Příloha č. 1 Technická specifikace předmětu plnění

Veřejná zakázka: Psychiatrická nemocnice Havlíčkův Brod - Kybernetická bezpečnost - SYSTÉM PRO ANALÝZU A DETEKCI ANOMÁLIÍ SÍŤOVÉHO PROVOZU

TECHNICKÁ SPECIFIKACE

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

Při definici technických požadavků jsou všechny uvedené požadavky závazné. Je-li definice požadavku „umožňuje, lze, je možné, možnost, …“ je uvedený parametr závazný a požadovaná funkcionalita musí být v rámci 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:

Obecné požadavky

Požadované funkcionality/vlastnosti	**Nabízené řešení splňuje/nesplňuje,** vč. vysvětlení, jak je zadání splněno, link na dostupnou dokumentaci – *vyplní účastník*
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.	**Splňuje /** Nabízené řešení je navrženo jako HW/SW appliance, která monitoruje síťovou komunikaci v reálném čase a identifikuje kybernetické hrozby, bezpečnostní rizika a anomální chování, na takové události upozorňuje v reálném čase.
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.	**Splňuje /** Nabízené řešení analyzuje zrcadlo síťového provozu ze SPAN portů nebo TAPů bez nasazení agentů na koncová zařízení.
Systém musí analyzovat obsah datových paketů v reálném čase a rovněž umožňovat analýzu aplikační vrstvy (L7), identifikaci aplikací a podrobný monitoring hlavních aplikačních protokolů (např. HTTP(S), DNS, DHCP).	**Splňuje /** Nabízené řešení analyzuje obsah paketů v reálném čase a umožňuje analýzu aplikační vrstvy, identifikaci aplikací a monitoring uvedených aplikačních protokolů.
Dodaný systém musí být schopen analyzovat síť také na základě zpracování statistických protokolů typu NetFlow, IPFIX, NetStream, Cisco NSEL a případně dalších.	**Splňuje /** Nabízené řešení analyzuje síť také na základě zpracování uvedených statistických protokolů.

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.	**Splňuje /** Nabízené řešení umožňuje fungování v offline prostředí organizace bez využití cloudu pro všechny uvedené operace.
Aktualizace systému musí být možné provádět uživatelsky v offline režimu.	**Splňuje /** Nabízené řešení umožňuje provedení uživatelské aktualizace 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.	**Splňuje /** Nabízené řešení ukládá síťové toky ve formátu umožňujícím analýzu komunikace na úrovni jednotlivých toků včetně dohledání informací o transakcích a metadatech z L2-L7.
Systém podporuje ukládání aplikačních metadat z transakcí využívajících protokoly DHCP, DNS, SMB/CIFS, HTTP, HTTPS, SMTP, POP3, IMAP, MS SQL (TDS) a VoIP SIP. Současně umožňuje analýzu zapouzdření SSL/TLS a extrakci SNI (Server Name Indication) z HTTPS a QUIC komunikace.	**Splňuje /** Nabízené řešení podporuje ukládání aplikačních metadat z transakcí využívajícíuvedené protokoly a umožňuje analýzu zapouzdření SSL/TLS a extrakci SNI (Server Name Indication) z HTTPS a QUIC komunikace.
Je požadováno vysokorychlostní úložiště pro uchování historie datových toků velikosti minimálně 5TB složené z SSD nebo NVMe disků.	**Splňuje /** Nabízená HW komponenta je osazena vysokorychlostním úložištěm pro uchování historie datových toků 7 TB složené z SSD disků.
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.	**Splňuje /** Nabízené řešení poskytuje jednotné GUI pro veškerou uvedenou činnost uživatelů.
Systém musí být schopen vytváření profilů a skupin uživatelů pro omezení funkcionality produktu a viditelnosti uložených dat s podporou minimálně:	**Splňuje /** Nabízené řešení vytváří profily a skupiny uživatelů pro omezení funkcionality a viditelnosti s podporou uvedených parametrů:
● vytváření vlastních filtrů veškerých dat a jejich sdílení mezi uživateli a skupinami uživatelů,	**Splňuje**
● vytváření vlastních uživatelských pohledů, reportů, dashboardů apod.	**Splňuje**
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,	**Splňuje /**

závažnosti události, kategorie události, země, uživatele, síťové služby, čísla portu, provozu do/z internetu.	Nabízené řešení umožňuje zasílání upozornění uživatelům emailem i logováním o všech událostech na základě všech uvedených parametrů.
Tyto alerty musí být systém schopen dodávat i ve strojově čitelném formátu pro vyžití v nástrojích typu SIEM a musí obsahovat minimálně bližší informace o detekované události.	**Splňuje /** Nabízené řešení umožňuje poskytování výše uvedených alertů ve strojově čitelném formátu pro využití v nástrojích typu SIEM a tyto obsahují detailní informace o dané události.
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.).	**Splňuje /** Nabízené řešení umožňuje vytvářet automatizované manažerské reporty o stavu kybernetické bezpečnosti z pohledu správy kybernetických incidentů dle různých parametrů, včetně oblasti vzniku.
Je požadováno vytváření automatizovaných reportů v českém jazyce.	**Splňuje /** Reporty lze generovat v českém jazyce.
Integrace systému	
Systém musí poskytovat hotové nástroje umožňující integraci se softwarem třetích stran, a to minimálně:	**Splňuje /** Nabízené řešení poskytuje hotové nástroje pro integraci uvedených SW třetích stran.
● syslog, CEF pro export událostí včetně plné podpory filtrů (exportování pouze požadovaných dat)	**Splňuje**
● přímé url odkazy na libovolnou obrazovku grafického uživatelského rozhraní	**Splňuje**
● export informací o toku ve formátu IPFIX nebo podobném formátu včetně plné podpory filtrů (exportovat lze pouze požadovaná data) včetně aplikačních metadat alespoň pro protokoly HTTP, HTTPS a SMTP	**Splňuje**
● Systém umožňuje integraci pro nástroje třetích stran, např. Firewall (zadavel používá firewall Barracuda), tj. možnost použít jejich otevřené rozhraní pro potřebu automatické, nebo manualní reakce.	**Splňuje /** Nabízené řešení umožňuje integraci s firewally – pro integraci lze použít otevřené rozhraní pro automatickou nebo manuální reakci.

Požadavky na architekturu nasazení

Požadované funkcionality/vlastnosti	**Nabízené řešení splňuje/nesplňuje,** vč. vysvětlení, jak je zadání splněno - *vyplní účastník*
Obecné požadavky pro nasazení	

Pro všechny HW komponenty senzor a kolektor je požadován formát 1U nebo 2U server o velikosti 19“.	**Splňuje /** HW komponenty nabízeného řešení jsou ve formátu 1U nebo 2U velikosti 19“.
Pro všechny HW komponenty senzor a kolektor je požadován duální zdroj napájení se schopností hot-swap.	**Splňuje /** HW komponenty nabízeného řešení zahrnují 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.	**Splňuje /** HW komponenty nabízeného řešení jsou vybaveny samostatným síťovým rozhraním pro vzdálenou správu serveru v případě výpadku systému uvedených typů.
Požadavky pro pokrytí IT prostředí	
Je požadován 1ks datový kolektor + 1ks sensor o průměrné propustnosti minimálně 500 Mbps ve formě hardware appliance s monitorovacím rozhraním alespoň 2x10/25 GbE s výkonem minimálně 0,75Mpps na každý port pro alespoň 1500 hostů.	**Splňuje /** Nabízené řešení je navrženo jako 1 ks HW appliance s předinstalovaným SW 1 x kolektor a 1 x sensor, které umožňují zpracovat průměrný průtok minimálně 500 Mbps, přičemž v peaku umožňuje zpracovat daleko vícenásobné průtoky. Navržený HW je osazen monitorovacím rozhraním 4x1GbE a 2x10/25 GbE s výkonem minimálně 0,75Mbps na každý port pro minimálně 1500 hostů. SW licence umožňuje překročení průtoku i počtu monitorovaných hostů bez sankcí a omezení funkcionalit.

Požadavky na schopnost detekce bezpečnostních událostí

Požadované funkcionality/vlastnosti	**Nabízené řešení splňuje/nesplňuje,** vč. vysvětlení, jak je zadání splněno - *vyplní účastník*
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:	**Splňuje /** Nabízené řešení identifikuje všechna zařízení připojená do sítě včetně koncových zařízení, serverů, IoT a dalších, a současně identifikuje všechny uvedené změny v síti:
● vytvoření nové podsítě,	**Splňuje**
● připojení nového zařízení,	**Splňuje**

● nedostupnost dříve dostupné a komunikující služby nebo dříve dostupného a komunikujícího zařízení,	**Splňuje**
● přístup nového zařízení ke službě či zařízení	**Splňuje**
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.	**Splňuje /** Nabízené řešení umožňuje uživateli pomocí detekčních metod nastavovat bezpečnostní politiky pro různé segmenty sítě a různá zařízení a na porušení 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.	**Splňuje /** Nabízené řešení používá matematické metody samostatného učení pro analýzu síťové aktivity, vytváří a v čase automaticky modifikuje modely chování na základě běžného chování zařízení a na nich provozovaných služeb v celé organizaci.
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:	**Splňuje /** Nabízené řešení identifikuje na základě matematického modelu zařízení a jeho služeb nestandardní síťové chování, zejména odchylky pro uvedené parametry sítě:
● odchylku od modelu pro přenos dat, toků a paketů,	**Splňuje**
● odchylku od modelu pro počet komunikačních partnerů,	**Splňuje**
● odchylku od modelu entropie na komunikačních portech,	**Splňuje**
● odchylku od modelu pro počet síťových toků a využitých síťových služeb,	**Splňuje**
● odchylku od modelu výkonnosti sítě (rychlost přenosu) a aplikací (doba odezvy).	**Splňuje**
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.	**Splňuje /** Nabízené řešení využívá samostatné učení na všech síťových zařízeních a na nich provozovaných službách – na všech uvedených portech a protokolech.
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:	**Splňuje /** Nabízené řešení detekuje uvedené a další typy neznámých hrozeb, které nelze identifikovat prostřednictvím detekčních

	signatur, a to všechny uvedené příznaky škodlivého chování:
• průzkumné aktivity v síti,	**Splňuje**
• detekce podezřelého strojového chování, které nevytvářejí lidští uživatelé sítě,	**Splňuje**
• detekce botnetů a ovládání kompromitované stanice,	**Splňuje**
• detekce příznaků těžení kryptoměn,	**Splňuje**
• útoky hrubou silou a enumerace dat,	**Splňuje**
• rozpoznání tunelovaného síťového provozu – alespoň IPv4 prostřednictvím IPv6 a DNS tunely.	**Splňuje**
Detekce na základě databáze známých hrozeb	
Systém musí být schopen identifikovat hrozby a reportovat události na základě	**Splňuje /** Nabízené řešení identifikuje hrozby a reportuje události na základě všech uvedených parametrů:
• 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,	**Splňuje**
• reputační databáze známých škodlivých IP adres, záznamů DNS a hostname, URL adres	**Splňuje**
Tyto databáze musí být poskytovaných výrobcem a aktualizovány nejméně každých 24 hodin. Systém umožňuje zapojit další zdroje IP a host reputačních dat pro automatickou detekci	**Splňuje /** Nabízené řešení disponuje databázemi hrozeb poskytovanými výrobce a aktualizovanými v řádu jednotek hodin; umožňuje zapojit další zdroje reputačních dat pro automatickou detekci.
Uživatel musí být schopen importovat vlastní záznamy.	**Splňuje /** Nabízené řešení umožňuje importovat vlastní záznamy pro automatickou detekci.
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.	**Splňuje /** Nabízené řešení využívá výše uvedenou detekci pro veškerý monitorovaný provoz.
Databáze detekčních pravidel (signatur) musí být založena na pokročilých regulárních výrazech pro zpracování řetězců, které dokáží provádět inspekci veškeré síťové komunikace v rámci těchto pravidel. Systém musí detekovat události na základě vysokého počtu signaturních pravidel (minimálně několik desítek tisíc).	**Splňuje /** Nabízené řešení disponuje databází signatur zranitelností založenou na pokročilých regulárních výrazech pro zpracování řetězců pro inspekci veškeré síťové komunikace; databáze zahrnuje desítky tisíc signaturních pravidel.

Uživatel musí být schopen přidávat vlastní detekční pravidla v praktickém a obecně využívaném formátu pomocí úpravy konfigurace a také mít možnost tyto nová pravidla řadit do kategorií.	**Splňuje /** Nabízené řešení umožňuje uživateli přidávat vlastní detekční pravidla v obecném formátu pomocí úpravy konfigurace; nová pravidla zařazuje do kategorií.
Analýza šifrované komunikace Vedle samostatného učení musí systém používat další metody pro analýzu šifrované komunikace, minimálně TLS fingerprinting a s ní možnost detekce známých hrozeb.	**Splňuje /** Nabízené řešení využívá kromě samostatného učení také další metody pro analýzu šifrované komunikace jako TKS fingerprinting a 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:	**Splňuje /** Nabízené řešení poskytuje přívětivé prostředí pro zpřesnění detekce a eliminace false positives na základě všech dále uvedených parametrů:
● IP adresa,	**Splňuje**
● segment sítě / podsíť,	**Splňuje**
● lokalita – ASN	**Splňuje**
● detekovaná událost – kategorie, název apod.	**Splňuje**
● libovolné kombinaci výše popsaných.	**Splňuje**

Požadavky na zajištění síťové viditelnosti

Požadované funkcionality/vlastnosti	**Nabízené řešení splňuje/nesplňuje,** vč. vysvětlení, jak je zadání splněno - *vyplní účastník*
Vyhledávání, filtrování a vizualizace dat	
Systém musí být schopen okamžitého vyhledávání a vizualizace pro forenzní analýzu a podporu threat hunting bez zvláštního dotazovacího jazyka.	**Splňuje /** Nabízené řešení okamžitě vyhledává a vizualizuje události pro forenzní analýzu a podporu threat hunting bez potřeby speciálního dotazování.
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:	**Splňuje /** Nabízené řešení umožňuje filtrovat a vyhledávat v reálném čase v plné historii uložených dat – bezpečnostních událostí, toků a agregovaných síťových statistikách dle všech dále uvedených parametrů:
● podle parametrů IP a MAC adresa, hostname, username (identita uživatele), příchozí a odchozí provoz, síťová služba,	**Splňuje**

lokální nebo vzdálená služba (služba z pohledu klient nebo server), číslo portu, VLAN, země, ASN,	
Systém musí být schopen filtrovat a vizualizovat výsledky v grafech, výčtových tabulkách s možností řazení a TOP N statistikách.	**Splňuje /** Nabízené řešení filtruje a vizualizuje výsledky v grafech, výčtových tabulkách s možností řazení a TOP N statistikách.
Systém musí být schopen **detekovat používání síťových protokolů** v rámci vnitřní infrastruktury organizace a zároveň **identifikovat útoky vedené proti těmto protokolům**. Detekce by měla zahrnovat běžně využívané služby, jako například: SSH, RDP, Telnet, FTP, HTTP, SMTP, POP3, SMB	**Splňuje /** Nabízené řešení detekuje používání síťových protokolů v rámci vnitřní infrastruktury organizace a současně identifikovat útoky proti uvedeným protokolům.
Kontextuální informace	
Systém musí být schopen pro každé zařízení získávat, vizualizovat a zobrazovat kontextuální informace:	**Splňuje /** Nabízené řešení umožňuje pro každé zařízení získávat, vizualizovat a zobrazovat všechny uvedené kontextuální informace:
• informace o identitě uživatelů získanou z prostředí LDAP, následně s danou informací pracovat a uchovávat její persistenci	**Splňuje**
• IP geolokace	**Splňuje**
• IP reputace, vč. údaje, jestli je IP adresa na blacklistu nebo podezřelá	**Splňuje**
• historie použitých MAC adresa a výrobce zařízení	**Splňuje**
• operační systém a jeho historie na zařízení	**Splňuje**
• seznam detekovaných bezpečnostních a provozních událostí daného zařízení.	**Splňuje**
Zaznamenávání, ukládání a zpětná analýza 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.	**Splňuje /** Nabízené řešení umožňuje nahrávání plného síťového provozu ve formátu PCAP na všech zařízeních na základě všech uvedených parametrů; záznam lze zapínat automaticky na základě detekovaných událostí nebo uživatelsky.
Detekce zdravotnické techniky a modalit	
Systém musí být schopen pro každé zařízení získávat, vizualizovat zobrazovat kontextuální informace:	**Splňuje /** Nabízené řešení pro každé zařízení v síti získává, vizualizuje a zobrazuje dále uvedené kontextuální informace:
• IP geolokace	**Splňuje**
• IP reputace, vč. údaje, jestli je IP adresa na blacklistu nebo podezřelá	**Splňuje**

• historie použitých MAC adresa a výrobce zařízení	**Splňuje**
• operační systém a jeho historie na zařízení	**Splňuje**

Další požadované oblasti využití

Požadované funkcionality/vlastnosti	**Nabízené řešení splňuje/nesplňuje,** vč. vysvětlení, jak je zadání splněno - *vyplní účastník*
Management bezpečnostních událostí a incidentů	
Systém musí poskytovat funkcionalitu pro reporting bezpečnostních incidentů (prohlášení identifikované události za bezpečnostní incident), včetně:	**Splňuje /** Nabízené řešení umožňuje reportování bezpečnostních incidentů včetně dále uvedených detailů:
● jednoduché sdílení informací o bezpečnostních incidentech, včetně uživatelem zadaných komentářů,	**Splňuje**
● možnost exportování dat do emailu, csv, pdf, syslogu a podobně,	**Splňuje**
● možnost exportu bezpečnostních událostí a incidentů do systémů typu ticket management třetích stran.	**Splňuje**
Monitoring výkonu aplikací a sítě	
Systém v celé monitorované síti, mezi všemi zařízeními a na všech službách měří pro výkonnostní parametry minimálně:	**Splňuje /** Nabízené řešení měří v celé monitorované síti a mezi všemi zařízeními a na všech službách dále uvedené parametry:
● přenosová rychlost sítě,	**Splňuje**
● rychlost odezvy aplikace,	**Splňuje**
● odezva systému z pohledu uživatele.	**Splňuje**
Výpočet uvedených výkonnostních parametrů a automatické detekce anomálií na základě odchylky od modelu normálního chování musí být prováděna pro:	**Splňuje /** Nabízené řešení provádí výpočet uvedených výkonnostních parametrů a automatické detekce anomálií na základě odchylky od modelu normálního chování pro všechny uvedené položky:
● všechny porty a služby TCP,	**Splňuje**
● pro všechny kombinace služeb a zařízení.	**Splňuje**
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.	**Splňuje /** Nabízené řešení v celé monitorovací síti a mezi všemi zařízeními a na všech službách měřit informace o všech uvedených událostech.
Inventarizace sítě a grafická vizualizace topologie	

Systém musí být schopen zobrazit celý inventář monitorované sítě s počtem zařízení v jednotlivých lokalitách, segmentech, nebo podsítích. Včetně detailního přehledu zařízení.	**Splňuje /** Nabízené řešení umožňuje zobrazit celý inventář monitorované sítě, počty zařízení v lokalitách a podsítích včetně detailního přehledu o všech zařízeních.
Systém umožňuje všechny inventarizační informace řadit dle různých parametrů.	**Splňuje /** Nabízené řešení umožňuje všechny inventarizační informace řadit dle nejrůznějších parametrů dle potřeb a nastavení uživatele.

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.

Dodavatel zajistí vyladění a nastavení detekce všech dodávaných systémů tak, aby nebyly detekované nežádoucí a falešně pozitivní události. Tato činnost bude provedena ve spolupráci s kompetentními osobami zadavatele. Dodavatel zajistí integraci nástroje s aktuálním log managementem zadavatele, dále pak nastavení aktivních alertů a reportů dle potřeb zadavatele.

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.

Administrátorské školení

V rámci realizace je požadováno administrátorské a uživatelské školení pro zaměstnance zadavatele v rozsahu nezbytném pro kvalifikovanou obsluhu včetně videozáznamu pro zpětné použití, který bude dostupný online na zabezpečeném úložišti dodavatele.

Termín plnění

Dodavatel musí zajistit plnění do 60 dnů ode dne nabytí účinnosti smlouvy.

Akceptační podmínky

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

Na závěr zástupci zadavatele potvrdí splnění všech akceptačních podmínek pro předání řešení do provozu potvrzením akceptačního protokolu ve znění:

Akceptační kritérium	splňuje/nesplňuje
Veškeré komponenty systému jsou řádně licencované	
Byla dodána fyzická zařízení dle požadované technické specifikace.	
Všechny HW i SW komponenty systému jsou nainstalovány a napojeny na infrastrukturu zadavatele.	
Dochází k záznamu zrcadleného provozu, informace jsou dostupné k zobrazení a dalšímu zpracování.	
V systému jsou zavedeny všechny zadavatelem dodané podsítě.	
Funguje asistované učení při označení falešně pozitivní detekce.	
Pro všechna zařízení v síti jsou okamžitě dostupné informace o zařízeních (název, mac adresy, IP adresa, uživatele, klientské služby, serverové služby, detekované události, …)	
Systém korektně načítá VLAN-ID ze zrcadlené komunikace a umožňuje filtrování informací podle VLAN-ID.	
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 (jsou aktivně využívána detekční pravidla/signatur a záznamy 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	