Příloha č. 2: Technická specifikace

Popis cílového stavu a specifikace předmětu plnění

Cílem projektu je zvýšení bezpečnosti a související modernizace IT infrastruktury, aby implementací projektu byly naplněny požadavky Standardu konektivity škol, rozšířena funkčnosti ICT prostředí školy a odstraněny nedostatky současného stavu. Dále jsou popsány rozvojové oblasti a specifikace rozvojových opatření pro naplnění požadavků Standardu konektivity.

Současné rozvody LAN pokrývají pouze nejzákladnější potřeby, proto dojde k vybudování nových páteřních optických tras a metalických koncových tras. Rozvody LAN budou vybudovány jako hvězdicovité, tj. distribuční přepínače (popř. sestavy/stohy přepínačů v datovém rozvaděči) budou přímo napojeny na centrální přepínač školy tak, aby na centrálním přepínači mohl být monitorován veškerý síťový provoz školy s výjimkou peer-to-peer komunikace v rámci distribučních přepínačů. Pro tyto potřeby budou pořízeny nové centrální a přístupové přepínače. Pro zajištění vysoké dostupnosti bude každý prvek 2x ve stohu = dva prvky se budou chovat jako jeden. Propojení aktivních prvků a důležitých systémů (serveru, NAS, páteřní rozvody) bude disponovat rychlostí 10Gbps. Pro potřeby rozvodu LAN a WiFi sítě budou vybudovány patrové rozvodové racky. Pokrytí WiFi v potřebných prostorách školy zajistí jednotlivé přístupové body, které budou umístěny do relevantních učeben a chodeb. Umístění pořízených AP bude provedeno dle projektové dokumentace, nicméně přesné umístění bude upřesněno na základě provedené analýzy pokrytí signálem pro zajištění konzistentní WiFi služby v pokrytých prostorách. Provedení WiFi analýzy bude součástí projektu. Architektura WiFi bude založena na řešení s centrální správou prováděnou virtuálním kontrolerem. Virtuální kontroler, bude součástí firmwarů přístupových bodů a bude konfigurován v režimu vysoké dostupnosti a zajistí automatické rozložení zátěže klientů, roaming mezi spravovanými přístupovými body a automatické ladění kanálů a síly signálu včetně detekce a reakce na non-Wi-Fi rušení.

Na všech koncových zařízeních a všech relevantních aktivních prvcích bude implementováno řízení přístupů k síti na základě rolí a členství uživatelské adresářové služby s využitím technologie 802.1X. Pro hosty a externí uživatele bude zřízena samostatná VLAN (Guest VLAN), která bude komunikačně (min. L3 pravidla, ACL) oddělena od vnitřních sítí organizace. Tato VLAN bude mít své L3 rozhraní až na úrovní firewallu, tak aby bylo možné komunikaci podrobit kontrole za pomoci UTM nástrojů (min. AV, IPS, DNS, CRT a WEB kategorizace obsahu) a mohl jí být přiřazen samostatný profil odlišný od profilů pro učitele a žáky. Ověřování přístupu do této VLAN bude zajištěno pomocí tzv. captive portálu – webové autorizace. Captive portál bude zajištěn firewallem případně jiným samostatným řešením nebo prvkem, ale vždy s důrazem na bezpečné oddělení uživatelského provozu od zbytku vnitřních sítí. Řízení provozu v rámci sítě LAN bude realizováno segmentací sítě. Zároveň bude k dispozici technologie QoS (Quality of Services) pro řízení provozu na úrovni kvality služeb.

Ověřování přístupu do LAN bude realizováno protokolem 802.1X vůči adresářové službě prostřednictvím protokolů radius a P/EAP. Používaná zařízení (min. stolní i přenosné počítače) budou vybavena tzv. suplikantem-softwarovou komponentou, která dokáže předávat ověřovací požadavky síťovým prvkům, které tyto požadavky ověří vůči adresářové služby. Pro ověření zařízení bez suplikantů (např. starší tiskárny, zařízení na bázi jednoduchých operačních systémů či firmware apod.) bude použit jiný-dodavatelem navržený vhodný způsob ověření. Neověřená zařízení nezískají přístup do sítě vůbec nebo jim bude zpřístupněna pouze VLAN s omezeným přístupem (např. Intranet). Spolu s ověřováním (autentizací) bude implementována i autorizace, tedy dynamické zařazení klientského zařízení nebo uživatele do určené VLAN.

Ověřování přístupu do WiFi sítě bude realizováno na stejném principu jako LAN (tj. protokol 802.1X + radius). Wifi bude nabízet více SSID (učitelé, žáci, Guest), které budou obsluhovány samostatnými VLAN a budou napojeny na radius servery. Učitelé a žáci budou prostřednictvím radius serveru ověřováni v adresářové službě. Zabezpečení vnitřních sítí (BSSID) školy bude provedeno dle 802.1i, tedy-WPA3 (v odůvodněných případech WPA2) s AES šifrováním a konfigurováno shodně pro obě frekvenční pásma. Výjimkou bude síť určená výhradně pro hosty (Guest WiFi), kde bude realizován tzv. captive portál zajišťující webovou autentizaci hostů pomocí přidělených účtů nebo za pomoci před-generovaných číselných kupónů. Preferován bude captive portál firewallu s tzv. lobby přístupem pro správu a generování účtů/kupónů ne-technickou osobou.

Bude implementováno řešení typu „log management“, které bude sloužit pro sběr, ukládání, sledování změn v konfiguracích, správu provozních a bezpečnostních informací a událostí ze sledovaných systémů. Mandatorní informace, která bude v systému vždy obsažena a uchována, je vazba IP-uživatel-čas.

V rámci projektu bude pořízen nový server, který bude sloužit jako hlavní virtualizační platforma, jak pro nově pořízené technologie, tak pro současné a díky tomu dojde k sjednocení několika pozáručních fyzických serverů, které škola aktuálně využívá. Server bude vybaven rychlými SSD disky a umožní připojení optickou linkou 2x 10Gbit. Dodávka licencí pro hypervizor, nové operační systémy a klientské licence je součástí projektu. Zároveň, při přenosu služeb na nový server, bude proveden upgrade všech operačních systémů na nové verze. Ochranou nově pořízených technologií vůči výpadku elektrického proudu bude UPS, která bude pořízena v rámci projektu.

Aktuálně nedostatečný systém zálohování bude nahrazen novým síťovým úložištěm „NAS“ s dostatečnou kapacitou pro ukládání provozních záloh. Zálohování bude řízeno pokročilým zálohovacím softwarem, který bude prostřednictvím virtualizačního hypervizoru zálohovat všechny virtuální servery. Zálohovací systém umožní zálohovat i fyzické servery a osobní počítače. Síťové úložiště NAS bude kvůli bezpečnému oddělení záloh umístěno mimo místnost serveru.

Požadavky technického řešení

- Je požadováno řešení zachovávající a rozvíjející současné softwarové platformy Microsoft pro zachování kompatibility se stávajícími systémy a aplikacemi. Přechod na jinou platformu by způsobil uživatelské a provozní potíže.
- Pokud dodavatelem nabízené řešení vyžaduje komponenty či služby neobsažené v požadavcích zadání, zahrne dodavatel do své ceny všechny náklady na jejich pořízení, instalaci, konfiguraci a další služby potřebné pro uvedení do provozu.
- Zadavatel z důvodů co nejjednodušší a jednotné správy a minimalizace provozních nákladů vyžaduje využití stávajících prostředků a používaných technologií. V případě, že dodavatel vyžaduje ve svém řešení stejné nebo podobné funkce, jaké poskytují stávající prostředky a technologie, je povinen využít nebo vhodným způsobem rozšířit stávající prostředky.

- Veškeré produkty, které dodavatel dodává v rámci plnění zadavateli, musí splňovat následující podmínky:
    - jsou nové, byly oprávněně uvedeny na trh v EU nebo pochází z autorizovaného prodejního kanálu výrobce,
    - mají plnou záruku od výrobce,
    - mohou být podporovány výrobcem a mohou být součástí servisního a podpůrného programu výrobce,
    - obsahují všechny nezbytné licence na používání příslušného softwaru,
    - jsou v databázi výrobce uvedeny jako prodaná kupujícímu,
    - jsou určeny pro provoz v České republice.

Tyto skutečnosti dodavatel doloží čestným prohlášením distributora, popř. dodavatelem samotným, nelze-li prohlášení distributora získat.

- Zadavatel si vyhrazuje právo na zjištění původu výrobků při jejich předávání, a to dle příslušných sériových čísel a právo podpisu akceptačního protokolu, osvědčujícího převzetí dodávky, až po ověření původu výrobku.
- Veškerá realizační dokumentace dodávaná v rámci veřejné zakázky, musí být zhotovena výhradně v českém jazyce, bude dodána v elektronické formě ve standardních formátech (např. MS Office, Open Office, PDF) používaných zadavatelem na datovém nosiči a 1x v papírové formě. Struktura i forma dokumentace musí být před předáním předána ke kontrole a výslovně schválena zadavatelem.

Implementační služby

Budou provedeny minimálně následující implementační práce na dodaných komponentech a případně dalších zařízeních. Účastník dále do nabídky zahrnul veškeré další činnosti a prostředky, které jsou nezbytné pro provedení díla v rozsahu doporučeném výrobci a dle tzv. nejlepších praktik, i v případě, pokud nejsou explicitně uvedeny, ale jsou pro realizaci předmětu plnění podstatné. Implementační služby budou minimálně v následujícím rozsahu:

- Zpracování předimplementační analýzy
- Zpracování prováděcí dokumentace
  Práce ovlivňující činnost uživatelů budou prováděny mimo běžnou pracovní dobu.
- Zajištění projektového vedení realizace předmětu plnění
- Dodávku, instalaci a konfiguraci nabízeného hardware
- Kompletní implementaci řešení splňující povinné parametry technického řešení, minimální tyto činnosti:

Prvek	Min. požadované činnosti
Obecné	- Pro každou jednotlivou technologii bude předložen návrh akceptačních testů, který podlého schválení zadavatelem - Návrh bude předložen v rámci Předimplementační analýzy - Aktualizace firmware všech dodaných zařízení na aktuální verzi
Server	- Montáž zařízení do racku - Návrh a kompletní implementace serverové virtualizační platformy - Analýza dat a systémů na stávajících serverech a jejich migrace na novou platformu - Upgrade operačních systémů na aktuální verzi
Licence SW pro virtualizační platformu	- Návrh a implementace virtualizační platformy - Migrace stávajících VM na novou platformu
Záložní zdroj UPS	- Implementace a fyzická instalace dodané technologie - Konfigurace řízeného shutdownu v případě výpadku el. Energie (korektní vypnutí běžících VM)
Licence operačních systémů serverů	- Zalicencování VM
Perimetrový firewall	- Montáž zařízení do racku - Migrace restrikcí ze současného FW - Provedení segmentace LAN (VLAN, adresování, routování, nastavení IPv4 pravidel) - Migrace současného VPN nastavení - Konfigurace dvoufaktorového ověření pro VPN účty pomocí Azure SSO SAML - Návrh a implementace bezpečnostních pravidel
HW pro sběr a správu logů (log management)	- Návrh a implementace systému pro centrální logování, které musí splňovat minimální požadavky „Standardu konektivity“. - monitoring a logování NAT (RFC 2663) provozu za účelem dohledatelnosti veřejného provozu k vnitřnímu zařízení - Logování přístupu uživatelů do sítě umožňující dohledání vazeb IP adresa – čas-počítačový systém - Logování provozu za účelem dohledatelnosti na úroveň koncového uživatele. - Logování konfiguračních změn všech monitorovaných zařízeních

	- Provedení souvisejících konfigurací monitorovaných systémů
Wildcard certifikát	- Zabezpečení komunikace publikovaných služeb pomocí nabízeného certifikátu. - Zavedení DNSSEC pro interní DNS služby i zabezpečení domén škol.
NAS (síťové úložiště) pro ukládání záloh	- Implementace a fyzická instalace zařízení - Konfigurace zařízení pro ukládání záloh - Konfigurace ochrany záloh vůči ransomware
SW licence zálohovací software	- Implementace dodaného systému - Návrh a nastavení zálohovacích jobů
Přepínače	- Návrh a implementace přepínačů, která musí splňovat minimální požadavky „Standardu konektivity“. - Konfigurace Multi-Chassis Link Aggregation - Vytvoření virtuálních stacků u distribučních přepínačů
Přístupový bod WiFi	- Analýza stávajícího síťového prostředí a návrh nové architektury LAN i WiFi - Analýza šíření WiFi signálu a rozmístění AP na základě jejího výsledku. - Zajištění vzájemně oddělených sítí pro zaměstnance školy, žáky/studenty školy a externí zařízení (hosty).
Eduroam	- Připojení do federovaného systému Eduroam.
Systém 802.1x	- Návrh a implementace 802.1X pro kabelovou LAN i WiFi včetně uživatelské dokumentace pro konfigurace obvyklých zařízení a jejich systémů - PC, notebooky, chytré telefony, tablety, tiskárny, Windows, Linux, MacOS, Android, IOS, embedded systémy periferií
Rozvody LAN	- Provedení detailního měření realizovaných metalických i optických rozvodů včetně přenosových parametrů (útlum, odrazy apod.), zhotovení a poskytnutí dokumentace měření.

- Dokumentace (prováděcí, následně provozní)
- Zajištění zkušebního provozu infrastruktury v délce minimálně 2 týdnů včetně technické podpory specialistů na dané zařízení/službu s dostupností maximálně do 2 hodin na místě realizace od nahlášení požadavku v pracovní den v době od 7h do 17h.
- Provedení akceptačních testů
- Předání do ostrého provozu
- Zajištění ostatních služeb potřebných pro realizaci projektu.

Náklady na provedení implementačních služeb musí být zahrnuty v nabídkové ceně k položce, ke které se vztahují a nelze je vyčíslit zvlášť.

Předimplementační analýza
Před implementací řešení zpracuje účastník předimplementační analýzu, jejímž výstupem bude písemná zpráva a návrh scénáře postupu, které podléhají schválení zadavatelem.

Prováděcí dokumentace
Účastník před zahájením implementačních prací zpracuje prováděcí dokumentaci, která bude důsledně vycházet ze schválené předimplementační analýzy a bude zahrnovat všechny aktivity potřebné pro řádné zajištění implementace předmětu plnění do stávajícího prostředí technologického centra.

Školení

- Účastník zajistí školení pracovníků zadavatele – administrátorů – na zařízení a systémy, dodávané v rámci této veřejné zakázky, a to v rozsahu předávané provozní dokumentace.
- Školení zajistí seznámení pracovníků zadavatele se všemi podstatnými částmi díla v rozsahu potřebném pro provoz, údržbu a identifikaci nestandardních stavů systému a jejich příčin.
- Rozsah školení je min. 40 hodin.
- Školení bude probíhat v sídle zadavatele.
- Náklady na školení budou zahrnuty v nabídkové ceně k položce, ke které se vztahují a nelze je vyčíslit zvlášť.

Provozní dokumentace

- Dodavatel zpracuje provozní dokumentaci, která bude detailně popisovat konfiguraci zhotoveného díla a jeho vazby na stávající systémy.
- Součást provozní dokumentace bude popis úkonů doporučené údržby a specifikace intervalů jejích provádění.
- Součástí provozní dokumentace bude popis základních chybových stavů a doporučený postup obsluhy při závadě na zařízení.

Záruky a servisní podmínky

- Požadavky na záruky a servisní podmínky
    - Zadavatel požaduje bezplatný (zahrnutý v ceně zakázky) přístup k aktualizacím software a firmware dodaného SW/HW minimálně po dobu záruky.
    - Veškeré opravy po dobu záruky budou provedeny bez dalších nákladů pro zadavatele.
    - Veškeré komponenty, náhradní díly a práce, poskytnuté v rámci záruky budou poskytnuty bezplatně.
    - Po dobu 60 měsíců od předání díla jako celku do plného provozu, musí dodavatel nebo výrobce všech zařízení garantovat běžnou dostupnost náhradních komponentů a dostupnost servisu.
    - Pro hlášení servisních požadavků zajistí dodavatel zhotoviteli přístup ke svému helpdeskovému systém s on-line přístupem pro kompletní správu požadavků včetně uchování historie požadavků a jejich řešení. Detailní popis helpdeskového systému a jeho obsluhy musí být součástí předávacích dokladů při předání díla. Provozní doba helpdeskového systému musí být minimálně 7-17 hod. v pracovních dnech.

Popis povinných parametrů dodávaného řešení

Prvek	Parametr	Popis povinného parametru
Server 1ks	Formát serveru	Dvou socketový server v rackové provedení, max. 1U, včetně montážního materiálu do racku (Zásuvné ližiny pro rack)
	Bezpečnost	Podpora TPM čipu minimálně verze 2.0
	CPU	1x osmi-jádrový procesor. Výkon serveru dle http://www.spec.org/ CPU 2017 Integer Rates Base Result min 127 bodů, CPU2017 Floating Point Rates Base Result min 145 bodů.
	RAM	minimálně 96GB DDR4, min. 3200MT/s
	Diskové šachty	min. 8x disková hotswap šachta pro disky 2,5”, přístupná zpředu
	HDD	min. 5x 480GB SSD kategorie Read Intensive 6Gbps
	Média pro hypervizor	přítomnost interního USB rozhraní s podporou zavádění hypervisoru a failoveru;
	Diskový řadič	typu SAS, podpora hot-plug disků SAS, SSD i SATA, Cache řadiče min. 8GB se zálohováním proti výpadku napájení na dobu min. 72hodin; Řadič nezabírá volné PCI-e sloty
		Řadič pro zavádění hypervizoru, osazený 2x 240GB M.2 disky s HW RAID1 (sw zrcadlení se nepřipouští)
	RAID	podpora min. RAID - 10, 50, 60
	Pass-thru	Podpora pass-thru přístupu k jednotlivým diskům
	Síťové rozhraní	Min. 2x 1000Base-T
		Min. 2x 10Gb SFP+ port typu OCP NIC 3.0 zakončený LC konektorem
	Napájení	Redundantní zdroje 230V, min. 700W; certifikaci min. Titanium
	Interface	min. 4xUSB port, sériový port
	Management	LCD display indikující základní informace o systému (min. IP adresa, model, chybové stavy, atd.) na čelním panelu, konfigurovatelný
	Podpora OS a virtualizace	Microsoft Windows Server 2016, 2019, 2022; VMware ESX 7-8
	Management a vzdálená správa	Nezávislý management serveru na operačním systému poskytující následující management funkce a vlastnosti:
		: vyhrazený LAN port
		: integrace managementu do ActiveDirectory a dvoufaktorová authentikace (TFA), encryption)
		: web GUI a dedikovaná IP adresa
		: připojení zařízení správce pomocí USB portu bez nutnosti mngmnt LAN
		: vzdálená konzole (KVM) přes IP
		: virtualizace vzdálených médií (USB, CD/DVD, file share, ISO)
		: nastavení IP konfigurace a čtení chybových stavů z out-of-band managementu, bez potřeby připojení monitoru a klávesnice
		: instalace OS přes management serveru (včetně driverů)
		: sledování hardwarových sensorů (teplota, napětí, stav, chybové sensory)

		: error alerty (server reset, kritické sensorové hodnoty, atd.) za použití email traps, SNMP atd.
		: podpora IPv6
		: server reset, reboot, power-on/off/cycle
		: failover management LAN portu na jinou síťovou kartu na desce serveru (LOM)
		: správa napájení serveru, včetně monitorování spotřeby
		: Management serveru nepožaduje instalaci agenta jak pro monitoring, tak pro update SW/FW/BIOS v jednotlivých HW komponentech serveru
		: REST API rozhraní součástí hardware serveru, včetně dokumentace - pro monitorování a správu serverů pomocí skriptů a pro integraci s dalšími systémy
	Záruka a servis	Záruka min. 60 měsíců, oprava následující pracovní den od nahlášení požadavku v místě instalace. Možnost kontaktovat (zadat požadavek) 24x7 přes telefon, chat, či web portál. Servis je poskytován výrobcem.
		Automatická a proaktivní detekce problémů s automatickým založením ticketu v případě problému a zahájením řešení opravy.
		nabízené zboží musí být pokryto oficiální podporou výrobce zařízení v ČR a záruku si musí být možné ověřit na webu výrobce po zadání sériového čísla zařízení.
	Podpora	Podpora prostřednictvím internetu musí umožňovat stahování ovladačů a manuálů adresně pro konkrétní server identifikovaný sériovým či produktovým číslem každého serveru bez nutnosti platné záruky či servisního kontraktu s výrobcem. Možnost provázání managementu serveru pro online spojení technickou podporou výrobce a automatickým otevíráním servisních požadavků včetně automatického odeslání HW a OS logů pro následný troubleshooting proces.
	Kompatibilita se stávajícím prostředím	Server musí být plně kompatibilní a plně 100% integrován do současného management nástroje Zadavatele OpenManage Enterprise.
Licence SW pro virtualizační platformu 1ks	Platforma	Virtualizační platforma umožňující běh neomezené množství virtuálních strojů.
	Licence	Licence umožňující použití min. pro 2 CPU
	Kompatibilita	Kompatibilní s nabízeným serverem a zálohovacím SW.
	Záruka	Podpora výrobce a nárok na nové verze minimálně po dobu 36 měsíců
Záložní zdroj UPS 1ks	Provedení	Provedení do racku, max. 4U, včetně montážního materiálu
	Napětí, vstup	Jmenovité napětí 230 V, 1f/1f
	Výkon	3000 VA, 2700 W
	Technologie	Line interaktivní
	Kapacita	Doba běhu na baterie min. 18 minut při 50% zátěži
	Výstupy	min. 8x zásuvka C13 a min. 2x zásuvka C19
	Stabilizace	Nepřetržitá vícepólová filtrace šumu Propuštěné přepětí podle ieee 0,3 % Nulová doba odezvy na klíčování

	Servis	Baterie musí být vyměnitelné za chodu, aniž by bylo nutné odstavovat připojená zařízení
	Komunikační porty	Karta pro řízení přes web/SNMP
	Stavové informace	Stavový grafický displej pro konfiguraci a základní informace o stavu UPS
	Řízení	Schopnost korektního shutdownu operačních systémů na nabízeném serveru.
	SW kompatibilita	UPS musí být plně podporována výrobcem pro použití ve virtuálním prostředí Vmware a Microsoft Hyper-V
	Úroveň hluku	Max. 55 dBA
	Záruka	Záruka UPS min 36 měsíců, na baterie záruka min, 24 měsíců
Licence operačních systémů serverů 4ks	Popis	Licence 64-bitového serverového operačního systému v poslední (nejnovější) verzi kompatibilní se stávajícím vybavením Zadavatele. Každá licence musí umožnit provoz min. 2 virtuálních serverů stejné verze v prostředí nabízené serverové virtualizace a reflektovat potřebný počet Core licence vůči nabízenému serveru. Dále musí umožnit provoz všech současných aplikací a management nástrojů.
Klientské licence operačních systémů 150ks	Popis	Klientské licence pro nabízené operační systémy umožňující využívat těchto systémů uživatelům celkem na 150 zařízeních.
Perimetrový firewall 1ks	Provedení	Umístitelné do racku
	HW parametry	Počet síťových rozhraní LAN RJ45 1 Gb - min 14x
		Počet rozhraní USB pro připojení ext. modemu - min. 1x
	Výkon	Propustnost firewallu min. 20 Gb/s nezávisle na velikosti paketu
		Propustnost firewallu - min. 15 Mpps (pps - paketů za sekundu)
		Počet FW politik min. 10 000
		Počet současných otevřených spojení - min 1,5 M
		Propustnost VPN - min. 11,5 Gbps
		Propustnost IPS - min 2,6 Gbps
		Propustnost antiviru - min. 1 Gbps
	Funkce	Režim vysoké dostupnosti - Active Active, Active Passive, Clustering
		Režim fungování L2 – transparentní režim, L3 – NAT/Router
		Podpora multicast, vytváření politiky pro multicast routování
		Podpora VPN: IPSec, SSL (portálový režim, tunelový režim), IPSEC (IKE, manual key, certifikát, gateway to gateway, hub and spoke, dial up konfiugrace, internet browsing konfigurace, podpora vice tunelů – redundantní VPN
		Podpora IPv6
		Podpora virtualizace (min. 10 virtuálních kontextů - firewallů)
		Podpora dynamických routovací protokolů - OSPF, PPTP, L2TP, GRE
	Firewall	Možnost nastavovat firewall politiku na základě geografických údajů.
		Podpora Identity based policy – nastavení bezpečnosti uživateli na základě členství ve skupině na doménovém kontroléru Active Directory.

		Funkce Load Balancing – možnost rozdělování zátěže směrující na virtuální IP na reálně servery, podpora health check funkcí, podpora SSL offload.
		Podpora centrální NATovací tabulky
	Filtrační funkce	Možnost výběru mezi file based režimem (buffer) nebo flow based (inspekce on-the-fly)
		Antivirus pro vybrané protokoly, možnost volby různých databází, podpora archivace škodlivého obsahu, podpora protokolu ICAP pro offload AV engine, možnost detekce tzv. Grayware (rootkit, malware, spywave, keylogger, atd)
		Email filter – antispamová a antivirová inspekce elektronické pošty
		Intrusion Protection System – detekce útoků založena na signaturové části a na anomálním filtru, možnost vytvářet vlastní signatury.
		Web Filter – založená na kategorizaci webového obsahu, možnost monitorování navštívených kategorii na uživatele či skupinu, možnost kvóty – uživatel může navštěvovat určitou kategorii jen po určitou dobu během dne.
		Application Control – detekce, monitoring, povolení či zakázání vice než 2000 síťových aplikací na základě signatury dané aplikace, nikoliv dle portu.
		Kontrola komunikace v SSL šifrovaných protokolech (HTTPS, IMAPS, POP3S)
		DoS Policy prevence proti základním útokům typu DoS, syn proxy
	Ověřování uživatelů	LDAP, Active Directory, Radius, TACACS+, Ověřování na základě certifikátu
		Podpora silné autentizace uživatelů – integrovaná podpora generátoru jednorázových hesel (OTP) – Token pro dvoufaktorovou autentizaci, podpora certifikátů pro ověření uživatelů
		Dynamické profily – možnost přiřadit konkrétní profil uživateli na základě jeho ověření.
	Dynamické routování	RIP, BGP, OSPF, IS-IS
		Policy routing
		Traffic Shaping, QoS s podporou DSCP markování a ToS
		Podpora VoIP, SIP včetně zabezpečení, rate limitingu, analýzy protokolu
		WAN optimalizace (optimalizace vybraných protokolů, byte chaching), Web Cache, Explicitní Proxy, Reverzní proxy, WCCP
	Reporty	Integrované logování a reporting, možnost vytváření vlastních reportů
	SFP+ moduly a patch cordy	Součástí dodávky jsou potřebné originální SFP+ moduly a optické/metalické propojovací kabely pro realizace díla.
	Záruka	Záruka výrobce min. 60 měsíců v režimu 24x7 na HW, OS, firmware a kompletní bezpečnostní SW. SW musí obsahovat IPS, AV, Web Filtering a Antispam aktualizace.
HW pro sběr a správu logů (log management) 1ks	Obecné požadavky na systém pro centralizovanou správu logů, událostí a strojových dat	Systém pracuje jako hardwarová appliance s jedním uceleným webovým rozhraním pro všechny administrátorské i operátorské činnosti. Nevyžaduje instalaci dalších systémů a aplikací, vyjma podpory sběru na pobočkách a agenta pro sběr Windows logů. Doložte katalogový list produktu (datasheet) podrobně popisující hardwarové i softwarové parametry nabízeného systému.
		Systém provádí zpracování událostí z předdefinovaných zdrojů logů napříč výrobci aplikací, operačních systémů a síťového hardware min. FortiGate, Dell, Cisco, Windows Defender, Microsoft 365, Vmware, Aruba

		Veškerá konfigurace systému se musí provádět v grafickém rozhraní jednotné uživatelské webové konzole. Systém poskytuje podporu pro vizuální programování pro všechny kroky zpracování strojových dat. Ve webové konzoli se nepřipouští konfigurace za využití skriptů, maker nebo textových konfiguračních polí, do kterých se složité textové skripty/makra vkládají.
		Systém umožňuje dopsání parserů pro výše neuvedená zařízení uživatelem bez nutnosti spolupráce s výrobcem nebo dodavatelem (vč. poddodavatelů) nabízeného systému - Uživatelsky definované parsery. Dokumentace musí obsahovat přehledný návod na vytváření zákaznických parserů a systém musí obsahovat možnost testování a ladění zákaznických parserů v jednotném ovládacím grafickém webovém rozhraní. Vytváření a testování parserů nesmí mít vliv na provoz systému. Pro psaní parserů nesmí být použito textové psaní programového kódu ale tzv. vizuální programování, které automaticky opravuje uživatele a upozorňuje ho na chyby. Požadujeme předložit příslušnou dokumentaci k vytváření parserů a testování jejich funkčnosti.
		Systém umožňuje v grafickém rozhraní vizuálního programovacího jazyka snadno provádět třídění a značkování vstupních dat pro jejich další zpracování. Nepřipouští se nastavování třídění vstupních dat ve formě skriptu/makra zobrazeného v textovém okně. Předložte příslušný odkaz na dokumentaci popisující funkčnost třídění vstupních dat.
		Systém přijímá a zpracovává logy, události a další strojově generovaná data prostřednictvím minimálně následujících protokolů: SYSLOG (dle RFC3164, RFC5424, RFC5425) a RELP. Systém musí umožňovat příjem logů i na rozsahu alespoň 50 UDP a TCP portů pro zjednodušené třídění vstupních zpráv. Dále požadujeme podporu sběru strojových dat z databází s nastavením v grafickém menu systému minimálně pro databáze MSSQL, MySQL, Oracle a PostgreSQL a to bez nutnosti instalovat na databázový server doplňkový software nebo agenta. Předložte detailní komunikační matrici s popisem všech použitých protokolů a portů pro nabízený systém a dokumentaci k nastavení sběru z databází v grafickém rozhraní systému.
		Přijaté logy systém standardizuje do jednotného formátu a logy jsou normalizovány (rozdělovány) do příslušných polí dle jejich typu. Zároveň systém uchovává i originální verzi zpráv. Integrované parsery systému automaticky přidávají ke zprávám, kterých se to týká, meta informace o jaký druh zprávy se jedná, minimálně požadujeme rozlišení těchto druhů zpráv: úspěšné přihlášení, neúspěšné přihlášení, odhlášení, konfigurační změna, značka/tag. Tyto meta informace musí být možné přidávat i v uživatelsky definovaných parserech.
		Hodnoty jednotlivých parsovaných polí je možné v definici parseru přetypovat a standardizovat alespoň na tyto základní druhy: číslo, IP adresa, MAC adresa, URL. Nad uloženými čísly je pak možné při prohledávání dat provádět matematické operace (součty všech hodnot, průměry, nejmenší/největší hodnota apod.).
		Systém zachovává původní informaci ze zdroje logu o časové značce události, ale nedůvěřuje jí a vytváří vlastní důvěryhodné časové razítko ke každému logu, které vzniká v okamžiku přijetí logu systémem a kterým se systém defaultně řídí.
		Všechna pole a položky přijaté systémem jsou automaticky indexovány. Nad všemi položkami je možné ihned provádět vyhledávání bez nutnosti dodatečného ručního indexování administrátorem.
		Možnost sběru událostí minimálně ve formátech RAW, Syslog RFC5424, CEF, LEEF, JSON RFC8259.

		Systém nesmí v žádném případě umožnit mazání nebo modifikování již uložených logů v rámci požadované retence. A to ani libovolnou konfigurační změnou - administrátorovi s nejvyššími oprávněními k navrhovanému systému. Každý zpracovaný log musí mít dohledatelný unikátní identifikátor, který umožní jeho jednoznačnou identifikaci.
		Systém musí umožňovat konfiguraci filtrace nerelevantních událostí v grafickém rozhraní vizuálního programovacího jazyka. Pro psaní filtrace nesmí být použito textové psaní programového kódu ale tzv. vizuální programování, které automaticky opravuje uživatele a upozorňuje ho na chyby. Předložte odkaz na dokumentaci popisující způsob filtrování nerelevantních událostí.
		Systém provádí konsolidaci logů na interním storage logovacího systému.
		Systém umožňuje snadné vyhledávání událostí a okamžité vytváření grafických reportů (ad hoc) bez nutnosti dodatečného programování nebo aplikování dotazů v SQL jazyce. Reportovací nástroj musí být integrální součástí navrhovaného systému a musí se obsluhovat v jednotném rozhraní nabízeného produktu. Předložte link nebo pdf popisující způsob vytváření reportů.
		Systém provádí ucelenou vizualizaci logů, událostí a strojových dat (grafy událostí). Vizualizace musí být dynamická, tj. volbou v jednom grafu se ostatní příslušné grafy v pohledu na data upraví dle požadované volby automaticky.
		Systém umožňuje snadno vytvářet grafické znázornění událostí v dashboardech nad všemi uloženými daty za libovolné časové období bez nutnosti nejprve modifikovat konfiguraci systému nebo parametrů uložených dat. Historická data v požadované délce retence uložená v systému je možné prohledávat okamžitě bez časových prodlev opětovného importu nebo dekomprimace starších dat, prohledávání dat nesmí vyžadovat manuální konfiguraci a zásahy uživatele.
		Systém umožňuje snadno vytvářet grafické znázornění událostí v dashboardech nad všemi uloženými daty za libovolné časové období bez nutnosti nejprve modifikovat konfiguraci systému nebo parametrů uložených dat. Historická data v požadované délce retence uložená v systému je možné prohledávat okamžitě bez časových prodlev opětovného importu nebo dekomprimace starších dat, prohledávání dat nesmí vyžadovat manuální konfiguraci a zásahy uživatele.
		Systém podporuje nativní získávání logů z Office365/Microsoft365 prostředí bez ohledu na použitou licenci 365 prostředí a bez nutnosti instalovat dodatečné externí komponenty. Požadujeme předložit link na dokumentaci popisující nastavení systému v jednotném grafickém rozhraní tak, aby získával logy z Office365/Mircosoft365.
		V případě krátkodobého (do 10 minut) až dvounásobného přetížení systému proti jeho tabulkovým hodnotám nesmí dojít ke ztrátě logů nebo nesprávnému stanovení časového razítka. Všechny přijaté nezpracované logy/události musí být ukládány do vyrovnávací paměti.
		Systém musí umožňovat unifikované vyhledávání napříč všemi typy dat a zařízeními dle normalizovaných polí (uživatelské jméno,zdrojová IP, značka/tag apod.).
		Dodavatel musí předložit potvrzení vystavené autorizovanou osobou o shodě, že nabízený systém splňuje požadavky normy ČSN/ISO 27001:2013 na pořizování auditních záznamů. Toto potvrzení není možné nahradit certifikátem na společnost dodavatele (subdodavatele) nebo výrobce nabízeného systému. Nelze nahradit čestným prohlášením.
		Systém musí mít možnost uložení uživatelem vytvořených pohledů na data (dashboardů) pro budoucí zpracování. Továrně dodané pohledy na data nesmí jít administrátorem ani uživatelem systému nevratně modifikovat nebo smazat.

		Systém obsahuje reportovací nástroj s přednastavenými nejběžnějšími reporty a možností vlastních úprav a vytvoření nových pohledů. Pro vytváření nových pohledů na data není přípustné používat povinně SQL jazyk.
		Systém obsahuje předpřipravené pohledy na uložená data dle jednotlivých kategorií zdrojových zařízení i dle logického členění.
		Na základě pohledu na uložená data lze provést export dat ve strukturovaném formátu tak, jak jsou v továrně nastaveném nebo uživatelsky nastaveném pohledu data skutečně zobrazena.
		Konfigurační a Systémové rozhraní a dokumentace k těmto rozhraním musí být identické v anglickém i v českém jazyce. Nepřipouští se omezená dokumentace v českém jazyce nebo zjednodušená dokumentace odkazující na další dokumentaci v anglickém jazyce, případně na dokumentaci třetích stran. Požadujeme předložit link na online dokumentaci nebo připojit pdf aktuální kompletní dokumentace k ověření jednotlivých vlastností navrhovaného systému.
		Systém nabízí kapacitní i výkonovou škálovatelnost.
		Čistá kapacita úložného prostoru (kapacita diskového pole) dostupná pro uložená data nabízeného systému musí být minimálně 12TB.
		Požadujeme, aby ze systému bylo možné za běhu vytáhnout libovolný disk, bez ztráty dat a vlivu na funkčnost řešení. Redundance disků nesmí ovlivňovat požadovanou kapacitu úložiště.
		Monitoring stavu systému - alertování při překročení prahových hodnot nebo chybě systému, přeposlání upozornění pomocí SMTP nebo Syslog.
		Požadujeme, aby systém obsahoval REST-API pro integraci s externím monitorovacím systémem (Zabbix, Nagios, MRTG a další) a umožňoval autorizovaný přístup ke strukturované databázi logů. Požadujeme předložit vzorový návod na integraci s externím monitorovacím systémem.
		Dodavatel doloží prohlášení výrobce o shodě s požadavky Vyhlášky 82 / 2018 Sb. „o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)“ k Zákonu 181 / 2014 Sb. „o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)“.
		Jednotná centrální webová konzole s jednotným grafickým rozhraním pro přístup k logům, alertům, reportům a pro správu systému. Z této konzole se provádí veškerá konfigurace, správa i analýza logů. Není přípustné, aby navrhovaný systém měl více rozdílných konzolí od různých výrobců s rozdílným ovládáním nebo aby se konfigurace musela provádět mimo jednotné webové rozhraní. Požadujeme předložit dokumentaci, ze které je zřejmé, jakým způsobem je realizována konfigurace v rámci jednotné konzole.
		Požadujeme, aby systém umožňoval jednotné vytváření uživatelských rolí definujících přístupová práva k uloženým událostem na základě typu zdrojů a značek a k jednotlivým ovládacím komponentům systému. Připojte odkaz na dokumentaci popisující vytváření uživatelských rolí v grafickém rozhraní systému.
		Dodaný systém musí obsahovat ucelené all-in-one řešení pro parsování a normalizaci přijatých událostí bez nutnosti dodatečné instalace externích aplikací nebo systémů. Jedinou přípustnou výjimkou je monitorování systémů Windows pomocí agentů.

		Systém musí podporovat ověřování uživatele systému na externím LDAP serveru. V případě výpadku externího LDAP systému musí podporovat ověření lokálního účtu. Systém automaticky zaznamenává uživatelská jména u akcí provedených konkrétním uživatelem.
	HW parametry požadovaného systému	Jedna hardwarová appliance o velikosti max. 1U, včetně ramena pro kabelový management umožňujícího vysunutí zapnutého systému z racku pro servisní účely.
		HW appliance obsahuje veškeré potřebné komponenty (CPU, RAM, diskový prostor) pro svoji činnost a je nezávislá na dalších systémech.
		min 1 procesor, min. 16 jader, s podporou HyperThreadingu nebo Multi-Threadingu.
		RAM Min. 64GB DDR-4.
		Minimálně 12TB pro integrovanou databázi podporovanou HW akcelerovaným SAS RAID řadičem. Řadič diskového pole musí obsahovat zálohovací baterii nebo být vybaven flash pamětí.
		Z výkonových důvodů požadujeme, aby v systému byly minimálně 4 ks stejných RAID edition disků určených pro použití v datacentrech, o rychlosti minimálně 7200 otáček/m.
		Minimálně 4x 1Gbit LAN porty + 1x dedikovaný 1Gbit port pro management HW. Konfigurace všech parametrů síťového rozhraní včetně link agregace dle LACP (802.3ad), VLAN a IP adresace v jednotném webovém rozhraní systému a doložte příslušný odkaz na dokumentaci.
		Větráky v systému musí být vyměnitelné za provozu a redundantní.
		2x napájecí zdroje s redundancí napájení 1+1.
		Virtuální KVM (tj. převzetí textové i grafické konzole serveru a zajištění přenosu povelů z klávesnice a myši vzdáleného počítače.
		Systém pro vzdálenou správu serveru včetně potřebné licence, pokud je třeba (obdoba HP iLO, Dell iDRAC apod).
	Výkonnostní a SW parametry systému	Systém funguje formou HW appliance (všechny části systémů je možné nastavit v centrální webové konzoli a není nutné editovat žádné konfigurační soubory, scripty nebo makra v příkazové řádce).
		Aktualizace systému jsou distribuovány v jednotném balíku a jejich instalace je prováděna uživatelsky přes centrální webovou správcovskou konzoli. Všechny aktualizace musí být prováděny z webového prostředí bez potřeby asistence dodavatele/výrobce dodávaného systému. Požadujeme předložení posledních 4 poznámek k novému vydání (release notes) pro kontrolu parametrů navrhovaného systému.
		Systém musí podporovat downgrade v jednom kroku, pro případ problémů s novou verzí systému po upgrade. Není přípustný downgrade pouze za součinnosti výrobce. Popište podrobně způsob realizace downgrade.
		Průměrný trvalý příjem min. 2000 událostí/s. Výkon musí být dosažen na požadované množství událostí s průměrnou délkou zpráv minimálně 700Byte trvale. Systém musí prokazatelně kompletně zpracovat přijaté události včetně vytváření očekávaných metadat (DNS-PTR, čísla a jména ASN, geolokace), zajišťovat normalizaci, zamezovat ztrátě přijatých událostí nebo posunutí důvěryhodného časového razítka oproti času skutečného příjmu každé události.
		Špičkový příjem minimálně 4000 událostí/s po dobu nejméně 10 minut a průměrnou délkou minimálně 700byte. Systém musí prokazatelně kompletně zpracovat přijaté události, zamezovat ztrátě ukládaných dat nebo posunutí důvěryhodného časového razítka oproti času skutečného příjmu zpráv. Při zpracování dat během špičkového příjmu

		akceptujeme zpoždění zobrazení zpracovávaných dat. Systém ani ve špičkovém výkonu nesmí dovolit ztrátu dat, skluz důvěryhodného časového razítka nebo jiné prokazatelné vady na zpracovávaných datech oproti zpracování při průměrném trvalému příjmu událostí.
		Licenčně neomezený počet zařízení pro příjem zasílaných událostí. Licenčně neomezený počet událostí v GB za den nebo licence na minimálně 200GB uložených událostí za den. Integrovaná databáze musí mít čistou velikost nejméně 12 TB a nad to musí podporovat kompresi ukládaných dat.
		Uživatelská konfigurace klasifikace dat, parserů, filtrů a alertů se provádí pomocí vizuálního programovacího jazyka v centrální správcovské webové konzoli. Vizuální programovací jazyk musí uživateli umožnit psát konfigurace bez nutnosti znalosti programování (např. Node-RED, Microsoft VPL, Blockly apod). Vizuální programovací jazyk není prezentován textově, ale graficky formou schémat-symbolů, které reprezentují aplikační logiku a kontrolují syntaxi. Doložte odkazem na dokumentaci systém vizuálního programování a popisu jednotlivých použitých komponent vizuálního programování nástroje.
		Konfigurace uživatelských parserů musí umožňovat automatické doplňování DNS reverzních záznamů, čísel a jmen autonomních sítí, geolokační informace a identifikace výrobce zařízení podle MAC adresy.
		Systém musí podporovat doplňování zpráv o informace z textových prohledávacích tabulek. (Například k uživatelskému jménu doplnit z textové prohledávací tabulky informaci o jeho emailu, členství v AD skupinách a podobně). Pro automatickou aktualizaci takto uložených doplňujících informací musejí být tyto textové prohledávací tabulky naplnitelné pomocí REST API nabízeného systému a modifikovatelné přes jednotné webové rozhraní. Doložte odkazem na dokumentaci, jakým způsobem lze plnit textové tabulky prostřednictvím REST-API nabízeného systému.
		Možnost on-line ladění uživatelsky definovaných parserů - při jejich vytváření je možné vložit skupinu testovacích zpráv, při změně je okamžitě zobrazena výsledná podoba rozparsovaných dat a případná chybová hlášení s upozorněním na chybná místa vytvářeného parseru. Pro snadnější vytváření parserů požadujeme mít možnost vložení minimálně 20 testovacích zpráv současně. Doložte odkazem na dokumentaci, ze které je zřejmé, jakým způsobem se vkládají testovací zprávy během psaní nového uživatelského parseru a jakým způsobem je prezentován výstup testu.
		V centrální správcovské konzoli je možné přidávat k jednotlivým zdrojům dat, aplikacím, zařízením nebo IP subnetům tzv. značky, označující například umístění zařízení, typ zařízení, kritičnost zařízení apod. Systém obsahuje předdefinované značky, které automaticky přidává k přijímaným zprávám. Příklady značek: konfigurační změna, úspešné ověření uživatele, neúspěšné ověření uživatele, zpráva přišla z windows, zpráva byla vygenerována firewallem atd...
		Všechny přidávané značky jsou ukládány s každou přijatou událostí, na základě značky je možné filtrovat data nebo omezovat oprávnění uživatelů systému k jednotlivým událostem.
		Pro budoucí nasazení ve vysoké dostupnosti a výkonnostní rozšíření je vyžadována podpora sestavení ve vysoké dostupnosti – požadujeme podporu minimálně 4 nodů v clusteru. Nastavení clusteru se musí kompletně realizovat v grafickém rozhraní správcovské konzole v jednom kroku, není přípustné konfigurovat sestavení scripty, makry nebo úpravou textové konfigurace systému a pomocí ručních restartů služeb. Systém ve vysoké dostupnosti musí přehledně informovat o stavu clusteru a procesu synchronizace databází. Dokumentace k realizaci vysoké dostupnosti musí být

		kompletní a popisovat všechny kroky sestavování a obnovení v případě výpadku komponenty clusteru. Doložte odkazem na dokumentaci, jakým způsobem se cluster vytváří a jakým způsobem se provádí obnovení po možném výpadku jednotlivých zúčastněných komponent.
		Vícenodový cluster se chová i ovládá jako jednotný systém, nutnost nezávislé konfigurace na každé jednotce v clusteru je vyloučena. Vícenodový cluster umožnuje geolokační oddělení a pro komunikaci v rámci clusteru musí využívat definovaný TCP/UDP port pro snadné nastavení prostupy firewallu. Veškerá komunikace v rámci clusteru musí být šifrovaná s vysokým kryptografickým standardem pro bezpečné vytvoření privátní virtuální sítě na síťové vrstvě. Popište použitou technologii zabezpečení komunikace v rámci clusteru.
		V případě využití více nodů v clusteru se automaticky zrychluje zpracování vstupních dat a vyhledávání v již uložených datech.
		V případě rozšíření systému na cluster musí navrhovaný systém zajistit bezvýpadkovost sběru logů.
		Systém musí umožňovat export dat ve formátu vhodném pro další strojové zpracování bez dodatečných omezení na časové období, množství nebo obsah exportovaných dat. Během exportu je možné označit pouze vybraná pole, která mají být do exportu zahrnuta.
		Podpora zálohování nebo obnovení konfigurace v jednom kroku a jednom souboru pro celý systém. Doložte odkazem na dokumentaci, jakým způsobem se provádí zálohování a obnova konfigurace systému.
		Podpora důvěryhodného zálohování dat na externí systém. Požadováno plánované i ad-hoc zálohování. Zálohy dat musejí být vhodně kompresovány a umožnit v budoucnosti obnovení bez ohledu na verzi systému, ve které byla záloha pořízena. Doložte odkazem na dokumentaci, jakým způsobem se realizuje zálohování a obnova záloh.
	Alerty	Systém je schopen na základě uživatelsky zadaných podmínek splněných v přijatých datech vygenerovat alert.
		Text emailu vygenerovaného alertem musí být uživatelsky definovatelný s proměnnými, které jsou vyplněny z přijaté rozparsované události.
		Systém musí obsahovat výrobcem předpřipravené sety/vzory alertů a korelací.
		Systém musí provádět konfigurace alertů a korelací pomocí vizuálního programovacího jazyka. Vizuální programovací jazyk není prezentován čistě textově, ale textově-grafickou formou, která vizualizuje aplikační logiku vytvářeného alertu. Konfigurace alertů musí umožňovat okamžitou kontrolu funkčnosti výstupu alertu nebo korelace vložením příslušné testovací zprávy, včetně zobrazení upozornění na případné uživatelské chyby. Doložte odkazem na dokumentaci, jakým způsobem realizujete konfiguraci a testovaní alertů a korelací.
		Jako výstupní pravidlo Alertu musí systém umět odeslat událost, která alert vyvolala, na externí systém minimálně prostřednictvím SMTP nebo Syslogu přes TCP protokol. U Syslog protokolu požadujeme možnost definice formátu odesílaných dat pro snazší integraci se systémy třetích stran. Doložte odkazem na dokumentaci, jakým způsobem se zpráva, která vyvolala spuštění alertu, odesílá na externí systém a jak se definuje formát odesílání dat.
		V alertech je možné nejen využívat, ale i přiřazovat značky (příklad: pošli alert jen v případě, že se událost stala na kritickém serveru a je označen názvem lokality, nebo pokud událost obsahuje podmínku, přiřaď novou značku). Doložte odkazem na dokumentaci, jakým způsobem lze v jednotném grafickém rozhraní systému definovat a přiřazovat značky.

		Systém podporuje základní funkce SIEM - funkce pro korelace událostí a upozornění s hraničními limity. Definice korelačních pravidel je prováděna pomocí vizuálního programovacího jazyka a musí obsahovat možnost vložení testovací zprávy a zobrazení výsledku testu o provedené akci.
	Sběr událostí z Microsoft prostředí	Události z Microsoft prostředí jsou vyčítány pomocí agenta instalovaného přímo v koncových systémech. Windows agent musí současně podporovat jak monitoring interních windows logů, tak monitoring textových souborových logů. Agent se nesmí instalovat individuálně, ale prostřednictvím MS AD Group Policy a nesmí vyžadovat žádnou konfiguraci na cílovém systému. Doložte odkaz na dokumentaci popisující požadované vlastnosti integrovaného Windows agenta.
		Agent provádí instalaci a podporuje centralizovanou konfiguraci Microsoft Sysmon pro obohacení logů, včetně globálního a selektivního zapínaní/vypínaní služby Sysmon a výběr z několika přednastavených konfigurací Sysmon v grafickém rozhraní centrální správcovské konzole systému. Doložte odkazem na dokumentaci, jakým způsobem se provádí centralizované řízení a konfigurace Microsoft Sysmon služby.
		Agent sběru z Microsoft podporuje globální i lokální nastavení filtrace odesílaných událostí pomocí centrální správcovské konzole. Například, zašli pouze logy z adresářů eventview Systém, Security, Sysmon a Terminal Services a zahoď logy s EventId 7036.
		Filtrace odesílaných událostí agenty se konfiguruje pomocí vizuálního programovacího jazyka z centrální správcovské konzole systému. Logy nastavené k filtraci jsou filtrovány na straně windows agenta a nejsou nijak odesílány po síti. Vizuální programovací jazyk není prezentován textově, ale textově-grafickou formou, která vizualizuje aplikační logiku vytvářeného alertu. Doložte odkazem na dokumentaci, jakým způsobem se vytváří a přiřazují filtry pro Windows agenty pro sběr logů a jakým způsobem se testuje účinnost filtru.
		Windows agent nevyžaduje administrátorské zásahy na koncovém systému – je centrálně spravovaný a jeho konfigurace musí být kompletně realizována v grafickém rozhraní systému bez využití skriptů nebo maker. Konfigurace musí být automaticky distribuována přímo z centrální konzole systému. Tj. vlastní správa a aktualizace Windows agenta se neprovádí z Group Policy.
		Komunikace Windows agenta a centrálního systému musí být zabezpečena TLS 1.2 a výše a musí podporovat ověřování certifikátem.
		Windows agent podporuje sběr nejen ze základních systémových logů (Aplikace, Zabezpečení, Instalace, Systém), ale je možné z centrální konzole v grafickém rozhraní nastavit i sběr všech ostatních logů ve složce Protokoly aplikací a služeb a logy rozšířené Sysmonem. Dále musí Windows agent podporovat centralizované nastavení z administrátorské konzole systému pro sběr textových logů včetně možnosti výběru jejich formátu. Doložte odkazem na dokumentaci, jakým způsobem se nastavují parametry sběru logů globálně a jakým způsobem u konkrétního agenta.
		Windows agent automaticky doplňuje ke všem odesílaným událostem jejich textový popis tak, jak je zobrazen v Prohlížeči událostí (Event Viewer) na koncovém systému. K bezpečnostním událostem hodným pozornosti doplňuje značku a popis dle MITRE ATT&CK® matrice a k takto detekovaným procesům a souborům automaticky vytváří SHA256 hash.
		Počet instalací Windows agenta by neměl být licenčně a časově omezen, pokud je licenčně nebo časově omezen, tak požadujeme dodání licencí na Windows agenty v množství 150 na dobu předpokládané morální životnosti produktu –

		7 let. Předpokládáme instalaci agentů na všechny systémy současně, proto je nutné potvrdit zda systém výkonnostně splňuje tento požadavek. Jedná se o klíčovou funkci, proto je nutné před uzavřením smlouvy předvedení požadovaných funkcí, stability i výkonnostní kapacity nabízeného systému pro sběr logů z prostředí Microsoft.
	Podpora pro sběr událostí z poboček	Systém musí obsahovat centrálně spravované řešení, které sbírá události na pobočkách a umožní jejich odeslání po saturované lince bez ztráty dat. Doložte odkazem na dokumentaci, jakým způsobem realizujete sběr událostí z poboček.
		Systém musí podporovat centralizovanou správu pro sběr událostí přímo z centrálního úložiště dat včetně dokumentace požadavků na virtualizaci a komunikační matici pro šifrovaný přenos dat.
		Řešení musí být schopno automaticky navázat spojení s centrálním úložištěm dat a přenášená data šifrovat. V případě výpadku spojení mezi pobočkou a centrálou musí spojení automaticky obnovit.
		Řešení musí komunikovat po definovaném TCP/UDP portu, aby mohl být snadno nastaven prostup přes firewally a řešena kvalita služby (QoS) pro přenos událostí. Doložte odkazem na dokumentaci, jak vypadá komunikační matice pro připojení rešení pro sběr událostí na pobočkách.
		Řešení musí poskytovat kapacitu vyrovnávací paměti pro minimálně 100GB událostí, které na pobočce mohou vzniknout během výpadku spojení mezi pobočkou a datovým centrem.
		Řešení pro sběr dat z poboček musí mít výkon minimálně 5 tisíc událostí/s, a to i v trvalé zátěži.
		Řešení musí poskytnout podporu pro sběr událostí na identických UDP i TCP portech jako hlavní dodaný systém.
		Řešení musí být k dispozici jako fyzický systém nebo jako virtuální systém pro VMware ESXi a Hyper-V.
		Řešení musí být schopno komunikovat z pobočky na centrálu i přes vícenásobný překlad adres (NAT).
	Vysoká dostupnost, SW Podpora a záruka na hardware	Požadujeme volitelnou podporu pro nasazení ve vysoké dostupnosti.
		HW - Požadovaná min. 3letá servisní podpora na hardware appliance s opravou v místě instalace serveru a s garantovanou odezvou následující pracovní den od nahlášení případné závady.
		Systém musí podporovat vygenerování TSR (technického support reportu) pro možnost diagnostiky bez vzdáleného přístupu.
		SW - Podpora výrobce na aktualizaci systému a parserů na 5 let. Podpora musí obsahovat aktualizaci SW minimálně 3x ročně, opravy chyb a telefonickou a emailovou podporu s diagnostikou vzdáleným přístupem.
Wildcard certifikát 1ks	Popis	Hvězdičkový (tzv. wildcard) certifikát veřejné certifikační autority pro zabezpečení služeb publikovaných do internetu. Kořenový certifikát certifikační autority musí být standardně obsažen v běžných desktopových a mobilních operačních systémech a být automaticky aktualizován v rámci aktualizace operačního systému.
	Záruka	min. 60 měsíců
NAS (síťové úložiště) pro ukládání záloh 1ks	Provedení	Samostatně stojící s možností osadit i mimo rack
	Výkon	64bit CPU, min 4 jádra
	HDD	Min. 6 pozic pro HDD, rozšíření min. na 16 HDD
	Rozšiřitelnost	Podpora připojení externích disků přes USB 3.2 (min 3 porty)
	Hot-swap	Disky vyměnitelné za chodu
	SSD HDD	Podpora SSD disků pro ukládání dat i akceleraci rotačních HDD

	Kapacita	Osazeno min. 4x 4TB HDD SATA od stejného výrobce, jako je výrobce NAS. Disky jsou výrobcem určeny pro použití v NAS.
	Konektivita	Min. 4x 1Gbit Ethernet porty s podporou agregace linek a redundance Min. 2x 10Gbit SFP+ porty včetně SFP+ modulů
	Kompatibilita	Plná podpora Windows ADS a ACL
	Virtualizace	Podpora virtualizace Vmware ESXi, Windows Server
	Komunikace LAN	Síťové protokoly CIFS, WebDAB, iSCSI, SSD, SNMP, https
	UPS	Podpora korektního vypnutí sygnálem z UPS přes LAN při výpadku napájení
	RAM	Min. 4GB
	Ochrana dat	Integrované typy ochrany dat RAID 1, RAID 5, RAID 6, RAID 10
	Záruka	Záruka na NAS min. 36 měsíců, na HDD min. 60 měsíců
SW licence zálohovací software 1ks	Licence	Licence zálohovacího software pro min. 10 zálohovaných zařízení (nerozlišuje se mezi VM, fyzickýcm serverem, PC - univerzální použití licence) bez omezení objemu dat
	Efektivita ukládání dat	Integrovaná technologie komprimace a deduplikace.
	Nároky na správu	„Bezagentové“ řešení – není nutná instalace agentů do zálohovaných virtuálních serverů nebo aplikací.
		Možnost replikace virtuálních strojů na jiný virtualizační nod za chodu serveru
	Ochrana dat	Provádění datově konzistentních záloh hlavních serverových aplikací - MS SQL, Active Directory, souborové systémy - bez nutnosti odstávky aplikace
	Fyzické servery	Vestavěná podpora zálohování fyzických serverů - pro fyzické servery je přípustné využívat agenty
		Podpora ukládání záloh nevirtualizovaných serverů a PC do společného úložiště a monitorování zálohovacích úloh
	Snapshoty	Využívání snapshotů, zálohování pouze dat změněných od poslední úspěšné zálohy
		Podpora operačních systémů Windows a Linux v zálohovaných virtuálních serverech
	Ověření záloh	Možnost otestování a ověření každého zálohovaného VM a jeho obnovitelnosti spuštěním přímo ze souboru zálohy; včetně podpory pro vlastní testovací skripty.
	Obnova položek Active Directory	Obnova jednotlivých i skupin objektů Active Directory – uživatelů, skupin, kontejnerů, objektů Group Policy včetně hromadného výběru a obnovy hesel účtů
	Uložiště záloh	Možnost ukládání záloh na diskový prostor
		Možnost nouzového spuštění zazálohovaného virtuálního serveru z NAS v izolovaném prostředí bez nutnosti obnovy
	Správa	Vytváření a správa úloh (zálohování, obnova apod.) pomocí průvodců
		Automatický reporting úspěšných i neúspěšných úloh
	Správa	Běžné úlohy obnovy (obnovení souboru, databáze SQL, objekty Active Directory) provádět pomocí průvodců.
		Záruka 60 měsíců včetně nároku na nové verze software
Centrální přepínač včetně příslušenství 2ks	Základní parametry	L2/L3 přepínač v rackovém provedení max. 1U
	Porty	min. 24x 1Gb/10Gb SFP+ porty, min. 2x 40Gb QSFP+ porty
	Propustnost	min. 640 Gbps

	Agregace portů	podpora Multi-Chassis Link Aggregation na úrovni všech portů a podpora LACP
	VLAN	Podpora VLAN
	Ověřování uživatelů a zařízení	Podpora 802.1X
	Dualstack	Podpora Dualstack pro IPv4 a IPv6
	Optické moduly	Součástí dodávky musí být SFP+ a QSFP+ moduly od stejného výrobce, jako je nabízený centrální přepínač a to v potřebném počtu pro redundatní připojení všech nabízených přepínačů a technologií.
	Monitoring a správa	CLI, WEB, SNMP, RPC-API, SSH
	Zdoje	min. 2x plně redundantní hot-swap zdroje
	Záruka	min. 60 měsíců
Přístupový přepínač 48p stohovatelný včetně příslušenství 4ks	Základní parametry	L2 přepínač v rackovém provedení max. 1U
	Porty	min. 48x 1Gb RJ45 portů, min. 2x 10Gb SFP+ porty
	PoE+	PoE+ min. 740W
	Propustnost	min. 176 Gbps
	Agregace portů	Podpora LACP
	VLAN	Podpora VLAN
	Stohování	Podpora stohování až 4 prvků v rámci jednoho stacku - jednotný management, několik switchů se chová jako jeden.
	Ověřování uživatelů a zařízení	Podpora 802.1X
	Dualstack	Podpora Dualstack pro IPv4 a IPv6
	Optické moduly	Součástí dodávky musí být SFP+ moduly od stejného výrobce, jako jsou nabízené přepínače a to v potřebném počtu pro redundatní připojení všech nabízených přepínačů.
	Monitoring a správa	CLI, WEB, SNMP, SSH
	Zdoje	min. 2x plně redundantní hot-swap zdroje
	Záruka	min. 48 měsíců
Přístupový přepínač 24p stohovatelný včetně příslušenství 8ks	Základní parametry	L2 přepínač v rackovém provedení max. 1U
	Porty	min. 24x 1Gb RJ45 portů, min. 2x 10Gb SFP+ porty
	PoE+	PoE+ min. 740W
	Propustnost	min. 128 Gbps
	Agregace portů	Podpora LACP
	VLAN	Podpora VLAN
	Stohování	Podpora stohování až 4 prvků v rámci jednoho stacku - jednotný management, několik switchů se chová jako jeden.
	Ověřování uživatelů a zařízení	Podpora 802.1X
	Dualstack	Podpora Dualstack pro IPv4 a IPv6

	Optické moduly	Součástí dodávky musí být SFP+ moduly od stejného výrobce, jako jsou nabízené přepínače, a to v potřebném počtu pro redundatní připojení všech nabízených přepínačů.
	Monitoring a správa	CLI, WEB, SNMP, SSH
	Zdoje	min. 2x plně redundantní hot-swap zdroje
	Záruka	min. 48 měsíců
Přístupový bod WiFi s příslušenstvím 56ks	Základní funkce	Přístupový bod (AP) WiFi včetně montážního materiálu na stěnu nebo strop
	Frekvence	Činnost v radiovém pásmu 2,4 a 5 GHz současně, 2 radiové moduly
	Anténní systém	Interní systém min. 2x2 (5GHz) a MIMO 2x2 (2,4GHz), optimalizovaný pro montáž na strop
	Prenosové rychlosti	SU-MIMO / MU-MIMO (5GHz) až 867 Mbps, SU.MIMO (2,4GHz) až 300 Mbps
	Standardy	Podpora 802.3at, 802.11n, 802.11ac, 802.1x včetně přiřazování do VLAN
	Řízení klientů	Automatické směřování komunikace klientů z 2.4Ghz na 5GHz (pokud klienti podporují obě pásma)
	Rušení	Průběžná detekce non-WiFi rušení a spektrální analýza
	Multi SSID	Podpora vysílání min. 8 SSID (WiFi) současně, podpora přiřazení každého SSID samostatné VLAN
	Zatížení	min. 256 přiřazených (asociovaných) klientů na radiový modul
	Porty	min. 1x 1Gb port, podpora napájení PoE
	Řízení provozu	Klasifikace a kontrola provozu, detekce obvyklých aplikací s možností určení priority nebo šířky pásma zvoleného provozu.
	Řízení kvality služeb	Automatické řízení kvality služeb (QOS) pro hlas a video.
	Současná obsluha více klientů	Podpora MU-MIMO (Multi-User MIMO) - multi-user miltiple input/multiple output
	Bezpečnost	Detekce cicích přístupových bodů zjištěných v LAN i v radiofrekvenčním pásmu.
	Virtuální kontroler	Virtuální, vysoce dostupný kontroler obsažený ve firmware každého přístupového bodu. Umožňuje kompletní centrální správu WiFi infrastruktury a řízení jejího provozu včetně roamingu klientů.
	Monitoring a správa	Plná podpora CLI, SSH, SNMP 1-3, syslog, web rozhraní
	Správa frekvenčního pásma	Automatické dynamické přidělování kanálů a řízení výkonu přístupových bodů pro vyrovnané pokrytí a minimalizaci interference
	Záruka	min. 60 měsíců
Eduroam	Popis	Připojení do federovaného systému Eduroam.
Systém 802.1x	Popis	Systém založený na protokolu RADIUS, integrovaný s Active Directory.
Datové rozvody	Popis	Detailní popis minimálních povinných parametrů silnoproudé a slaboproudé elektroinstalace je uveden v přiloženém Výkaz / Výměr.