovány a napojeny na infrastrukturu zadavatele.
* Dochází k záznamu flow a zrcadleného provozu, informace jsou dostupné k zobrazení a dalšímu zpracování.
* Výsledná informace (graf nebo tabulka) definovaná libovolně nastaveným základním filtrem (např. IP adresa, podsíť, služba, událost, …) v 24hodinovém intervalu musí být zobrazena do 20s.
* Funguje asistované učení při označení falešně pozitivní detekce.
* Systém korektně načítá VLAN-ID ze zrcadlené komunikace a umožňuje filtrování informací podle VLAN-ID.
* Systém zobrazuje netflow na základě adres nebo portů po překladu NAT.
* Systém graficky znázorňuje skutečně přenesená data (In/Out) filtrovaná podle jednotlivých zdrojů flow nebo fyzických/logických interface.
* Systém detekuje známé hrozby na základě databáze známých hrozeb (je aktivně využíváno alespoň 40.000 detekčních pravidel/signatur a alespoň 100.000 záznamů typu Threat Intelligence).
* Systém detekuje anomálie na základě dynamicky se měnících modelů chování jednotlivých zařízení, systém má nastavené (samostatně naučené) prahové hodnoty, na základě kterých detekuje anomálie. Prahové hodnoty jsou jasně viditelné pro každé zařízení a každou jeho službu.
* Bylo provedeno školení v požadovaném rozsahu, tak aby vyškolené osoby /min 3 osoby/ byly schopny zajistit komplexní obsluhu systému.

Na závěr zástupci zadavatele potvrdí splnění všech akceptačních podmínek pro předání řešení do provozu potvrzením „akceptačního protokolu“.