Požadovaná funkcionalita řešení NDR	Způsob naplnění Uchazeč 1	Způsob naplnění Uchazeč 2	Způsob naplnění Uchazeč 3	Vyhodnocení - způsob zapracování do Zadávacích
Umožňuje řešení záznam popisných metadat o síťové komunikaci pro její pozdější analýzu? Záznamem je myšleno uložení popisných informací přímo v nabízeném řešení, kde bude probíhat také jejich následná analýza. Pokud „ANO", tak uveďte detail, který je o komunikaci zaznamenán v případě, že se jedná o: - nešifrované SMTP spojení (e-mail nesoucí .DOCX jako přílohu) - šifrované SMTP spojení - nešifrovaný přístup k webové stránce (http), ze které byl stahován soubor - šifrovaný přístup k webové stránce (https) Popište způsob uložení metadat (např. logy, databáze)	Řešení poskytuje úplnou analýzu kompletního provozu na všech portech a aplikační vrstvě. Každá komunikace je identifikována na úrovni aplikace a obsahu přenášeného souboru. Šifrovaný provoz lze dešifrovat a analyzovat jeho obsah. Každá komunikace je na základě definic a strojového učení kontrolována na přítomnost známých i neznámých hrozeb. Zahrnuje také ochranu proti hrozbám nultého dne, neznámým útokům nultého dne. Všechny informace se ukládají do DB v zařízení, případně se předávají do samostatného virtuálního prostředí k další analýze.	- nešifrované spojení: IP adresy a porty, počet paketů, velikost přenosu, SMTP hlavičky, MIME obálka, analýza typu souboru u přílohy a pokud obsahuje další vložené komponenty, pak i analýza a typ komponent - šifrované SMTP spojení bez TLS dešifrátoru: IP adresy a porty, počet paketů, velikost přenosu, informace o tom, že spojení bylo šifrováno - nešifrovaný http provoz: IP adresy a porty, počet paketů, velikost přenosu, hlavičky HTTP klienta a serveru, analýza obsahu přenášených dat – u souboru určení jeho typu, hash přenášeného obsahu, u kompozitních souborů analýza vložených komponent - šifrovaný http provoz bez TLS dešifrátory: IP adresy a porty, počet paketů, velikost přenosu, informace o tom, že spojení bylo šifrováno a pro TLS bude uvedeno SNI, JA3, JA3S a typ a síla šifry Při použití TLS dešifrátorů bude úroveň detailu pro šifrovaná spojení stejná jako u nešifrovaných spojení. Metadata jsou ukládána do databáze a je možné v metadatech vyhledávat komplexními dotazy.	Veškerá dat jsou uložena v softwarově akcelerovaných databázích pro okamžitý přístup k datům. U všech toku jsou obsaženy volumetrické, statické a dynamické vlastnosti toku a dále dle protokolu obsah aplikačních metadat, nebo plný obsah protokolu. GreyCortex detailně (aplikační detail) zpracovává asi 70 protokolů, šifrovaných i nešifrovaných a uchovává až 2000 parametrů pro jeden síťový tok. Dále uživatel může nechat zaznamenávat definovanou velikost aplikačního obsahu, nebo třeba celý aplikační obsah u každého toku. Nešifrované SMTP obsahuje informace z hlavičky - adresáty, předmět zprávy, návratové SMTP kódy a názvy a velikosti příloh a jejich souborový HASH v MD5 SHA1 a SHA256. files: name: /filename.txt size: 40077 md5: 388DDFF79D4E485D0C2B9E52C7B6A1E2 sha1: 200DE62BEE4DC9296A746C8F98C021E780FBCA75 sha256: 9D273B6DDA79C206D8A5BBD5D165E2A60F8A0E40563A74B2B332BB9E421FA789 Šifrované SMTP nese informace o použitém šifrování, platnosti certifikátu	
Probíhá analýza síťového provozu pro veškerý IT síťový provoz, a to bez ohledu na použité komunikační protokoly, probíhající spojení a síťové porty?	Řešení poskytuje úplnou analýzu kompletního provozu na všech portech a aplikačních vrstvách.	Analyzovány jsou všechna spojení vedená IP protokoly a bez ohledu na použitý aplikační protokol a číslo portu	Na všech obdržených datech od L2(Ethernet bez IP, apod.) až po L7 (Aplikační vrstva) jsou prováděny veškeré detekční mechanizmy založené na učení a signaturní detekci. TZN. jsou vytvářeny modely pro detailní analýzu komunikace všech zařízení na všech portech a všech protokolech (TCP/UDP 0-65535, ICMP, IPv4 i IPV6, ARP, WakeOnLine na ethernetu, atd), kdy se vychází z 30 denní historie dat pro detekci anomálie.	
Pracuje funkcionalita analýzy a záznamu síťového provozu nad zrcadleným provozem sítě?	Řešení umí provádět také všechny analýzy, tedy i SPAN či Mirror port.	Sensor systému může být zapojen na zdroj zrcadleného provozu nebo volitelně i in-line.	Zpracovává data ze zdrojů jako je SPAN, RSPAN, ERSPAN a z TAPovaných linek. Jako alternativu lze využít různé formáty protokolu netflow pro zajištění visibility v nepokrytých lokalitách.	
Zahrnuje řešení připravená pravidla pro analýzu provozu umožňující definovat podmínky odkazující se na přenášený obsah a parametry aplikační vrstvy? (Například odhalit přenášené soubory, kde koncovky souborů nesouhlasí s obsahem, nebo čísla typických portů nesouhlasících s typem rozpoznaného komunikačního protokolu.) (*V sekci **Způsob naplnění** uveďte i typ a počet takových pravidel.)*	Aplikační vrstva je vždy detekována a zaznamenána do logů za všech okolností. Analýza dílčích souborů je tzv. trutype, kde se vždy analyzuje obsah podsouboru, nikoliv jeho konec. Typy souborů, které detekuje, je k dispozici na této adrese URL. K 14.12.2022 to je 334 typů souborů: https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIEtCAK Počet aplikací ke dni 14. 12. 2022 je 3790, seznam je k dispozici na této adrese: https://applipedia.paloaltonetworks.com/	Pro všechna spojení je detekován protokol a typ přenášeného obsahu, pokud nějaký je a spojení není šifrované. Uvedené případy užití je tedy možné realizovat. Celkově nad provozem systém vyhodnocuje cca 300 pravidel pracující na úrovni celého obsahu komunikace a několik set pravidel pracujích na úrovni jednotlivých paketů (DPI). Korelaci událostí pokrývají desítky pravidel.	Technologie analyzuje obsah, tudíž je možné libovolným způsobem reportovat anomálie v obsahu. Tj. změněné soubory, anomální využití portů, různá porušení politik, apod. Např: Anomalies: FTP but not tcp port 20 or 21 Policy: hidden zip extension .scr Policy: ZIPPED EXE in transit Info: SUSPICIOUS .LNK File Inside of Zip Celkem je obsaženo asi 16.000 různých pravidel analyzující anomálie v obsahu komunikace.	
Umožňuje řešení přizpůsobení pravidel pro analýzu provozu nebo tvorbu vlastních pravidel pro analýzu?	Přímo v rozhraní GUI je možné definovat pravidla pro analýzu, vlastní aplikace a vlastní reportovací sestavy.	Všechna pravidla (DSI, DPI, korelace) jsou v systému viditelná a lze je modifikovat. Vlastní pravidla lze doplnit, typicky za použití do rozhraní vestavěných editorů.	Uživatele může libovolně vytvořet nové nebo modifikovat stávající detekční mechanizmy.	
Umožňuje řešení definovat pravidla hledající souběh událostí nebo posloupnost událostí v síťovém provozu a generovat upozornění (alerty) a to kontinuální analýzou okamžitého dění i analýzou již uložených historických záznamů o	Zaznamená se detail každé komunikace a zobrazí se začátek, konec a případně všechna relevantní spojení související s touto komunikací.	K tomuto účelu jsou používána korelační pravidla a ta jsou vyhodnocována kontinuálně, nebo je lze vytvořit a zpustit zpětně nad metadaty.	Je možno vytvářet korelační pravidla. Zpětná analýza je možná jen na základě zpracování již uložených dat za pomocí uživatelských dotazů.	
Jsou historické informace o provozu s určenou dobou retence pro následnou analýzu chráněna před narušením jejich integrity?	Všechny protokoly jsou uloženy v DB, která je chráněna proti porušení integrity.	Metadata jsou uložena v relační databázi a z rozhraní systému je nelze mazat ani zpětně měnit. Alerty jsou uloženy také v relační databázi a lze je volitelně i šifrovat.	Žádný uživatel nemá právo modifikace historických dat. Některá oprávnění mohou měnit nastavení detekce a přiřazenou závažnost (severity) identifikovaných zjištění.	
Umožňuje řešení provádět analýzu šifrovaného spojení a detekci narušení i při nevyužívání SSL dešifrování (např. díky kontrole konzistence použitých certifikátů, kvality šifrovacích algoritmů, nebo JA3 tagů)?	Detekce anomálií, typů certifikátů, slabých šifrovacích algoritmů atd. v šifrovaném provozu i bez dešifrování SSL.	S využitím ML/AI, analýzou certifikátů a na základě JA3/JA3S.	Mimo přímého dešifrování jsou dělány následující kontroly nad každou šifrovanou SSL/TLS komunikací. Jedná se o: - Volumetrické anomálie - Výkonnostní anomálie - Behaviorální anomálie – Beaconing (skryté CnC kanály) - Kontrola na přítomnost známých hrozeb JA3 HASH - Kontrola platnosti certifikátu - Kontrola úrovně a síly šifrovacích mechanizmů - Kontrola důvěryhodnosti certifikátu – ověření kořenové autority - Kontrola na základě Threat Intelligence (IP blacklist, Domain Balcklist, Certificate Blacklist) - Kontrola na základě přístupových bezpečnostní politik - A další	
Je detekce malware prováděna pomocí vyhledávání signatur?	**!!! Uchazeč neuvedl způsob naplnění !!!**	Malware je detekován pomocí signatur, emulací a heuristikou, sandboxingem, a pravidly (DSI, DPI, korelační pravidla).	Je používána databáze GreyCortex + ProofPoint + ESET. Aktualizace detekčních signatur probíhá jednou za hodinu. Dále uživatel může využít vlastní zdroje, či se napojit na libovolný MISP zdroj (např. NUKIB).	
Je detekce malware prováděna pomocí heuristické analýzy?	**!!! Uchazeč neuvedl způsob naplnění !!!**	Malware je detekován pomocí signatur, emulací a heuristikou, sandboxingem, a pravidly (DSI, DPI, korelační pravidla).	Heuristika v rámci anomálií, např. beaconing. Označení skrytých komunikačních kanálů	
Je detekce malware prováděna pomocí vyhledávání typického chování (behaviorální analýza)?	**!!! Uchazeč neuvedl způsob naplnění !!!**	Malware je detekován pomocí signatur, emulací a heuristikou, sandboxingem, a pravidly (DSI, DPI, korelační pravidla).	Každé zařízení má profil chování, ve kterém je vyhodnocováno asi 370 parametrů. Jedná se o model systému, ve kterém jsou strojovým učením definovány hodnoty popisující běžné chování pro jednotlivé podsítě, zařízení a všechny služby na nich provozované (lokální i vzdálené). Tento strojově vytvářeny model je dostupný uživateli a systém na základě něj dokáže detekovat odchylky od normálního chování – behaviorální analýza. Systém se přeučuje jednou za 30 – 60 minut, tzn. model chování jednoho zařízení je jiný pro neděli večer a středu po obědě.	
Je detekce malware prováděna detekcí na sandboxu virtuálním provedení?	**!!! Uchazeč neuvedl způsob naplnění !!!**	Malware je detekován pomocí signatur, emulací a heuristikou, sandboxingem, a pravidly (DSI, DPI, korelační pravidla).	Tato funkcionalita je přenechávána hraničním prvkům jako jsou firewally, emailové a webové brány, které na ní mají více výkonu a z pohledu architektury detekce jsou pro tuto úlohu vhodnější.	
Je součástí dodávky pravidelná služba aktualizace signatur (definice chování malware) a aktualizace pravidel sandboxu? (*V sekci **Způsob naplnění** uveďte obvyklý interval jejich aktualizací.)*	Každých 5 minut	Všechen threat-intel je dodáván a aktualizován dodavatelem. Obvykle je vydána minimálně jedna aktualizace denně.	Jsou aktualizovány všechny znalostní zdroje na hodinové bázi.	
Je řešení schopné detekovat také malware skrytý hluboko v přenášeném obsahu? (Například v komprimovaných souborech, v embeded obsahu dokumentů kancelářských aplikací).	**!!! Uchazeč neuvedl způsob naplnění !!!**	Toto je pokryto funkcionalitou DSI (Deep Session Inspection). Systém je schopný analyzovat obsah kompozitních souborů a rekurzivně je rozpižlávat.	Pouze v některých případech, např embeded soubory a funkce v PDF, skrytý spustitelný obsah, skryté datové komunikace v DNS, ICMP apod.	
Podporuje řešení pro účel huntingu obsahovou analýzu?	**!!! Uchazeč neuvedl způsob naplnění !!!**	Pravidla mohou reagovat na obsah přenášených dat a generovat alerty, nebo záznamy metadat označit. Následný hunting lze pak realizovat na základě metadat obohacených o tyto značky vztahující se k obsahu. Alert obsahuje i část obsahu, který pravidlo spustil.	Ano, formou analytického modulu nad uloženými daty, který dokáže vyhodnocovat, agregovat a jinak zpracovávat uložený obsah. Analytický modul je součástí základní licence.	
Je možné definovat vlastní pravidla pro analýzu a detekci obsahu?	**!!! Uchazeč neuvedl způsob naplnění !!!**	Jako DSI pravidla.	Je dodržována syntaxe Sirucata IDS a SNORT. Existují pouze rozšíření u klíčových slov a funkcí, kterou jsou popsány v uživatelské dokumentaci.	

Je možné pracovat s metadaty popisujícími obsahové části síťového provozu?	**!!! Uchazeč neuvedl způsob naplnění !!!**	Metadata sama neobsahují obsah přenášených dat, ale jejich popis. Nicméně nesou informaci o hash přenášeného obsahu, jeho typu a velikosti, případně jménu souboru a volitelně také značky přidané pravidly reagujícími na obsah. Všechny atributy metadat lze využít pro jejich vyhledávání a pro tvorbu korelačních pravidel.	Je možné pracovat se všemi daty libovolně dle potřeb uživatele.	
Poskytuje řešení webové uživatelské rozhraní pro analýzu zaznamenaného provozu bezpečnostními specialisty, které bude součástí jednotného	**!!! Uchazeč neuvedl způsob naplnění !!!**	Systém poskytuje jednotné webové uživatelské rozhraní.	... uvedeny screenshoty ...	
Poskytuje uživatelské rozhraní vysokou granularitu řízení přístupových oprávnění k jednotlivým modulům systému a zpracovávaným/zaznamenaným metadatům? Umožňuje řešení řídit oprávnění pro pracovníky pracoviště SOC v úrovních: - L1 operátor, který musí pracovat jen s přiděleným alertem a jemu relevantními metadaty - L2 analytik pracující napříč aletry a jim přidruženými metadaty - L3 security exprt, který může provádět hunting, tedy vyhledávání nespecifických metadat	**!!! Uchazeč neuvedl způsob naplnění !!!**	Systém je vybaven RBAC mechanismem řízení přístupu. Je předpřipraveno 9 typických rolí uživatelů s možností tvorby vlastních. Uvedené úrovně lze realizovat.	Vše je definováno interní politikou dané organizace.	
Podporuje řešení monitorování provozu na rozhraních Ethernet s rychlostí 40Gbps?	**!!! Uchazeč neuvedl způsob naplnění !!!**	Provoz lze rozkládat na několik senzorů, například na 4x 10G senzor.	Řešení umožňuje zpracovávat data do rychlosti 100Gbps a podporuje všechna poskytovaná rozhraní Ethernet.	
Podporuje řešení monitorování provozu na rozhraních Ethernet s rychlostí 25Gbps?	**!!! Uchazeč neuvedl způsob naplnění !!!**	Senzor s tímto výkonem bude k dispozici do cca čtvrt roku, nebo lze již dnes provoz rozkládat na několik 10G senzorů	Řešení umožňuje zpracovávat data do rychlosti 100Gbps a podporuje všechna poskytovaná rozhraní Ethernet.	
Podporuje řešení monitorování provozu na rozhraních Ethernet s rychlostí 10Gbps?	**!!! Uchazeč neuvedl způsob naplnění !!!**	Ano 10G senzor je k dispozici	Řešení umožňuje zpracovávat data do rychlosti 100Gbps a podporuje všechna poskytovaná rozhraní Ethernet.	
Podporuje řešení monitorování provozu na rozhraních Ethernet s rychlostí 1Gbps?	**!!! Uchazeč neuvedl způsob naplnění !!!**	Ano 1G senzor je k dispozici	Řešení umožňuje zpracovávat data do rychlosti 100Gbps a podporuje všechna poskytovaná rozhraní Ethernet.	
Umožňují komponenty systému, které uchovávají data pro analýzu, provoz v on-premise prostředí? *(Pro Zadavatele není přípustné přenášet data o síťovém provozu do cloudových platforem výrobce.)*	**!!! Uchazeč neuvedl způsob naplnění !!!**	Celý systém lze realizovat jako on-premise řešení s aktualizací threat-intelu a sandboxingem na zdrojích výrobce v internetu. Případně lze i sandboxing realizovat on-premise. Případně lze celý systém vystavět v air-gap režimu bez nutnosti jakékoliv on-line komunikace do internetu.	Řešení ukládá data lokálně, a dokáže fungovat zcela bez přístupu k internetu. Velikost úložiště si klient určuje sám dle potřeby, a nevztahují se na něj žádné licenční poplatky.	
Jaké jsou podporované způsoby nasazení nabízeného řešení? (např. fyzické appliance výrobce, open-servery, virtualizace, ...)	HW appliance výrobce Virtuální prostředí	Systém je možné nasadit v podobě hardware appliancí výrobce, nebo jako virtualizované appliance na platformě VMware, nebo jej lze poskytovat jako službu z cloudu.	HW Appliance, Virtuál Appliance. Instalační soubor, s možností instalovat do libovolných prostředí cloudu, případně specifické HW a VA aplikace.	
Podporuje řešení logování a napojení do systému log managementu? (*V sekci **Způsob naplnění** specifikujte i používané protokoly a možnost úpravy logovaných informací.)*	Format BSD Format IETF Protokol TCP/UDP Port 1025-65535	Systém je schopný odesílat alerty pomocí SMTP (email komunikace), SNMP trapů, http GET/POST, syslog zpráv. Formát zprávy lze specifikovat – tedy vybrat, která atributy alertu a v jaké podobě budou odeslány.	Řešení dokáže generovat i zpracovávat logy, v rámci nastavení lze zvolit libovolný formát a provést detailní nastavení obsahu.	
Podporuje řešení napojení do systému SIEM? (*V sekci **Způsob naplnění** specifikujte typ předávaných informací i používané protokoly.)*	Format BSD Format IETF Protokol TCP/UDP Port 1025-65535	Pro napojení SIEMů je k dispozici podpora formátů LEEF (Qradar), CEF (ArcSight) a formát pro Splunk. Nicméně formát zprávy lze také ručně specifikovat výběrem jmen atributů alertů a případných oddělovačů v rámci odesílané zprávy.	Prostřednictvím zasílání logů (syslog, leef, idea, cef, email, snmp) a RestAPI pro zpětné využití dat v SIEM a provádění příkazů, např označení False Possitive, nebo vytvoření pravidla pro zaznamenání PCAP souboru ze sítě.	

Zadavatel požaduje, aby případné spojení nástrojů NDR a EDR bylo na úrovni: - Integrace GUI nástrojů, se kterými pracuje analytický tým SOC - Vzájemném obohacování informací o událostech mezi NDR a EDR - Podpora automatizačních procesů při reakci na události Popište, zda a jakým způsobem, je integrace NDR a EDR podporována ve vámi nabízeném řešení.	Propojení EDR a NDR je v jednotné konzoli ve virtuálním prostředí, toto propojení se nazývá XDR a řešení je připraveno pro propojení s dalšími výrobci.	Systém je integrovatelný s dalšími moduly řešení, a to modulem Endpoint, který pokrývá funkcionalitu EDR a modulem, který je orientovaný na tvorbu vnitřních „honeypotů". Systém tvoří integrovanou bezpečnostní platformu, která je vnitřně integrována a nevyžaduje při nasazení i provozu integraci s dalšími technologiemi, ani žádné dodatečné náklady. Kromě toho jsou platformou podporovány i další integrace, například napojení na aplikace typu SIEM/SOAR a pracoviště SOC. Platforma je nasaditelná v cloudu i on-premise, moduly lze nasazovat samostatně a postupně. Spolupráce modulů zajišťuje požadované funkcionality: - Integrace GUI nástrojů, se kterými pracuje analytický tým SOC - Vzájemném obohacování informací o událostech mezi NDR a EDR - Podpora automatizačních procesů při reakci na události Systém je také schopen spolupracovat s EDR systémy třetích stran: - Carbon Black - SentinelOne - Trellix MVISION ePO - Forescout eyeInspect	Řešení je komplementární a plně integrovatelné s výrobky EDR třetích stran. Je možné doplnit o informace z detekčních nástrojů třetích stran jako Sentinel One, BitDefender, Microsoft apod. Integrace je možná oboustranná nebo v nástrojích třetích stran jako SIEM a SOAR. GreyCortex umožňuje přímý sběr a poskytování dat prostřednictvím RestAPI pro dotazy na podsítě, zařízení, uživatele, eventy, flow data, threat intelligence, apod. Případně dokáže sám uchovávat a vyhodnocovat informace z EDR získané formou logu a/nebo napojením na API daného EDR. Automatickou reakci na událost je možné dosáhnout jak prostřednictvím EDR, tak prostřednictvím přímého ovládání nástrojů typu firewall, NAC výrobců jako jsou Cisco, Checkpoint, Fortinet, PaloAlto, ForcePoint, Mikrotik, apod. Dále je možné také integrovat s libovolným nástrojem v rámci zákaznické podpory.	Účastníci PTK uvedli, že jejich řešení umožňují úzké integrační vazby mezi nástroji Network Detection and Response (NDR) a Endpoint Detection and Response (EDR). Z tohoto důvodu se Zadavatel rozhodl o sloučení požadavku na společné řešení Extended Detection and Response, které reprezentuje integrované řešení NDR a EDR, přičemž přináší obrovskou efektivitu při detekci, vyšetřování a reakci na projevy kybernetických hrozeb.
Popište licenční model a licenční podmínky platné pro všechny součásti řešení. Jaký je licenční model produktu NDR, tedy dle jakých vstupních údajů se odvíjí licencování a výkonnostní plánování řešení. - objem síťového provozu - množství síťových zařízení, která se účastni sledovaného provozu - objem dat, generovaných nástrojem pro analýzu - počet administrátorů systému - případně uveďte jiné licenční parametry	Licence pro XDR se vztahují na počet koncových bodů a prostor, který se bude používat ve virtuálním prostředí, o velikosti nejméně 1 TB.	Systém je licencován na základě: - objemu monitorovaného síťového provozu - doba retence (uchovávání) systémem generovaných metadat (násobky 30 dnů) Taková licence pak pokrývá nasazení neomezeného počtu sensorů (včetně specializovaných senzorů pro emailový provoz [SMTP] a webový provoz [ICAP připojení na proxy]), kolektorů a jednu konzoli. Administrátorská konzole je schopna obsloužit/zaregistrovat až 20 dalších komponent systému (podřízené konzole, kolektory, senzory) a umožňuje činnost až 20 současných uživatelů a správců. Licence může mít podobu: - perpetuální licence, pak je nutné počítat s pořízením podpory výrobce, která obsahuje SW update/upgrade/patche, kontinuální aktualizace threat-intel, cloud sandbox a služby technické podpory. - subskripce, která již v sobě obsahuje výše uvedené součásti podpory. Pro sizing je třeba vědět, zda bude Zadavatel schopen poskytnou zdroje na platformě VMware, nebo bude systém provozován na HW appliance výrobce. Systém lze efektivně provozovat na VMware pro objem provozu do cca 10Gbps. Nad tento objem je výhodnější využít HW appliance výrobce. Systém umožňuje vytvoření hierarchické topologie systému/struktury konzolí, a tím pádem i rozdílné a selektivní vhledy to jednotlivých nadřízených/podřízených struktur v rámci celé skupiny.	Nasazení technologie je distribuované, dle velikosti pokrývané topologie v modelu sensor :kolektor (n:1). Pořízení je možné jako perpetuální licence + roční podpora, nebo měsíční pronájem. Licencování vychází ze dvou základních parametrů 1.množství pokrývaných lokalit 2.objem zpracovávaných dat 3.a dvou dodatečných parametrů: počet monitorovaných IP adres a toků za sekundu **1. Množství lokalit.** Každá lokalita, která nedokáže odeslat svá data do jiné centrální lokality, vyžaduje nasazení HW nebo virtuálního sensoru. Tyto sensory následně posílají již zpracovaná metadata na jeden centrální kolektor. Samotný kolektor může sloužit i jako sensor pro danou lokalitu. Komunikace mezi sensorem a kolektorem představuje cca 1-2% analyzovaného provozu. Př: Pokud existují tři lokality Praha, Brno a Ostrava, budou potřeba 1x kolektor pro DC Prahy a 2x sensor pro lokality Brno a Ostrava. Celkem se tedy jedná o tři appliance, HW nebo VA. **2. Objem zpracovávaných dat** Licence u jednotlivých boxu jsou škálovány dle objemu dat – bps, fps a počtu adres v síti. U sensorů a kolektoru se jedná o následující licence: 100Mbps, 200Mbps, 500Mbps, 1Gbps, 2Gbps, 4Gbps, 10Gbps, 25Gbps, 50Gbps, 100Gbps Každý sensor může být osazen libovolným počtem a typem ethernetových portu, kdy uživatel platí pouze cenu HW. Stejně tak kolektor mmůže mít libovolnou velikost úložiště dle potřeb uživatele.	Zadavatel na základě uskutečněného PTK rozhodl, že sjednotí parametr požadované retence dat potřebných pro retrospektivní detekci a vyšetřování na dobu minimálně 30 dní.

Uveďte, jaké jsou potřebné informace, které by Zadavatel měl uvést v rámci zadávací dokumentace tak, aby budoucí uchazeči mohli sestavit svou nabídku včetně nabídkové ceny za poptávané plnění. V případě, že pro tento účel využíváte formuláře pro sběr potřebných dat, prosíme o jejich přiložení k odpovědi.	Pro nabídku jsou vyžadovány následující údaje – počet koncových bodů, objem logů v TB a požadovaná propustnost infrastruktury na aplikační úrovni modelu L7 OSI.	Pro vypracování návrhu řešení a stanovení ceny bude potřeba získat informace v těchto oblastech: - Objem systémem analyzovaného/monitorovaného provozu – součet maxim (peaků) monitorovaného provozu ve všech bodech, kde bude nasazen senzor - Požadovaná doba retence metadat v násobcích 30 dnů - Bude možné využít VMware zdroje Zadavatele pro systém? - Je požadován on-premise sandboxing? - Je požadováno dešifrování provozu? - V kolika místech sítě bude provoz monitorován a v jakém objemu (špičková a průměrná rychlost)? - Preferujete perpetuální licence nebo subskripce? - Jaká je očekávaná doba kontraktu?	Pro návrh architektury je potřeba znát: - Počet monitorovaných lokalit. - U každé lokality odhadovaný průměrný průtok v bitech za sekundu (bps), počet flow za sekundu (fps), počet zařízení, případně počet IP adres v lokalitě. - Specifikaci počtu HW nebo VA nasazení u sensorů. Kolektor bývá u větších nasazení vždy HW appliance, ale záleží na zadavateli. - Dále pak počet a typ požadovaných síťových rozhraní u jednotlivých HW sensorů, např. 2x 10GE a 2x 1GE, nebo 4x 25GE a 4x 10GE, apod. U VA jsou ethernet rozraní volitelné uživatelem, a nijak se nelicencují. - Pro kolektor požadovanou dobu retence dat (1,3,6,12,16,24 měsíců), případně přímo velikost úložiště, které je vždy tvořeno kombinací 3,84TB, nebo 7,68TB SSD nebo NVMe disků v RAID 5,6 nebo 10. - Případně požadavek na monitorování operačních technologii (řízení provozu, technologické sítě atd.) u jednotlivých lokalit. - Počet let podpory / pronájem. - Úroveň služeb – základní implementace, školení, servisní dohled

Souhrnné informace o indikativních cenách jednotlivých uchazečů - NDR & EDR			
	Uchazeč 1	**Uchazeč 2**	**Uchazeč 3**
Náklady na dodávku, implementaci a podporu výrobce řešení NDR na 5 let	4 827 000 Kč	63 787 653 Kč	17 499 900 Kč
Náklady na dodávku, implementaci a podporu výrobce řešení EDR na 5 let	25 728 000 Kč	18 964 371 Kč	11 232 636 Kč
Služby technického partnera na 5 let	5 760 000 Kč	8 064 000 Kč	972 000 Kč
Celkové náklady za řešení, implementaci, podpory a služby na	**36 315 000 Kč**	**90 816 024 Kč**	**29 704 536 Kč**

Rozpad indikativních cen jednotlivých uchazečů - NDR & EDR			
Požadovaná položka cenové kalkulace řešení NDR	**Uchazeč 1**	**Uchazeč 2**	**Uchazeč 3**
Náklady na licence nabízeného řešení	4 032 000 Kč	22 920 000 Kč	4 905 400 Kč
Náklady na hardware	- Kč	6 710 453 Kč	2 643 000 Kč
Náklady na technické podpory výrobce nabízeného řešení	- Kč	29 120 400 Kč	8 997 500 Kč
Náklady na technické podpory výrobce hardware	- Kč	- Kč	- Kč
Jednorázové služby technického partnera: - Před-implementační analýza - Instalace a konfigurace - Optimalizace bezpečnostní / detekční politiky řešení - Napojení na platformu Log management / SIEM - Zaškolení servisního týmu zadavatele - Zaškolení týmu SOC zadavatele	795 000 Kč	5 036 800 Kč	954 000 Kč
Požadovaná položka cenové kalkulace řešení EDR			
Náklady na licence nabízeného řešení	25 728 000 Kč	7 800 000 Kč	10 932 636 Kč
Náklady na hardware	- Kč	1 027 571 Kč	300 000 Kč
Náklady na technické podpory výrobce nabízeného řešení	- Kč	9 756 000 Kč	- Kč
Náklady na technické podpory výrobce hardware	- Kč	- Kč	- Kč
Jednorázové služby technického partnera: - Před-implementační analýza - Instalace a konfigurace - Optimalizace bezpečnostní / detekční politiky řešení - Napojení na platformu Log management / SIEM - Zaškolení servisního týmu zadavatele - Zaškolení týmu SOC zadavatele		380 800 Kč	- Kč
Služby technického partnera			
Průběžné služby technického partnera / dodavatele řešení: - Technická podpora servisního týmu zadavatele (řešení chybových stavů) - Údržba řešení (profylaxe, upgrade, update) - Konzultace a rozvojové aktivity (nová pravidla, změna architektury)	5 760 000 Kč	8 064 000 Kč	972 000 Kč