## Příloha číslo 1. ZD - Technická specifikace

Předmětem zakázky je komplexní zajištění služeb dohledového centra kybernetické bezpečnosti (SOC – Security Operation Centrum), především:

* formou služby provozovat centralizovanou správu, ukládání a vyhodnocování logů v nezměnitelné podobě ze síťových aktivních prvků, operačních systémů a používaného aplikačního software, tj. nástroje (NetFlow, Firewall, Logmanagement, Provozní monitoring). Implementace systému bude provedena v souladu s §23 Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí.
* formou služby provozovat centralizovanou správu, ukládání a vyhodnocování komunikačních spojení a výkonnostních parametrů datové sítě, tj. nástroj sběru a vyhodnocení NetFlow. Implementace systému bude provedena v souladu s §22 Nástroj pro detekci kybernetických bezpečnostních událostí.
* Systém musí provádět analýzu síťového provozu a bezpečnostní monitoring v prostředí technologické a klasické sítě, který okamžitě identifikuje bezpečnostní rizika a události a který splňuje klíčové požadavky uvedené níže.
* Nabízená technologie musí být určená pro český trh. HW a 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.
* Objednatel požaduje uživatelský přístup ke čtení do nástroje GREYCORTEX MENDEL, případně srovnatelné eventuálnosti pro dispečink SCADA systémů.
* 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 Systému dodána/naimplementována a případně licencována. Tyto technické požadavky jsou minimální možné, Poskytovatel (dále také „dodavatel“) může nabídnout charakteristiky (funkce) lepší.

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

*Popis nabízených komponent musí dodavatel zpracovat podle následujících podmínek:*

* 1. *Ve 2. sloupci následujících tabulek v každém řádku dodavatel potvrdí, že splňuje požadované technické podmínky uvedené v 1. sloupci tabulky slovem „ANO“ 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 dodavatel splňuje anebo překračuje požadované technické podmínky.*
  2. *Údaje stanovené zadavatelem v 1. sloupci tabulky nesmí být měněny, vynechány nebo jinak přeskupeny.*
  3. *Výčet požadované konfigurace může dodavatel doplnit o další řádky na konci tabulky s užitečnými údaji nebo parametry o nabízené komponentě.*

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

## Obecné požadavky

|  |  |
| --- | --- |
| **Požadované funkcionality/vlastnosti** | **Nabízené řešení splňuje/nesplňuje,** vč. vysvětlení jak je zadání splněno |
| **Systém pro analýzu síťového provozu** | |
| Systém složený z hardwarových zařízení 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. |  |
| 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. |  |
| 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. |  |
| Dodaný systém musí být schopen analyzovat síť také na základě zpracování statistických protokolů typu NetFlow, IPFIX, NetStream, Cisco NSEL a případně dalších. |  |
| 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. |  |
| Aktualizace systému musí být možné provádět uživatelsky v offline režimu. |  |
| **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. |  |
| Požadované protokoly pro ukládání aplikačních metadat z jednotlivých transakcí jsou: MODBUS, PROFINET, DCE/RPC, 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. |  |
| Je požadováno vysokorychlostní úložiště pro uchování historie datových toků na dobu minimálně 18 měsíců složené z SSD disků. |  |
| **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. |  |
| **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. |  |
| 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), |  |
| * granulárního nastavení přístupu k datům z různých segmentů sítě organizace s definovanými úrovněmi přístupu (alespoň read, write, execute), |  |
| * vytváření vlastních filtrů veškerých dat a jejich sdílení mezi uživateli a skupinami uživatelů, |  |
| * vytváření vlastních uživatelských pohledů, reportů, dashboardů apod. |  |
| **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. |  |
| 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. |  |
| 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.). |  |
| Je požadováno vytváření automatizovaných reportů v českém jazyce. |  |
| **Integrace systému** | |
| Systém musí poskytovat hotové nástroje umožňující integraci se softwarem třetích stran bez použití API systému, a to minimálně: |  |
| * syslog, CEF a LEEF pro export událostí včetně plné podpory filtrů (exportování pouze požadovaných dat) |  |
| * přímé url odkazy na libovolnou obrazovku grafického uživatelského rozhraní a filtrovaná zobrazení v grafickém uživatelském rozhraní |  |
| * export informací o toku ve formátu IPFIX nebo podobném formátu včetně plné podpory filtrů (exportovat lze pouze požadovaná data) |  |
| * integrace se službami identity uživatelů bez nutnosti konfigurace zasílání logů do systému – minimálně Cisco ISE a Microsoft Active Directory |  |
| * integrace s firewally, alespoň Palo Alto, Fortinet a Checkpoint, pro automatické a manuální reakce vyvolané systémem |  |
| * integrace s nástroji pro řízení přístupu k síti minimálně Cisco ISE, pro automatickou a manuální reakci systému. |  |

## Požadavky na architekturu nasazení

|  |  |
| --- | --- |
| **Požadované funkcionality/vlastnosti** | **Nabízené řešení splňuje/nesplňuje,** vč. vysvětlení jak je zadání splněno |
| **Obecné požadavky pro nasazení** | |
| Pro všechny HW komponenty senzor a kolektor je požadován formát 1U nebo 2U server o velikosti 19“. |  |
| Pro všechny HW komponenty senzor a kolektor je požadován duální zdroj napájení se schopností hot-swap. |  |
| Pro všechny HW komponenty senzor a kolektor je požadováno samostatné síťové rozhraní pro vzdálenou správu serveru v případě výpadku systému typu IPMI, IDRAC, ILO apod. |  |
| **Požadavky pro pokrytí IT a OT prostředí** | |
| V síti je předpokládáno cca do 1000 aktivních zařízení s průměrným celkový průtokem do 500Mbps, ve špičce do 6Gbps |  |
| Je požadován 1x HW datový kolektor/sensor o celkové propustnosti minimálně 1Gbps s monitorovacím rozhraním 2x 1GE a 2x10/25GE.  Na zařízení je požadována dostupná historie dat minimálně 18 měsíců zpětně, uložená na rychlém úložišti typu SSD o velikosti alespoň 6TB. Požadován je minimálně RAID10 nebo RAID6 se schopností hot-swap. |  |
| Je požadován 10x HW datový sensor o propustnosti minimálně 100Mbps s monitorovacím rozhraním 2x 1GE. |  |

## Požadavky na schopnost detekce bezpečnostních událostí

|  |  |
| --- | --- |
| **Požadované funkcionality/vlastnosti** | **Nabízené řešení splňuje/nesplňuje,** vč. vysvětlení jak je zadání splněno |
| **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 nebo vznik nové služby, |  |
| * nedostupnost dříve dostupné a komunikující služby nebo dříve dostupného a komunikujícího zařízení, |  |
| * přístup nového zařízení ke službě či zařízení |  |
| * ověřování platnosti interních certifikátu pro validní TLS šifrování u HTTPS a upozornění před datem jejich vypršení. |  |
| 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. |  |
| **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. |  |
| 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, |  |
| * odchylku od modelu pro počet komunikačních partnerů, |  |
| * odchylku od modelu 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 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, |  |
| * detekce podezřelého strojového chování, které nevytvářejí lidští uživatelé sítě, |  |
| * detekce repetitivních vzorců chování na síti (označováno jako beaconing), |  |
| * 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** | |
| Systém musí být schopen identifikovat hrozby a reportovat události na základě |  |
| * detekční databáze známých hrozeb, tj. malware, známých útoků a zranitelností, porušení bezpečnostních pravidel a „best practices“ a dalších rizik, |  |
| * reputační databáze známých škodlivých IP adres, TLS certifikátů, záznamů DNS a hostname, URL adres a hashů souborů. |  |
| 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. |  |
| Uživatel musí být schopen importovat vlastní záznamy. |  |
| 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. |  |
| 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). |  |
| 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;)* |  |
| **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. |  |
| **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, |  |
| * MAC adresa, |  |
| * hostname, |  |
| * segment sítě / podsíť, |  |
| * lokalita – ASN, země, apod. |  |
| * směr komunikace – určení klienta, nebo serveru, |  |
| * detekovaná událost – kategorie, název apod. |  |
| * použité služby, protokolu, portu, |  |
| * libovolné kombinaci výše popsaných. |  |
| Systém musí být schopen eliminovat falešné alarmy i pro události detekované v historii. |  |

## Požadavky na zajištění síťové viditelnosti

|  |  |
| --- | --- |
| **Požadované funkcionality/vlastnosti** | **Nabízené řešení splňuje/nesplňuje,** vč. vysvětlení jak je zadání splněno |
| **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. |  |
| 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, příchozí a odchozí provoz, síťová služba, lokální nebo vzdálená služba (služba z pohledu klient nebo server), číslo portu, VLAN, země, ASN, |  |
| * prostřednictvím full-textového vyhledávání v datech a vyhledávání na základě definice směru (zdroj, cíl) a logických výrazů and, or, not. |  |
| Systém musí pro vyhledávání poskytovat již předpočítané hodnoty výkonnostních a behaviorálních charakteristik pro každé zařízení a pro všechny na něm provozované služby, bez nutnosti zpracování surových dat ze síťových logů. |  |
| Systém musí být schopen filtrovat a vizualizovat výsledky v grafech, výčtových tabulkách s možností řazení a TOP N statistikách. |  |
| 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, MODBUS. |  |
| Systém umožnuje provádět uživatelsky jednoduché a okamžité vizualizace síťových prostupů mezi zařízeními a podsítěmi. Využitím uživatelského datového filtru lze vizualizační pohledy libovolně modifikovat. |  |
| **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 |  |
| * hostname zařízení a jeho historie na základě zpracování relevantních dat z DNS a DHCP provozu |  |
| * IP geolokace |  |
| * IP reputace, vč. údaje, jestli je IP adresa na blacklistu nebo podezřelá |  |
| * historie použitých MAC adresa a výrobce zařízení |  |
| * operační systém a jeho historie na zařízení |  |
| * uživatelem zadané poznámky a informace k zařízení |  |
| * automaticky nebo uživatelem vytvořené značky/tagy zařízení, které popisují jejich chování – alespoň server doménového řadiče, webový server, poštovní server, server DNS, server SSH, databázový server, tiskárna, administrátorské zařízení, datové úložiště, kamerové systémy, aktivní dohledy, skenery zranitelností a technologické systémy vč. PLC, historian, pracovní stanice a další zařízení ICS/SCADA. |  |
| **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. |  |

## Požadavky na monitoring technologické sítě

|  |  |
| --- | --- |
| **Požadované funkcionality/vlastnosti** | **Nabízené řešení splňuje/nesplňuje,** vč. vysvětlení jak je zadání splněno |
| **Podpora průmyslových protokolů** | |
| Řešení musí podporovat analýzu a ukládání aplikačních metadat pro průmyslové/OT protokoly využívané v prostředí VAK PCE. |  |
| Jsou vyžadována podpora minimálně těchto protokolů: ModBus, ProfiNet, TELNET, http-service, S7, DCE/RPC, SNMP, BACnet, CC-link, Ethercat. |  |
| **Aktivní získávání informací**  Řešení umožňuje aktivní dotazování (tzv. active polling pověřený uživatelem a bezpečný pro monitorovaná zařízení) pro zjištění a identifikaci verze firmware, typu zařízení a konfigurační nastavení prostřednictvím příslušných průmyslových protokolů. Tyto informace je nutné (dle potřeb a nastavení uživatele) s příslušnou pravidelnosti ověřovat a hlásit případné změny. |  |
| **Pasivní získávání informací**  Základní informace o zařízení jako operační systém, výrobce zařízení a použité aplikace a služby musí být získávány pasivní analýzou komunikace. |  |
| **Informace o přítomných zranitelnostech CVE**  Systém musí být schopen informovat na základě identifikovaných verzí firmware, výrobce a operačních systémů průmyslových/technologických zařízení o přítomnosti známých zranitelností na základě aktuální databáze CVE. |  |
| **Detekce známých hrozeb v prostředí technologické sítě**  Systém musí být schopen identifikovat a reportovat události na základě detekční databáze známých útoků a zranitelností příslušných průmyslových/technologických zařízení na základě analýzy síťového provozu L2 až L7 ISO/OSI modelu. |  |
| **Detekce anomálií v prostředí technologické sítě**  Systém musí být schopen identifikovat anomální stavy a nebezpečné aktivity typu:   * Změna data * Stažení software * Update firmware * Změna informací o zařízení * Změna IP adresy * Neobvyklá adresa přistupující k zařízení * Změna módu kontroléru - run/stop/program * Detekce systémových funkcí jako - reboot, upload,… * Neúspěšný přístup k HMI, Engineering atd. * Nový přístup k technologickým i řídícím zařízením. |  |
| **Pokročilá detekce v prostředí technologické sítě**  Systém musí být schopen kontrolovat a interně korelovat parametry předávané mezi jednotlivými prvky OT a řídícími SCADA prvky prostřednictvím příslušných průmyslových protokolů. Zejména se jedná o:   * Modifikace dat přecházející mezi PLC, Engineering stanicí, Historian DB apod. * Podvržení řídících dat * Časová desynchronizace * Podvržené datové smyčky a přehrávání neplatných dat * Podvržené přístupy oprávněných uživatelů * Jiné typy útoků |  |
| **Analýza logů technologických zařízení**  Systém musí být schopen analyzovat systémové logy ve formátu syslog z průmyslových i IT zařízení a identifikovat nebezpečné nebo potenciálně škodlivé aktivity. |  |
| **Kategorizace nálezů v prostředí OT**  Systém musí být schopen kategorizovat jednotlivá zařízení a vizualizovat celou síť dle obecného OT schématu **Purdue network model**. Dále je požadována klasifikace identifikovaných hrozeb dle **Mitre ICS framework**. |  |

## Další požadované oblasti využití

|  |  |
| --- | --- |
| **Požadované funkcionality/vlastnosti** | **Nabízené řešení splňuje/nesplňuje,** vč. vysvětlení jak je zadání splněno |
| **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. |  |
| * detekce změn v síti – přinejmenším nové komunikační vektory, nová nebo změněná zařízení a podsítě, obcházení perimetru. |  |
| Pro účely monitorování politik kybernetické bezpečnosti musí systém poskytovat uživatelský rámec pro definování pravidel pomocí: |  |
| * uživatelem definované podsítě na základě rozsahů IP adres |  |
| * uživatelsky libovolně definovaných skupin zařízení |  |
| * automaticky nebo uživatelem vytvořené značky/tagy zařízení, které popisují jejich chování – alespoň server doménového řadiče, webový server, poštovní server, server DNS, server SSH, databázový server, tiskárna, administrátorské zařízení, datové úložiště, kamerové systémy, aktivní dohledy, skenery zranitelností a technologické systémy vč. PLC, historian, pracovní stanice a další zařízení ICS/SCADA. |  |
| **Management bezpečnostních událostí a incidentů** | |
| Systém musí poskytovat funkcionalitu pro reporting bezpečnostních incidentů (prohlášení identifikované události za bezpečnostní incident), včetně: |  |
| * spolupráci a sdílení informací při analýze identifikovaných bezpečnostních incidentů včetně potřebného workflow mezi jednotlivými uživateli s podporou automatizovaných oznámení o změně stavu události či přiřazení řešitele, |  |
| * jednoduché sdílení informací o bezpečnostních incidentech, včetně uživatelem zadaných komentářů, |  |
| * možnost vyhledávání a filtrování nad všemi událostmi z pohledu workflow bezpečnostního incidentů (reportovaná událost, událost v řešení, vyřešená událost, události v řešení daného uživatele apod.), |  |
| * možnost exportování dat do emailu, csv, pdf, syslogu a podobně, |  |
| * možnost exportu bezpečnostních událostí a incidentů do systémů typu ticket management třetích stran. |  |
| **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). |  |
| Systém musí být schopen detekovat přenosy citlivých souborů a dat alespoň u následujících protokolů: HTTP, FTP, SMTP, SMB, NFS. |  |
| 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, |  |
| * 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) model normálního chování pro výkonnostní parametry minimálně: |  |
| * přenosová rychlost sítě, |  |
| * rychlost odezvy aplikace, |  |
| * odezva systému z pohledu uživatele. |  |
| 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, |  |
| * pro všechny kombinace služeb a zařízení. |  |
| 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. |  |
| **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. |  |
| Systém musí být schopen tyto informace autonomně a průběžně získávat z aplikačních rozhraní těchto cloudových služeb bez nutnosti využití řešení třetích stran. |  |
| **Inventarizace sítě a grafický vizualizace topologie** | |
| Systém musí být schopen zobrazit celý inventář monitorované sítě s počtem zařízení v jednotlivých lokalitách, segmentech, nebo podsítích. Včetně detailního přehledu zařízení. |  |
| Systém musí být schopen graficky vykreslit celou topologii sítě, dle zaznamenané komunikace. |  |
| Systém musí být schopen zobrazit inventář jednotlivých lokalit, přehledy zařízení, přehledy výrobců, tagy zřízení, uživatele. |  |
| Systém umožnuje všechny inventory informace řadit dle různých parametrů. |  |
| **Monitoring automatizace budov** | |
| Systém musí být schopen monitorovat síťový provoz v technologické síti a: |  |
| * identifikovat zařízení v technologické síti a informace o těchto zařízeních: minimálně výrobce, výrobní číslo, verze HW, verze firmware, |  |
| * detekce běžných útoků, zneužití zranitelností, chybných konfigurací a porušení zásad dobré praxe v technologické síti, |  |
| * automatizovaně měřit výkon zařízení v technologické síti a detekci anomálií – alespoň pomalá doba odezvy, porucha a restart systému řízení budovy atd., |  |
| * zajistit úplný přehled o provozovaných protokolech automatizace budov, přinejmenším CC-Link, BACnet, KNX, MQTT, Modbus. |  |

## Služby SOC

|  |  |  |
| --- | --- | --- |
| **Minimální technické požadavky, které Zadavatel požaduje** | | **Splnění požadavků Zadavatele (ANO/NE)** |
|  | **Požadavky na služby SOC** |  |
| 1. | Zadavatel předpokládá realizaci uvedených úloh prostředky a technologiemi zadavatele, nejméně v rozsahu řešení sběru NetFlow, Firewall, Logmanagement, Provozní monitoring, které zadavatel již vlastní. Služba poskytovatele zohlední přítomnost těchto prostředků na straně zadavatele v tom smyslu, že jako primární a rozhodné nástroje dodavatel využije tyto prostředky a celý rozsah služby bude provádět jejich prostřednictvím. |  |
| 2. | Bezpečnostní dohledové centrum poskytovatele služby musí podporovat práci s nástroji zadavatele včetně SCADA systémů, které mají svoji vlastní LAN síť. |  |
| 3. | Poskytovatel služby navrhne modifikaci relevantních procesů na straně zadavatele, včetně atributů a parametrů procesů potřebných pro doručení služby.  Konfigurační změny a úpravy prostředků zadavatele nutných pro připojení k službě provede poskytovatel v součinnosti se zadavatelem jako součást služby. |  |
| 4. | Poskytovatel služby navrhne modifikaci konfigurace řešení na straně zadavatele, včetně atributů a parametrů potřebných pro doručení služby. |  |
| 5. | Služba dostupná v českém jazyce. |  |
| 6. | Služba dohledu je zajišťována z území ČR. |  |
| 7. | V rámci služby bude poskytovatelem služby vytvořeno bezpečné uložiště pro sdílení kompletních materiálů k poskytované službě. |  |
| 8. | **Správa a dohled zdrojů** – zajištění Performance a Capacity management |  |
| 9. | **Síťový dohled** – zajištění Network Performance Monitoring and Diagnostics, zajištění Detection Anomaly. Zajištění Apps Performance Monitoring. |  |
| 10. | **Bezpečnostní dohled –** zajištění bezpečnostního dohledu s využitím NetFlow, Firewall, Logmanagement nástroji zadavatele |  |
| 11. | **Incident management** – zajištění Operátorské činnosti, Incident handling, Incident Response. |  |
| 12. | **Analýza incidentů** – zajištění odborné činnosti v detekci a lokalizaci příčin incidentů Analytikem ze strany poskytovatele služby. |  |
| 13. | **Návrhy systematických opatření** – Sestavení opatření v organizační a technické úrovni pro posouzení zadavatelem. |  |
| 14. | **Návrhy řešení incidentů** – zajištění odborné činnosti pro kategorizaci na interní a externí příčiny incidentů a k nim příslušných opatření. |  |
| 15. | **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. |  |
| 16. | **Správa informací o aktivech informačních systémů zadavatele** – Zajištění automatizace pro pasportizaci ICT pracovišť manipulujících s klasifikovanými informacemi nebo obsahující privilegované oprávnění k výkonu kritických činností. |  |
| 17. | **Kybernetická bezpečnost** – Personální zajištění služby pracovníky s odbornou způsobilostí vyhovující požadavkům na zajištění kybernetické bezpečnosti kritické infrastruktury v souladu s požadavky *zákona 181/2014Sb. o kybernetické bezpečnosti* v celém průběhu služby a všech jejích procesů a rutin. |  |
| 18. | **Režim Maintenance** – Plánování odstávek poskytované služby se zajištěnou náhradou. |  |
| 19. | **Business Continuity** – Služba (včetně všech komponent, které využívá) musí být odolná proti výpadkům a poruchám. Všechny komponenty služby musí být schopny dlouhodobého provozu bez změny chování a úbytku výkonu. |  |
| 20. | **Zajištění souladu se zákonem ZoKB (Compliance)** - Všechny parametry služby musí zajistit na úrovni technologií i procesů splnění požadavků na zajištění potřebné míry informační bezpečnosti, zejména pak: Důvěrnost, Dostupnost, Nepopiratelnost, Autentizaci, Autorizaci. |  |
| 21. | Pokud zadavatel z organizačních důvodů rozhodne pro in-sourcing části procesů nebo workflow (např. Zřízení analytického týmu, útvaru provozu bezpečnostní infrastruktury, Operation centra pro aplikace, systémy, databáze, datovou síť, bezpečnostní komponenty atp.) musí služba poskytovatele umožnit separaci na úrovní procesů, systémů, dat, přístupových oprávnění, včetně transferu historických dat a informací do prostředí zadavatele. Náklady na změnu hradí zadavatel. Požadavek na vydělení části služby do samostatné části, není důvodem k okamžité výpovědi smlouvy. |  |
| 22. | **Adaptace a akceptace sdílených procesů** – Služba zajistí úpravu procesů na straně poskytovatele služby a návrh na jejich integraci s relevantními procesy na straně zadavatele. |  |
| 23. | **SLA procesních vstupů a výstupů** – Služba zajistí monitoring procesů na straně poskytovatele služby a zadavatele. |  |
| 24. | **Vizitace zadavatele v místě výkonu služby** – poskytovatel služby před podpisem smlouvy umožní zadavateli návštěvu vlastního bezpečnostního dohledového centra, aby si mohl ověřit splnění požadavků. Zjištění nedodržení požadavků je důvod pro vyloučení poskytovatele služby. |  |
|  | **Technické požadavky na SOC** |  |
| 25. | Poskytovatel služby provozuje vlastní *Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí*, který umožňuje napojení na nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí zadavatele. |  |
| 26. | Rozhodné operace a manipulace jsou prováděny prostředky zadavatele a nástroje poskytovatele služby budou sloužit na jeho straně pro případnou agregaci informací v rámci jeho procesů. Žádný ze způsobů propojení nesmí omezit nebo narušit primární autonomní fungování celého řešení jen prostředky zadavatele. |  |
| 27. | V rámci služby poskytovatel zajistí *provozní monitoring* bezpečnostních nástrojů zadavatele, dle předmětu zakázky, v rozsahu:   * dostupnost a funkčnost bezpečnostních nástrojů, * vytíženost bezpečnostních nástrojů, * detekce vyčerpání kapacitních zdrojů u bezpečnostních nástrojů. |  |
| 28. | V rámci služby poskytovatel zajišťuje *nastavování bezpečnostních nástrojů* zadavatele, dle předmětu zakázky, v rozsahu:   * úprava a optimalizace korelačních pravidel, dle požadavku zadavatele nebo dle best-practice poskytovatele, * přidávání nových zařízení, * vytváření nových scénářů pro detekci, * úprava nastavení nástrojů, dle požadavku zadavatele nebo NÚKIB. |  |
|  | **Požadovaná podpora SOC** |  |
| 29. | **Ticketovací systém** – služba s on-line přístupem pro kompletní správu požadavků, včetně uchování historie požadavků a jejich řešení. |  |
| 30. | Přístup zadavatele k podpoře *provozu systémů* – HotLine |  |
| 31. | Přístup zadavatele k podpoře *Incident Response* – HotLine, telefon/ email na členy CSIRT |  |
| 32. | Zakládání tiketů, proaktivní komunikace o jejich řešení. Komunikace s třetí stranou jako NBÚ, NÚKIB, kooperující CSIRT atd. |  |
| 33. | Přístup *administrátorů zadavatele* ke sledovaným parametrům služby prostřednictvím grafického rozhraní (GUI – dashboard apod.), alespoň v režimu čtení nebo v přístupové roli *Auditor*. |  |
| 34. | **Notifikace/Eskalace** – Informování odpovědných osob zadavatele o vzniku bezpečnostního incidentu v reálném čase za pomocí základních komunikačních nástrojů (mail / SMS / telefon). |  |
| 35. | **Vulnerability management** – služba kontinuálního skenování aktiv zadavatele definovaných danou sítí/sítěmi a zranitelností relevantních pro daná aktiva. Minimálně na začátku poskytování služby budou provedeny plné skeny a dále vždy 1x měsíčně skeny rozdílové. |  |
| 36. | **Vulnerability management** – Relevance ***zranitelnosti*** – U aktiv musí být ověřena relevantnost incidentů pro dané aktivum vulnerability scannerem. |  |
| 37. | **Reporty – Rozšířený *reporting*** – detailní report o událostech a incidentech s návrhy systematických opatření 1x měsíčně. Vzdálená prezentace reportu, např. formou videokonference. Prezentace měsíčních reportů v rozsahu min. 30 minut - max. 2 hod. |  |
| 38. | **Reporty** – on***-demand*** – Služba zajistí provádění on-demand spouštění některých pravidel a z výstupu bude vytvářet reporty. |  |
| 39. | **Reporty** – ***Standard*** – poskytovatel v rámci služby zpracuje a poskytne zadavateli každý měsíc Report, ve kterém je popsáno:   * průběh realizace Plnění služby za uplynulé období; * provedené služby za uplynulé období; * návrh doporučených opatření pro další období pro zvýšení bezpečnosti, dostupnosti a v prevenci eliminace incidentů. |  |
| 40. | **Technologie sběru dat** – Služba zajistí užití bezpečnostních nástrojů v majetku zadavatele (NetFlow, Firewall, Logmanagement, Provozní monitoring) jako základního zdroje dat a bude s ním komunikovat průmyslově standardními protokoly.  Navrhované řešení poskytovatele služby:   * zajištuje na straně zadavatele sběr, přenos a uložení logů a jejich vyhodnocování v rámci nástrojů Zadavatele. * zajištuje na straně zadavatele sběr a vyhodnocení NetFlow v rámci nástroje Flowmon zadavatele. * zajištuje na straně zadavatele sběr a vyhodnocení logů v rámci nástroje Fortigate a Logmanager zadavatele. * je schopno regulovat zatížení přenosové linky (Bandwidth throttling) podle specifikace zadavatele (minimum 500kbs, maximum 4 Mbs)., jak na vstupu, tak na výstupu VPN/Internetu ze strany zadavatele. * má na své straně služby ve svém komunikačním bodu zařazen VPN akcelerátor. * má na své straně služby ve svém komunikačním bodu Internetu zařazenu komponentu „DDoS pračku“. * má interní storage prostor na konektivitě v propustnosti minimálně 1Gb s využitím VPN v redundantní konfiguraci. * umí detekovat nové nebo dosud neznámé log data či transakční záznamy, a identifikovat jejich relevanci k provozní nebo bezpečnostní kategorii u zadavatele. |  |
| 41. | **Base line analýza** – Služba zajistí porovnání neobvyklých počtů určitých událostí oproti jinému období z minulosti. |  |
| 42. | **Členění aktiv** – Aktiva musí:   * být možno rozdělit:   + podle jejich důležitosti v procesech zadavatele;   + podle typu a povahy generování dat:     - Log data na struktuře Syslog přes UDP/TCP ve standardu IETF],     - NetFlow ve standardu IETF.     - SNMP ve standardu IETF.     - Transakční záznamy – SIP, DNS, DHCP, FRAUD ve standardu IETF nebo dle požadavků zákona eIDAS nebo zákona o Spisové službě. * mít uživatelsky definovatelné kategorie a parametry podle požadavků zadavatele. |  |
| 43. | **Kategorizace aktiv** – Služba zajistí jednotnou evidenci a vyhodnocení kategorie aktiv, podle povahy aktiva (viz bod 48.). Podle těchto kategorií bude poskytovatel služby utvářet další pravidla nebo reporty v prostředcích zadavatele. |  |
| 44. | **Manuální parsovací pravidla** – Služba zajistí generování parsovacích pravidel a reportů v prostředcích zadavatele. |  |
| 45. | **Historická korelace** – Služba zajistí ověření nového korelačního pravidla proti historickým datům. |  |
| 46. | **Služba Monitoring Privilegovaných účtů – Sdílené *účty*** – Služba zajistí detekci užití privilegovaných přístupů pro konkrétního uživatele v systémech zadavatele. |  |
| 47. | **Režim Maintenance** – Služba musí být schopna běhu v režimu údržby ohlášenou zadavatelem, kdy se údržbou dotčených zdrojů/aktiv nebudou vyhlašovat alerty. |  |
| 48. | **Služba Monitoringu a detekce**   * Průběžné sledování provozu prostředí zadavatele. * Real-time analýza situace v napojených zařízeních podle skupin, kategorií zařízení a podle kontextu log záznamů nebo událostí. * 2x denně odborné posouzení bezpečnostní situace a provozního stavu. V případě anomálie posouzení její relevance a závažnosti. * Posouzení kontextu anomálie a příčin vzniku situace s případnou eskalací problému zadavatele na analytického specialistu poskytovatele služby. |  |
| 49. | **Služba včasné výstrahy a reakce na nestandardní situace v provozu bezpečnostních systémů**   * Zpracování analytických scénářů na aktuální kybernetické hrozby. * Posouzení eskalovaného problému Zadavatele analytickým specialistou Předkladatele. * Detekce a vyhodnocení závažnosti identifikovaných anomálií. * Posouzení a případná eskalace nestandardní situace v provozu Zadavatele na službu včasné výstrahy a reakce na incident v rámci bezpečnostních struktur ČR. |  |
|  | **SLA** |  |
| 50. | Poskytovatel služby musí provozovat vlastní bezpečnostní dohledovou službu v režimu 24x7x365, včetně zajištění Operátorů a Analytiků ve stejném režimu, tj. 24x7x365 |  |
| 51. | Pro každý kybernetický incident (dle §7, ZokB) prochází poskytovatel služby následným postupem k určení kategorií kybernetických bezpečnostních incidentů (dle §31, VoKB) podle následků a negativních projevů pro doporučení opatření či součinnosti v následné reakci:  Fáze Detekce   * Monitoring prostředí vymezeného zadavatelem. * Dohledování bezpečnostní situace zadavatele. * Detekce anomálie – rozpoznání odchylky od běžného stavu nebo od zadavatelem normovaného stavu.   Fáze Přiřazení   * Klasifikace anomálie – určení závažnosti ve škále:   + False-Positive Alarm – způsobuje falešný alarm z důvodu:     - chyby v úsudku míry závažnosti anomálie;     - nepřesnosti rozpoznání odchylky vzniklé při dohledování a monitoringu v předchozí fázi Detekce.   + Bezpečnostní událost – anomálie, která může způsobit narušení bezpečnosti:     - informací v informačních systémech zadavatele;     - služeb zadavatele;     - a integrity datových sítí zadavatele.   + Bezpečnostní incident – anomálie, která narušila či narušuje bezpečnost:     - informací v informačních systémech zadavatele;     - služeb zadavatele;     - a integritu datových sítí zadavatele nebo jiných subjektů.   Fáze Analýza   * Vyhodnocení anomálie – vyhodnocení relevance:   + k systémům zadavatele;   + k procesům zadavatele;   + k zákonným normám ČR vztažených na zadavatele. * Klasifikace incidentu – začlenění incidentu do bezpečnostního typu kategorie dle určení zadavatelem nebo dle §30, VoKB:   + Podle příčiny:     - incident způsobený kybernetickým útokem nebo jinou událostí vedoucí k průniku do systému nebo k omezení dostupnosti služeb;     - incident způsobený škodlivým kódem;     - incident způsobený překonáním technických opatření;     - incident způsobený porušením organizačních opatření;     - incident spojený s projevem trvale působících hrozeb;     - ostatní incidenty způsobené kybernetickým útokem.   + Podle dopadu:     - incident způsobující narušení důvěrnosti aktiv;     - incident způsobující narušení integrity aktiv;     - incident způsobující narušení dostupnosti aktiv;     - incident způsobující kombinaci výše uvedených dopadů. * Kategorizace incidentu – začlenění incidentu podle významnosti. |  |
| 52. | **Kategorie III** – do 60 minut – velmi závažný kybernetický bezpečnostní incident, při kterém je přímo a významně narušena bezpečnost poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje neprodlené zásahy obsluhy s tím, že musí být všemi dostupnými prostředky zabráněno dalšímu šíření kybernetického bezpečnostního incidentu, včetně minimalizace vzniklých i potenciálních škod. |  |
| 53. | **Kategorie II** – do 4 hodin – závažný kybernetický bezpečnostní incident, při kterém je narušena bezpečnost poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje neprodlené zásahy obsluhy s tím, že musí být vhodnými prostředky zabráněno dalšímu šíření kybernetického incidentu včetně minimalizace vzniklých škod. |  |
| 54. | **Kategorie I** – do 24 hodin – méně závažný kybernetický bezpečnostní incident, při kterém dochází k méně významnému narušení bezpečnosti poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje zásahy obsluhy s tím, že musí být vhodnými prostředky omezeno další šíření kybernetického bezpečnostního incidentu včetně minimalizace vzniklých škod. Jedná se o bezpečnostní incidenty, které nespadají do kategorií III a II. |  |

**Implementační služby**

Všechna dodavatelem instalovaná zařízení nebo komponenty musí být dodavatelem profesionálně nainstalovány a zprovozněny a po jejich nasazení řádně dokumentovány a otestovány, 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 60 měsíců od podepsání akceptačního protokolu po předáním monitorovacího systému.
* záruku na veškerá dodaná HW zařízení minimálně v rozsahu 5 let NBD ode dne akceptace (Next Business Day) On-Site.

## Provozní dokumentace

V rámci realizace řešení služeb bude dodavatelem zpracována a předána dokumentace řešení minimálně v tomto rozsahu:

* Provozně-technická dokumentace v rozsahu požadovaném Vyhláškou č. 529/2006 Sb. §10 a §11
* Plán zálohování a obnovy včetně doporučení pravidel pro pravidelné ověřování jednotlivých postupů
* Bezpečnostní dokumentace dle zákona 181/2014 Sb. o kybernetické bezpečnosti, včetně jeho novel a jeho prováděcích právních předpisů, především pak analýza aktiv ve vazbě na interní metodiku a plán obnovy
* Integrační dokumentace popisující jednotlivá aplikační rozhraní (WS a API služby) používaná k integraci IS na jednotlivé funkce včetně funkčních prototypů volání jednotlivých funkcí

## Administrátorské školení

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

## Termín plnění

Dodavatel musí zajistit zahájení plnění do 1 měsíce od nabytí účinnosti smlouvy.

## Akceptační podmínky

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

* Veškeré komponenty systému jsou řádně licencované.
* Byly dodány fyzické zařízení dle požadované technické specifikace.
* Všechny HW i 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.
* Byla vytvořena a dodána provozní dokumentace.
* Bylo provedeno školení v požadovaném rozsahu.

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