Popis současného stavu:

Popis řešení:

Cílem projektu je zvýšení kybernetické bezpečnosti celé IT infrastruktury, výměna nevyhovujících prvků, doplnění bezpečnostních technologií s cílem výrazně zvýšit auditovatelnost dění v IT prostředí.

Celý projekt se skládá z těchto dílčích částí:

Pořadí	***Popis***	***Počet kusů***	
1	Pořízení a implementace nástroje pro zálohování a archivaci	1 komplet	Veeam Data Platform Essentials Enterprise Veeam Backup for Microsoft 365
2	Zabezpečení komunikační sítě pomocí 802.1x	1 komplet	Implementační služba

	Implementace segmentace dle dokumentu 2023		
3	Pořízení a implementace NG Firewall včetně IPS/IDS	2 ks	2 ks FortiGate 120G
3-4	Pořízení a implementace WIFI AP	41 ks	41ks FortiAP 231G
5	Nástroj pro analýzu a monitoring síťového provozu	1 komplet	FortiAnalyzer VM
6	Nástroj pro log management	1 komplet	Wazuh
7	Služby SOC		Služba ARICOMA
8	Dodávka a implementace nástroje pro řízení přístupů a identit (bez Endpoint protection řešení)	1 komplet	Wallix Bastion
9	Servery pro Kybez	2 servery	2x HPE DL325 G11 8SFF
9	Diskové pole pro Kybez	1 storage	1x HPE MSA 2062 10GbE iSCSI SFF Storage
9	Backup servery pro Kybez	2 servery	2x HPE DL345 Gen11 8LFF
10	Licence pro Kybez infra	1 komplet	Microsoft licence
11	Pořízení kryptografického systému zajišťujícího ochranu informací mezi datovými centry a uživatelskými pracovními stanicemi	1 komplet	1x FortiWeb virtual apliance 1x FortiAuthenticator Virtual Appliance 25x FortiToken Software License Key
12	Drobný montážní a spojovací materiál	1 komplet	Dle realizačních potřeb projektu
	Implementace	1 komplet	Služba implementace

POŘÍZENÍ A IMPLEMENTACE NÁSTROJE PRO ZÁLOHOVÁNÍ A ARCHIVACI (LICENCE)

Stávající licence zálohovacího SW Veeam hodlá Zadavatel využívat i nadále a požaduje jejich rozšíření na nové prostředí a sjednocení délky podpory ke koncovému datu 13.9. 2025

Požadovaná licence	***Splňuje (ANO/NE)***	***Popis/ komentář***
Licence zálohovacího SW včetně licencí na sockety dle nabídnutého HW pro zálohování	ANO	3x Veeam Data Platform Essentials Enterprise
Záloha pro 93 licencí poštovních cloudových služeb uživatelů	ANO	93x Veeam Backup for Microsoft 365

ZABEZPEČENÍ KOMUNIKAČNÍ SÍTĚ POMOCÍ 802.1X

Implementace segmentace sítě LAN Dodavatel provede podle existujícího prováděcího dokumentu. Seznam požadovaných činností:

- Vytvoření segmentu pro zálohování, readresace dotčených zařízení a serverů, nastavení přístupu a bezpečnostních politik do tohoto segmentu
- Readresace koncových zařízení – tiskárny, uživatelské stanice, IP kamery atd.
- Vytvoření definovaných segmentů a bezpečnostních politik pro komunikaci mezi nimi
- Vytvoření serverového segmentu bez readresace serverů
- Příprava DMZ segmentu a nastavení komunikačních politik
- Úprava wifi sítí dle prováděcího dokumentu (redukce stávajících)
- Dokumentace cílového stavu

POŘÍZENÍ A IMPLEMENTACE NG FIREWALL VČETNĚ IPS/IDS

Stávající dvojice firewallů FG 200E slouží také jako management nástroj nejen pro funkce firewallu, ale také jako management nástroj pro řízení a konfiguraci LAN switchů. Požadujeme tuto funkci zachovat a nově osazované FW musí být s LAN switchi 100% kompatibilní a umožnit jejich management.

Požadavky na dodávané řešení (název výrobku / produktové číslo)			
(FG-120G) FortiGate 120G		***Splňuje (ANO/NE)***	***Popis / komentář***
Parametr	Požadovaná hodnota		
Provedení	Do racku 1U, včetně montážního kitu	ANO	---
Porty	min. 18x Gb RJ45, min 8x 1Gb SFP, min. 4ks 10 Gb SFP+	ANO	---
NGFW	Min. základní funkce Next-generation firewall - viz https://en.wikipedia.org/wiki/Next-generation_firewall - firewall, aplikační firewall s DPI, IPS. Administrace na bázi "objektů" (aplikace, uživatelů, lokality apod.) namísto IP adres, portů apod.	ANO	---
Počet současných spojení	min. 2,9 miliónu	ANO	3 mio
Propustnost SSL VPN	min. 1,5 Gbps, při licenčním nebo technickém omezení počtu klientů požadujeme min. 150 klientů	ANO	1,5Gbps

Propustnost SSL inspekce	min. 3 Gbps	ANO	3 Gbps
Propustnost firewallu	min. 39 Gbps pro pakety 512 bytů a větší	ANO	39 Gbps
Propustnost NGFW	min. 3,1 Gbps	ANO	3,1 Gbps
Propustnost IPS	min. 5,2 Gbps	ANO	5,3 Gbps
Propustnost detekce škodlivého kódu	min. 2,8 Gbps	ANO	2,8 Gbps
Logování	min. 7 dnů historie v zabezpečeném cloud prostředí	ANO	7 dnů
Virtualizace	min. 10 virtuálních kontextů	ANO	---
Vysoká dostupnost	Režim Active/Passive i Active/Active se společnou konfigurací v případě zapojení druhého firewallu	ANO	---
Dualstack	podpora současného běhu IPv4 a IPv6	ANO	---
Aplikační kontrola	detekce, monitoring, povolení či zakázání obvyklých síťových aplikací na základě signatury dané aplikace, nikoliv dle portu Kontrola komunikace v SSL šifrovaných protokolech (HTTPS, IMAPS, POP3S, …)	ANO	---
Antivir	Integrovaný antivirus, možnost volby různých databází signatur, podpora archivace škodlivého obsahu, podpora protokolu ICAP pro offload AV detekce, možnost detekce tzv. Grayware (rootkit, malware, spywave, keylogger, atd)	ANO	---
Kategorizace a blokace provozu	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	ANO	---
Antispam	antispamová a antivirová inspekce elektronické pošty	ANO	---
Sandbox	Možnost integrovaného sandbox (ověření škodlivosti kódu spuštěním v reálných operačních systémech) v zařízení nebo integrované rozhraní pro napojení na externí službu výrobce zařízení (služba není součástí dodávky)	ANO	---
Aktualizace	automatická aktualizace bezpečnostních funkcí poskytovaná výrobcem zařízení	ANO	---
Ověřování uživatelů	LDAP, Active Directory, Single Sign On vůči Active Directory, Radius, Ověřování na základě certifikátu	ANO	---
Management a monitoring	HTTP/S, SSH, SNMP, syslog	ANO	---
Administrativní rozhraní	Centrální administrativní rozhraní musí umožnovat integraci switchů a WiFi AP stejného výrobce jako je Firewall	ANO	---
Záruka	min. 60 měsíců v režimu 24x7 poskytovaná výrobcem zařízení. Doručení náhradního zařízení max. následující den po nahlášení závady, včetně nároku na bezpečnostní aktualizace firmware a bezpečnostních funkcí - URL filtrace, IPS, antimalvare, antispam, aplikační kontrola)	ANO	---

WIFI AP PŘÍSTUPOVÝ BOD

Požadavky na dodávané řešení (název výrobku / produktové číslo)		
(FAP-231G-E) FortiAP 231G	***Splňuje (ANO/NE)***	***Popis / komentář***
Přístupové body musí být centrálně řízeny a spravovány řešením v podobě on-premise nástroje, který je plně kompatibilní s řešením NGFW a LAN switchů.	ANO	---
Nástroj centrální správy umožňuje terminovat provoz SSID, v tunelovém režimu, s ohledem na možnou potřebu segmentace drátového a bezdrátového provozu	ANO	---
On-premise varianta řešení centrální správy může být součástí jiného, v tomto projektu nabízeného, produktu stejného výrobce	ANO	FG-120
automatická nebo manuální autorizace přístupových bodů na základě auto discovery mechanismu	ANO	---
jednotné management rozhraní, ze kterého lze spravovat přístupové body a případně i další produkty stejného výrobce	ANO	---
jednotné management rozhraní pro správu bezdrátové sítě a bezpečnostních politik souvisejících s konkrétním SSID	ANO	---
jednotné management rozhraní pro zobrazení stavu všech přístupových bodů včetně jim přiřazených SSID, asociovaných klientů interferujících SSID včetně síly signálu interferujícího SSID vůči konkrétnímu přístupovému bodu	ANO	---
možnost vyhledávání, v jednotném management rozhraní, konkrétních připojených zařízení nebo uživatel na základě minimálně následujících parametrů: IP adresa, MAC adres, uživatelské jméno	ANO	---
možnost automatické aktualizace operačního sytému přístupového bude po jeho připojení do sítě	ANO	---
možnost automaticky registrovat přístupový bude na servisní portál výrobce	ANO	---
možnost automatické karantény konkrétního uživatele z jednotného management rozhraní, která zamezí další možnosti připojení se uživatele k bezdrátové síti	ANO	---
možnost hromadného upgrade firmware z jednotného management rozhraní	ANO	---
Konkrétní technické požadavky na bezdrátový přístupový bod s interními anténami	ANO	---
Formát zařízení: indoor s interními anténami	ANO	---
Příslušenství k montáži na zeď/strop/T-Rail	ANO	---
Počet rádií: minimálně 3 pro přenos v pásmech 2,4, 5, 6GHz s podporou Wifi 6E	ANO	---
Minimálně 2x2 MIMO	ANO	---
Dedikované Bluetooth rádio pro lokalizační služby	ANO	---
Alespoň 1x 10/100/1000 Base-T RJ45 uplink, 1x 100/1000/2500 Base-T RJ45	ANO	---
Možnost souběžně provozovat až 16 SSID	ANO	---
Podpora Celulární Co-existence	ANO	---
Podpora napájení pomocí 802.3at	ANO	---
Podpora všech následujících standardů - 802.11a, 802.11b, 802.11d, 802.11e, 802.11g, 802.11h, 802.11i, 802.11j, 802.11k, 802.11n, 802.11r, 802.11u, 802.11v, 802.11w, 802.11ac, 802.11ax, 802.1Q, 802.1X, 802.3ad, 802.3af,	ANO	---

802.3at, 802.3az, 802.3bz		
Kensigton lock na samotném AP	ANO	---
Spektrální analýza přímo na AP	ANO	---
Možnost zachytávání paketů na AP pro jejich analýzu	ANO	---
Podpora výrobce na HW, operační systém a řešení konfiguračních a systémových problémů v režimu 24/7 a možnost výměny vadného zařízení v režimu 8x5. Obojí po dobu 60 měsíců. Záruka opravy nebo výměny vadného zařízení, garantovaná výrobcem, nejméně po dobu 60 měsíců.	ANO	---

NÁSTROJ PRO ANALÝZU A MONITORING SÍŤOVÉHO PROVOZU

Požadavky na dodávané řešení (název)		
(FAZ-VM-GB5) FortiAnalyzer VM, 6 GB Logs (FC1-10-LV0VM) FortiAnalyzer VM, FortiGuard IOC and Outbreak Detection Service	***Splňuje (ANO/NE)***	***Popis / komentář***
Virtuální appliance pro platformu minimálně pro nabízený hypervizor, dále pak VMWARE ESX, Microsoft Hyper-V, KVM	ANO	---
Plná podpora pro instalovanou platformu NGFW	ANO	---
Podpora pro Syslog kompatibilní zařízení	ANO	---
Výkon logování minimálně 6GB/den	ANO	6 GB
Kapacita storage (uložení historických dat) min 500GB	ANO	3TB
Real-time prohledávání logovaných dat	ANO	---
Vyhledávání historických dat podle typu události nebo typu provozu	ANO	---
Vyhledávání podle zařízení	ANO	---
Korelace logů	ANO	---
Funkce zpětné kontroly logů o přístupu na web (až 7 dní) z důvodu „zero-day“ malicious websites	ANO	---
Uživatelská definice reportů (vzhled, obsah apod.)	ANO	---
Automatické generování reportů v daném čase a periodě	ANO	---
Automatické odesílání reportů emailem	ANO	---
Včetně předplatného na službu vyhledávání indikátorů o kompromitaci v logovaných datech.	ANO	---
Bezplatný nárok na nejnovější firmware	ANO	---
Podpora výrobce v režimu 24x7 pro platformu i její provozní konfiguraci včetně politik na 5 let	ANO	---

NÁSTROJ PRO LOG MANAGEMENT

Požadavky na dodávané řešení (název)		
WAZUH	***Splňuje (ANO/NE)***	***Popis / komentář***
Základní funkce: Systém pro sběr, ukládání a správu provozních a bezpečnostních informací a událostí ze sledovaných systémů	ANO	---
Protokoly sběru logů: syslog, TCP, UDP, HTTP, JSON	ANO	---
Zdroje logů: Min. REST API, textové soubory, Radius, Active Directory, MS SQL databáze, Windows Event Log - včetně rozšířených "Applications and Services Logs", síťové prvky - syslog a Netflow, ostatní	ANO	---

aktivní prvky - syslog, SNMP trap		
Parsování logů: Integrovaný nástroj pro parsování logů. Možnost nahrání části logu, online vytváření parseru a snadné testování výsledku. Podpora vytváření opakovaně použitelných vzorků např. definice IP adresy regulárním dotazem apod.	ANO	---
Retence: Uchovávání logů min. 6 měsíců, automatická retence logů a indexů	ANO	---
Geolokace: Podpora automatické doplňování logů o informaci o lokalitě podle IP adresy	ANO	---
Normalizace logů: Sjednocení názvů shodných dat z různých zdrojů logů např. pro snadné vyhledávání napříč zdrojí	ANO	---
Rozšíření logů: Podpora rozšíření logů o vlastní statické a dynamické (kalkulované) položky integrovaným nástrojem.	ANO	---
Bezpečnost: Podpora šifrované komunikace se zdroji (SSL apod.), ověřování zdrojů (TLS apod.)	ANO	---
Dashboardy: Uživatelské vytváření dashboardů (pracovních desek) včetně možnosti využití grafických prvků (grafy, mapy, histogramy apod.) i strukturovaných dat (tabulek)	ANO	---
Export dat: Export dat do csv - min. výsledky hledání	ANO	---
Kanály: Možnost vytváření kanálů - datových sad či toků - na základě pravidel (logických podmínek) a to i napříč různými zdroji. Podpora dalšího zpracování - tvorba alarmů, zobrazení na dashboardu,	ANO	---
Online odesílání do nadřazeného systému apod.	ANO	---
Alerty, notifikace Podpora vytváření alertů - překročení okamžitých či kumulovaných hodnot, zasílaní upozornění	ANO	---
Active Directory: integrace s Active Directory pro ověřování uživatelů, nastavení oprávnění min. administrator a operator.	ANO	---
Vyhledávání: Rychlé a intuitivní vyhledávání v záznamech napříč všemi zdroji i při velkých objemech dat (řády TB). Jednoduchý dotazovací jazyk. Rychlá vyhledávání či filtrování bez tvorby dotazů - např. výběrem v kontextovém menu vybraného pole uloženého záznamu.	ANO	---
Ovládání: Intuitivní grafické webové rozhraní dostupné z běžných prohlížečů (Edge, Chrome, Firefox)	ANO	---
Kompatibilita: Podpora provozu v prostředí serverové virtualizace	ANO	---
Ukládání dat do databáze, případná databázová licence musí být součástí dodávky.	ANO	---
Výstupy: Možnost výstupů do nadřazeného systému pro účely vzdáleného expertního dohledu.	ANO	---
Zabezpečený přenos vhodným protokolem	ANO	---

SLUŽBY KYBERNETICKÉ BEZPEČNOSTI (SOC)

Záměrem Zadavatele je získat komplexní řešení pro řízení kybernetických bezpečnostních událostí a incidentů v podobě služeb spočívajících v kontinuálním sběru, převzetí, detekci, analýze a investigaci bezpečnostních událostí a incidentů, jejich evidenci, reportování opatření a jejich řešení v podobě reakce.

Služba Zadavateli zajistí

- Kontinuální sběr, normalizace, kategorizace a korelace informací (nejen logů) prostřednictvím technologických řešení.

- Převzetí detekovaných skutečností a postoupení procesu řízení bezpečnostních událostí a incidentů, zejména pak v prvé řadě Short Event Triáži, ve které se validuje, zda se jedná o reálnou hrozbu.
- Detailní analýza bezpečnostních událostí a jejich finální vyhodnocení, zda se jedná o bezpečnostní incidenty, nebo o falešné poplachy. V případě falešných poplachů jsou předávány podněty ke zlepšení bezpečnosti, a to zejména detekčních mechanismů jednotlivých bezpečnostních, ale i jiných prvků v infrastruktuře. V případě detekce bezpečnostního incidentu (potvrzení, že se nejedná o falešný poplach), je tento incident v rámci procesu řízení kybernetických bezpečnostních událostí a incidentů podroben investigaci.
- Investigaci kybernetických bezpečnostních incidentů realizujeme s cílem stanovení vektoru útoku, dopadu a dalších informací nezbytných pro vyšetření bezpečnostních incidentů a stanovení adekvátní reakce.
- Následně navrhneme reakci a kooperujeme při reakci. Zde můžeme i na vyžádání poskytnout koordinaci při řízení kybernetických bezpečnostních incidentů, poskytnutím role tzv. Incident koordinátora, případně vyžádat zásah reakčního CSIRT týmu.
- Post incident aktivity, spočívající zejména v evidenci a doporučení pro další rozvoj bezpečnosti.

Požadavky na dodávané řešení		***Splňuje (ANO/NE)***	***Popis / komentář***
Služba Aricoma SOC			
Lokace	Služba je zajišťována z území ČR.	ANO	Ostrava
Jazyk	Služba je dostupná v českém, případně slovenském jazyce.	ANO	Čeština, v domluvených případech angličtina
Prostory	Dodavatel zajistí prostory a hardwarové vybavení pro poskytování služby.	ANO	Součástí služby je veškerý HW.
Kontaktní osoba	Dodavatel zajistí jednotný komunikační kanál pro poskytování služby (kontaktní email, telefon).	ANO	Součást smluvního vztahu
Referenční návštěvy	Dodavatel umožní Zadavateli pravidelné referenční návštěvy dohledového centra za účelem synchronizačních schůzek se SOC operátory jež budou součástí služby a to minimálně 2x ročně.	ANO	Očekáváme referenční návštěvy dle předem definovaného kalendáře
Bezpečnostní požadavky	Dodavatel se zavazuje plnit bezpečnostní požadavky Zadavatele a jako poskytovatel outsourcingové služby podléhá bezpečnostním pravidlům Zadavatele včetně práva na audit. Dodavatel rovněž umožní před podpisem smlouvy Zadavateli návštěvu bezpečnostního dohledového centra za účelem ověření splnění požadavků.	ANO	---

Nástroje Zadavatele	Služba Dodavatele musí podporovat práci s nástroji Zadavatele, dle předmětu VŘ. Zadavatel si vyhrazuje právo během trvání smlouvy na Služby SOC jednotlivé produkty obměnit za jiné v dané kategorii. Takovéto změny se Zadavatel zavazuje vždy předem oznámit Dodavateli.	ANO	---
Adaptační fáze služby bezpečnostního dohledu	Dodavatel zajistí: a) Prvotní analýzu kybernetických bezpečnostních hrozeb relevantních pro aplikace a služby provozované zadavatelem a návrh relevantních Detekčních scénářů b) doplnění nebo rozšíření zdrojů logů, jejichž provozně bezpečnostní informace bude vhodné také sbírat, korelovat a analyzovat c) Návrh nastavení dohledových a monitorovacích nástrojů, včetně atributů a parametrů potřebných pro řádné a efektivní provozování dohledového centra, zahrnující mj. • definice logovacích schémat , která určí, z jakých zdrojů, jakým způsobem a pomocí jakých senzorů (agent, sonda, apod.) budou data sbírána, případně obohacována a korelována • doporučení nastavení logování pro jednotlivé zdroje • doporučení nastavení korelačních pravidel, reportů, parametrů • výběr událostí a parametry jejich záznamů a metody sběru z jednotlivých zdrojů • návrh doplňování logovaných informací z dalších zdrojů pro zlepšení jejich relevantnosti či srozumitelnosti d) Návrh relevantních procesů, potřebných pro řádné a efektivní provozování dohledového centra, zahrnující mj. činnosti při zjištění bezpečnostního incidentu, výpadku či omezení dostupnosti vybraných informačních systémů, způsoby	ANO	Je to součást poskytované služby ve fázi Adaptace.

	notifikace kompetentních osob objednatele podle schváleného eskalačního schématu e) Revize a popis integrace do procesu zvládání KBI zadavatele (např. klasifikace…) f) Návrh komunikačních a eskalačních schémat g) Definice, popis reakčních scénářů (IRP, Workbooky/SOP, Playbooky – automatizované části rekací) h) Kategorizace událostí a incidentů a způsob reakce na tyto incidenty včetně definování SLA i) Vytvoření návrhu vzorového reportu (struktura) o událostech a incidentech j) Součástí služby je také revize definovaných schémat, a to minimálně jednou ročně, případně v rámci významné změny (dle definice v procesu zadavatele)		
Monitoring a detekce	Služba po celou dobu provozu musí zajistit: - průběžný bezpečnostní dohled/monitoring napojených technologií - příjem strojově detekovaných událostí z dohledových systémů (Zadavatele i SOC) identifikovaných na základě definovaných „Detekčních scénářů“ - příjem událostí zaznamenaných pracovníky SOC týmu Dodavatele v rámci služby Threat Hunting - příjem událostí a požadavků od pověřených uživatelů Zadavatele, případně smluvní (třetí) strany	ANO	Je to součást poskytované služby.

Analýza událostí	Dodavatel zajistí analýzu potenciálních incidentů z bezpečnostních alertů, podrobných logů událostí zachycených systémem Zadavatele, včetně návrhu na protiopatření. • úvodní vyhodnocení zaznamenaných událostí a rozhodnutí o dalším postupu (Triage) • probíhá prvotní sběr informací a prověření, zda se nejedná o událost charakteru „False Positive“, případná úprava detekčních scénářů, které vedly k zaznamenání událostí • pro události vyžadujících další kontrolu (charakteru „Event of Interest“) dochází k jejich prvotní analýze a klasifikaci. • v průběhu této fáze jsou informovány kontakty dle platné komunikační matice a definovaných „Scénářů reakce“ (notifikace), dochází také k vytvoření ticketu v Service Desku a předání k dalšímu řešení • dodatečný sběr informací a artefaktů s využitím Operations nástrojů • vyhodnocení události • určení dopadu a zpřesnění klasifikace události • notifikaci kontaktů dle platné komunikační matice a definovaných „Scénářů reakce“ • Update informací, v již otevřeném tiketu v Help Desku	ANO	Je to součást poskytované služby.
Hlášení incidentů	Při zjištění bezpečnostního incidentu s významným dopadem Dodavatel zajistí hlášení směrem k Zadavateli. Toto hlášení musí probíhat předem smluvenými komunikačními kanály (telefonní čísla (hovor, SMS), email), které Zadavatel prokazatelně oznámí Dodavateli před zahájením poskytování služeb.	ANO	Je to součást poskytované služby.

Řešení incidentů	Cílem řešení incidentů je zajistit co nejrychlejší obnovení dostupnosti dohledovaných služeb Zadavatele a současně minimalizovat důsledky incidentu. Dodavatel poskytne osobě MKB Zadavatele know-how analytického týmu, spolupráci a součinnost při koordinaci činností a při vyhodnocování vývoje incidentu a reakcí na KBI.	ANO	Primárně je nastavení procesu na straně Manažera kybernetické bezpečnosti zadavatele. Nicméně jsme připraveni se do procesu IM zapojit dle jeho požadavků, případně být nápomocni při jeho tvorbě.
Koordinační aktivity	Dodavatel se v rámci služby zavazuje zajistit následující koordinační aktivity: a) min. 1x měsíčně synchronizační schůzka (online) se Zadavatelem za účelem seznámení s aktuální bezpečnostní situací a vyhodnocení KPI. b) min. 2x ročně synchronizační schůzka (dle domluvy v prostorách Zadavatele nebo Dodavatele) pro hlubší posouzení bezpečnostní situace a pro návrhy a plánování neustálého zlepšování úrovně SOC.	ANO	Je to součást poskytované služby.
Kontinuální rozvoj	V rámci služby Dodavatel zajistí kontinuální rozvoj služby pro případné úpravy bezpečnostních pravidel, detekcí a reportů a to přinejmenším v následujícím rozsahu: a) tvorba nových korelačních pravidel b) úprava a optimalizace stávajících korelačních pravidel c) reporting	ANO	Je to součást poskytované služby. O tyto aktivity se primárně stará SecDevOps, součást skupiny Aricoma SOC.
Forenzní analýza	Služba Bezpečnostní analýzy a forenzního vyšetřování. Popište službu, případné omezující podmínky.	ANO	Základní kroky analýzy a forenzního pohledu jsou obsaženy přímo ve službě ve formě tzv. Triage, neboli roztřídění a prvotní klasifikaci událostí. Kompletní forenzní analýzu konkrétní události či incidentu nabízíme jako službu v hodinové sazbě Analytika.
Threat intelligence	Služba Threat Intelligence. Popište službu, případné	ANO	využíváme několik OpenSource zdrojů, jako

	omezující podmínky.		je Mittre Attack, MISP, AlienVault OTX, Virus Total a také vlastní TI platformy, kterou využíváme jako klíčovou, tedy Wazuh. V případě síťové detekce a analýzy využíváme TI našich integračních partnerů WhaleBone a Greycortex a také placenou formu TI ProofPoint ETPRO.
Threat hunting	Služba Threat Hunting. Popište službu, případné omezující podmínky.	ANO	Je to součást poskytované služby.
Systém včasného varování	Služba Vulnerability Assesment. Popište službu, případné omezující podmínky.	ANO	Služba Vulnerability Assesment je součástí poskytované služby.
Tvorba scénářů a pravidel	V rámci služby Dodavatel navrhne vytvoření relevantních scénářů KYBEZ na straně Zadavatele, včetně vybudování nové sady detekčních pravidel pro stávající i budoucí produkty a nástroje Zadavatele	ANO	Požadované činnosti jsou předmětem Adaptační fáze služby SOC
Řádná dokumentace	Dodavatel bude využívat vlastní ticketovací systém, kam bude Dodavatel řádně dokumentovat celý životní cyklus každého incidentu.	ANO	V případě delší spolupráce jsme připraveni v případě požadavku integrovat API propojení s Vaším HelpDesk systémem, součástí služby je přístup do našeho HelpDesku MS Dynamic 365.
Komunikace	Komunikace v rámci služby bude probíhat v prostředcích Dodavatele (např. MS Teams).	ANO	---

Kapacity	Dodavatel zajistí realizační tým pro dodávku služeb SOC v navržené kapacitě pro zajištění proaktivního monitoringu v režimu 8x5 a to minimální s následující úrovní kvalifikace: a) L1 operátor - s dostatečnou odborností pro vykonávání činností SOC s prokazatelnou minimální roční praxí jako SOC operátor L1. b) L2 analytik - s prokazatelnou minimální dvouletou praxí jako SOC operátor L1 či jako SOC operátor L2, nebo analytik kybernetické bezpečnosti c) Expertní analityk/architekt - s prokazatelnou minimální dvouletou praxí jako SOC L2 analytik, nebo analytik kybernetické bezpečnosti s pětiletou praxí d) - z toho musí vždy být na straně Dodavatele k dispozici minimálně jeden člen realizačního týmu minimálně na úrovni SOC L2, který bude disponovat odbornou znalostí nástrojů Zadavatele.	ANO	Operačnímu středisku SOC je v případě nutnosti, umožněno k řešení incidentu či události, přizvat někoho z našich cca 120 systémových specialistů na dané technologie. Zvyšuje se tím odbornost při řešení konkrétních systémů, na které jsou tito lidé specializováni.
Expertíza pro krizové situace	Dodavatel zajistí dostupnost kapacit a odpovídající expertizu pro řešení ad hoc bezpečnostních incidentů s významným dopadem.	ANO	Viz předchozí řádek

DODÁVKA A IMPLEMENTACE NÁSTROJE PRO ŘÍZENÍ PŘÍSTUPŮ A IDENTIT

Požadavky na dodávané řešení	***Splňuje (ANO/NE)***	***Popis / komentář***
Wallix Bastion ***- Počet souběžných připojení: bez omezení*** ***- Počet uživatelů: bez omezení***		
Architektura, řízení přístupů		
Nástroj je dodáván jako fully packaged software (obsahuje i OS) s podporou pro virtuální prostředí jako Hyper-V/VMWARE či možností instalace do cloudové infrastruktury (Amazon Web Services, Microsoft Azure).	ANO	---
Systém je spravován pomocí jednotné centrální konzole.	ANO	---
Nástroj funguje jako jednotný přístupový bod pro několik instancí v necentralizované infrastruktuře.	ANO	---
Nástroj funguje jako přístupová proxy.	ANO	---

Nástroj podporuje protokoly SSH a RDP protokoly pro primární spojení, tedy mezi privilegovaným účtem a proxy.	ANO	---
Nástroj podporuje protokoly SSH, RDP, VNC, RLOGIN a TELNET pro sekundární spojení, tedy mezi proxy a monitorovaným systémem.	ANO	---
Nástroj u nepodporovaných protokolů umožňuje spuštění klientské aplikace na jump serveru tak, aby uživateli byla přístupná pouze daná klientská aplikace.	ANO	---
Nástroj nevyžaduje žádné instalace software agentů na monitorovaný systém.	ANO	---
Nástroj podporuje integraci s externími uživatelskými databázemi v minimálním rozsahu LDAP/LDAPS/Microsoft Active Directory/RADIUS/KERBEROS/TACACS+	ANO	---
Nástroj umožňuje uživatelskou autentizaci pomocí jména / hesla, X.509 certifikátu či SSH klíče.	ANO	---
Integrace nástroje s LDAP či Active Directory by nezávisí na periodických synchronizacích. Systém mapuje schémata uživatelských skupin z LDAP/AD do lokálních PAM skupin.	ANO	---
Nástroj umožňuje tvorbu účtů s rozdílnými rolemi- minimálně správce, uživatel a auditor.	ANO	---
Nástroj umožňuje definici uživatelů, spravovaných zařízení a jejich skupin, u kterých bude jednotlivým auditorským účtům uděleno oprávnění prohlížet záznamy.	ANO	---
Nástroj umožňuje konfigurace uživatelských profilů se zahrnutím možnosti filtrovat příchozí připojení na základě zdrojové IP adresy, síťové adresy a masky sítě či FQDN.	ANO	---
Nástroj umožňuje definování cílových systémů zadáním IP adresy, DNS nebo zadáním IP adresy a masky.	ANO	---
Nástroj umožňuje definování přístupových politik přiřazováním uživatelských účtů či skupin k cílovým systémům či jejich skupinám.	ANO	---
Nástroj podporuje integraci se SIEM/SYSLOG.	ANO	---
Nástroj podporuje integraci s ICAP pro kontrolu průchozích souborů prostřednictvím antiviru či DLP s možností blokace nežádoucích přenosů.	ANO	---
Nástroj umožňuje zaznamenávání všech zprostředkovaných relací formou videozáznamu s doplňujícími metadaty.	ANO	---
Nástroj umožňuje aktivaci / deaktivaci zaznamenání relací dle jednotlivých uživatelských skupin.	ANO	---
Nástroj umožňuje shlédnutí záznamů relací prostřednictvím webového rozhraní.	ANO	---
Nástroj umožňuje následný export videozáznamu do běžně podporovaného typu souboru (.mp4 či .flv)	ANO	---
Nastroj umožňuje ukládání zaznamenaných relací lokálně či na externí úložiště CIFS/NFS.	ANO	---
Nástroj zaznamenává a uchovává všechny uživatelem zadané příkazy v průběhu SSH a RDP relací.	ANO	---
Nástroj zaznamenává a uchovává názvy všech oken a procesů otevřených v průběhu RDP relace.	ANO	---

Nástroj umožňuje sběr metadata v průběhu RDP relace alespoň v rozsahu: 1. Změna aktivního okna. 2. Operace s tlačítkem v okně. 3. Volba na radio buttonu či check boxu v okně. 4. Změna obsahu textového pole v okně. 5. Změna rozložení kláves. 6. Začátky a ukončení procesů. 7. Manipulace se soubory prostřednictvím clipboardu. 8. Manipulace se soubory prostřednictvím přesměrovaných lokálních diskových jednotek.	ANO	---
Nástroj umožňuje blokace všech či vybraných TCP spojení zahájených z monitorovaného RDP serveru za účelem navázání neautorizovaných spojení.	ANO	---
Nástroj umožňuje blokování vybraných procesů na systémech Windows Server.	ANO	---
Nástroj u relací SSH a RDP umožňuje definovat vzory regulárních výrazů pro prováděné příkazy, a pokud je takový vzor detekován, umožní nastavit jednu z akcí: ukončení relace nebo odeslání oznámení o detekci vzoru.	ANO	---
Nástroj umožňuje přiřazení definovaných vzorů k monitoringu / ukončování relací k vybraným skupinám uživatelů či systémů.	ANO	---
Nástroj poskytuje ochranu hesel zadávaných v průběhu RDP relace prostřednictvím detekce vstupu kurzoru do pole pro vyplnění hesla či UAC (User Account Control) okna.	ANO	---
Nástroj umožňuje schvalování přístupu privilegovaného uživatele k určitým monitorovaným systémům. Schvalování přístupu musí fungovat minimálně v následujícím rozsahu: 1. Privilegovaný uživatel požádá o přístup 2. Definovaní uživatelé obdrží žádost o schválení přístupu. 3. Minimální definovaný počet uživatelů schválí žádost. 4. Privilegovaný uživatel po schvalovacím procesu automaticky získá přístup k monitorovanému systému.	ANO	---
Nástroj umožňuje vyžadování výše uvedených schvalování v určitých časových rámcích- Např. Pondělí-pátek, 9:00-16:00 bez potřeby schválení, v jiných časech pouze po schválení.	ANO	---
Správce nástroje/auditor má možnost pozorovat probíhající relace v reálném čase, včetně možnosti pozorovanou relaci ukončit.	ANO	---
Při auditu či kontrole proběhlé relace má nástroj možnost zobrazit metadata a videozáznam relace na jedné stránce s časovou osou propojující metadata s vizuální reprezentací.	ANO	---
Nástroj dokáže pracovat se sdílenými účty s možností určení, kdo v daný moment tento účet využíval.	ANO	---
Nástroj poskytuje různé metody autentizace privilegovaných uživatelů na monitorovaných systémech, minimálně: 1.Autentizace privilegovaného uživatele na monitorovaném systému pomocí stejných přihlašovacích údajů, které byly využity pro autentizaci na proxy. 2.Autentizace privilegovaného uživatele na monitorovaném systému pomocí statických a bezpečně uložených přihlašovacích údajů. (např. root, admin, privilegovaný lokální účet). 3.Vyzváním uživatele k opětovnému zadání přihlašovacích údajů k monitorovanému systému, bez jejich zaznamenání.	ANO	---

Nástroj umožňuje vyhledávání systémů a privilegovaných účtů formou scanování RDP + SSH portů a importů z AD.	ANO	---
Nástroj disponuje mechanismem pro plnou či částečnou automatizaci onboardingu nově nalezených zařízení / účtů.	ANO	---
Nástroj lze rozšířit o modul umožňující centralizaci přístupu k několika odděleným instancím prostřednictvím jednotného webového HTML5 rozhraní s integrovaným RDP a SSH klientem pro primární spojení.	ANO	---
Modul pro centralizaci přístupů podporuje prohlížeče Internet Explorer, Microsoft Edge, Google Chrome a Mozilla Firefox bez potřeby instalace pluginů (java, flash)	ANO	---
Modul pro centralizaci přístupů je dodáván jako fully packaged software (obsahuje i OS) s podporou pro virtuální prostředí jako Hyper-V/VMWARE	ANO	---
Modul pro centralizaci přístupů umožňuje auditorským účtům globální vyhledávání napříč metadaty ze všech realizovaných relací všech instancí nástroje.	ANO	---
Zabezpečení a správa přihlašovacích údajů		
Nástroj se shoduje se standardy ISO 27001, HIPAA, SOX a PCI-DSS.	ANO	---
Nástroj bezpečně ukládá citlivá data včetně šifrování hesel pomocí AES 256.	ANO	---
Nástroj bezpečně spravuje a distribuuje SSH klíče.	ANO	---
Nástroj umožňuje automaticky měnit hesla a SSH klíče pro specifické systémy či skupiny účtů.	ANO	---
Nástroj umožňuje definovat výjimky pro zamezení automatických rotací hesel a SSH klíčů u určitých účtů.	ANO	---
Nástroj umožňuje definovat časové intervaly pro provádění automatizovaných změn hesel a SSH klíčů.	ANO	---
Nástroj umožňuje iniciovat změnu hesel a SSH klíčů po každém odhlášení.	ANO	---
Nástroj umožňuje definovat komplexitu generovaných hesel dle počtu znaků, využití malých / velkých písmen a speciálních znaků.	ANO	---
Nástroj nativně podporuje změny hesel u těchto systémů: AIX, F5 BIG IP, SAP IQ, AWS IAM, Checkpoint, ESX, Fortinet Fortigate, HP iLO, MS SQL Server, ORACLE, Stormshield, Teradata, Unix, Microsoft Windows, Cisco, Dell iDRAC, IBM 3270, Juniper SRX, LDAP, MySQL, Palo Alto PA-500, Grafana.	ANO	---
Nástroj musí umožňovat změnu hesel pomocí REST API.	ANO	---
Licence		
Nástroj pochází z oficiálního distribučního kanálu výrobce v zemích EU.	ANO	---
Nástroj je dodáván v poslední verzi publikované jeho výrobcem.	ANO	---
Licencování nástroje není omezeno na počet jeho instancí nasazených v infrastruktuře uživatele.	ANO	---
Podpora		
Zajištění fyzického a vzdáleného šifrovaného přístupu do kompetenčního centra na území ČR, kde budou předinstalovány provozované bezpečnostní systémy zadavatele, včetně příslušných reportovacích nástrojů, a kde bude možné minimálně ověřit funkčnost nových verzí, simulovat problémy produkčního prostředí	ANO	---

a řešit další rozvoj bezpečnostního perimetru zadavatele.		
Podpora výrobce systému - Zahrnuje bezplatný přístup k hotfixům - Zahrnuje bezplatný přístup k novým verzím SW - Zahrnuje přístup k podpoře minimálně Po-Pá, 8:00-18:00 - Reakční čas nejvýše NBD	ANO	přístup k podpoře Po-Pá, 8:00-19:00

SERVER PRO KYBEZ

Požadavky na dodávané řešení		***Splňuje (ANO/NE)***	***Popis / komentář***
(P54199-B21) 2x HPE DL325 G11 8SFF			
Parametr	Požadovaná hodnota		
Form Factor a vnitřní uspořádání	1U, varianta rack	ANO	1U
CPU	jednosocketový systém, osazený jedním procesorem s 16 core, musí mít minimálně 43.500 bodů v testu CPU benchmark https://www.cpubenchmark.net/ Z licenčních důvodů musí být počet 16core dodržen.	ANO	AMD EPYC 9124 Benchmark 43.680
RAM	min. 12 slotů, podpora pamětí typu DDR5 4800MT/s RDIMM s minimální celkovou kapacitou 3TB. Požadujeme osadit 12x64GB	ANO	12x 64GB
Diskový subsystém	Nepožadujeme diskový subsystém pro klasické disky. Pro start OS požadujeme diskový prostor v RAID1 o velikosti min 480GB	ANO	RAID1 480GB
Diskový řadič	Nepožadujeme diskový řadič pro klasické disky.	ANO	---
Interface	- min. 3x externí USB, z toho min. 1x USB 3.0 - dedikovaný USB management port - min. 1x VGA port	ANO	- 3x externí USB, z toho 1x USB 3.0 - dedikovaný USB management port - 1x VGA port
Napájecí zdroje	Dva napájecí zdroje: min. 1000W, účinnost min. 96%	ANO	1.000W Účinnost 96%
Síťové porty	Požadujeme - 1 port 1Gbit RJ-45 pro management - 4 porty 10Gbit SFP+	ANO	---
Kompatibilita	- Canonical® Ubuntu® Server LTS - Microsoft® Windows Server® with Hyper-V - Red Hat® Enterprise Linux VMware® ESXi®	ANO	---
Management a vzdálená správa	- Server musí disponovat vyhrazeným Gb portem pro vzdálený management, port musí mít k dispozici úložiště pro firmware, ovladače a další sw komponenty. Úložiště musí být	ANO	---

	konfigurovatelné pro vytváření instalačních sad s možností rollback/patch při pádu aktualizace. - Server musí podporovat bez agentový vzdálený management. Vzdálený management musí podporovat standardní webové prohlížeče pro grafickou vzdálenou konzoli spolu s tlačítkem pro Virtual Power a podporovat vzdálený boot z DVD/CD/USB zařízení a být schopen uchovávat historická data o sw upgradech a patchích. - Musí být podporována vícefaktorová autentikace. - Musí být monitorovány změny v hw a systémové konfiguraci, musí být podporována rychlá diagnostika vzniklých problémů. - Pro vzdálenou správu musí být podporována mobilní zařízení Android a Apple OS. Vzdálená konzola musí umožnit současný přístup až 6 uživatelům během pre-OS a OS runtime operací, musí existovat schopnost uchovat video z poslední zásadní poruchy a posledního bootovacího procesu, musí být podporována MS TS integrace včetně 128bitové SSL enkrypce a Secure Shell Version 2, musí být podporovány AES a 3DES na prohlížeči a vzdálený firmware update a JAVA free pro vzdálenou konzoli. - Musí být podporována současná podpora většího množství serverů, a to v následujících komponentách: Power Control, Power Caping, Firmware Update, konfigurace, Virtual Media, Licence Activation. - Musí být podporována RESTFullAPI integrace a předávání hw událostí přímo na výrobce serveru.		
Podpora a servis	- podpora na 5let, servisní zásah následující pracovní den - oprava v místě instalace serveru, - servis je poskytován výrobcem serveru - zdarma aktualizace firmware min. po dobu platné podpory - možnost automatického generování servisního incidentu přímo u výrobce hardware.	ANO	---

Podrobný rozpad serveru

1	P54199-B21	HPE DL325 G11 8SFF CTO Svr
1	P53702-B21	AMD EPYC 9124 CPU for HPE
12	P50312-B21	HPE 64GB 2Rx4 PC5-4800B-R Smart Kit
1	P55029-B21	HPE DL3X5 Gen11 1U x16 LP Sec Riser Kit
2	P26256-B21	BCM 57412 10GbE 2p SFP+ OCP3 Adptr
7	P58462-B21	HPE DL3XX Gen11 1U Perf Fan Kit
2	P03178-B21	HPE 1000W FS Ti Ht Plg PS Kit
1	BD505A	HPE iLO Adv 1-svr Lic 3yr Support
1	S1A05A	HPE Cmp Cloud Mgmt Srv FIO Enablement
1	P48183-B21	HPE NS204i-u Gen11 Ht Plg Boot Opt Dev
1	P52351-B21	HPE DL3XX Gen11 Easy Install Rail 2 Kit
1	P57013-B21	HPE DL3X5 G11 NS204i-u NVMe Boot Cbl Kit
1	P58456-B21	HPE DL3XX Gen11 Stnd 1U Heat Sink Kit
1	R7A12AAE	HPE COM Enh 5yr Up ProLiant SaaS
1	HU4B2A5	HPE 5Y Tech Care Basic SVC
1	HU4B2A5#R2M	HPE iLO Advanced Non Blade Support
1	HU4B2A500DE	HPE ProLiant DL325 Gen11 Support

DISKOVÉ POLE PRO KYBEZ:

Požadavky na dodávané řešení		***Splňuje (ANO/NE)***	***Popis / komentář***
(R0Q82B) HPE MSA 2062 10GbE iSCSI SFF Storage			
Parametr	Požadovaná hodnota		
Parametry řadičů pole	- 2x hot-swap řadič, alespoň Active-Active architektura - Diskové pole osazeno alespoň 24GB paměti - 12Gbit/s SAS připojení disků (Backend konektivita) - 8x 10Gb SFP+ Host porty pro připojení k serverům - 2x dedikovaný 1000MBaseT management port	ANO	Dual řadič Active-Active 24GB RAM 12Gbit SAS backend 8x SFP+ 10Gbit frontend 2x 1Gbit management port
Rozšiřitelnost pole	- pole v dodané konfiguraci musí být za provozu rozšiřitelné pomocí expanzních polic na nejméně 238SFF/108 LFF hot-plug disků - možnost kombinovat SSD, rotační SAS i rotační NL_SAS disky, bez omezení - SSD disky musí být konfigurovatelné jako datové nebo také v režimu minimálně read akcelerátoru (cache)	ANO	Maximální počet rozšiřujících polic je 9 Maximální počet disků 238 SFF / 108 LFF
Konstrukce	- HW provedení pole: - Max. 2U - v rámci 2U musí být k dispozici základní jednotka pole (2x řadiče a napájení) a základní osazení disky - Min. 24x 2,5" hot-plug diskových pozic v rámci základní jednotky - Redundantní napájení dimenzované pro plný počet disků a řadiče (základní jednotka) - Rackmount, včetně montážního kitu do	ANO	---

	standardního 19" racku.		
Počet a typ disků	Osazení hot-plug disky v poptávané konfiguraci - 8x 1,92TB SSD SAS 12Gbit/s 1DWPD, Hot Plug - 5x 12TB HDD SAS 12Git/s, HotPlug Poptávanou konfiguraci musí být možné kdykoli rozšířit o další disky SSD, SAS i NL_SAS (připouští se doplněním příslušných expanzních jednotek)	ANO	8x 1.92TB SAS RI SFF M2 SSD v základním boxu. 5x 12TB SAS 7.2K LFF M2 HDD v rozšiřujícím boxu
Podpora RAID	- JBOD - RAID 0,1, 5, 6, 10 - Možnost použít více typů RAID v rámci jednoho pole.	ANO	---
Funkcionalita	Software funkcionalita (licence bez omezení na počet serverů nebo kapacitu pole) - thin provisioning - hotsparing - standardní RAID skupiny a dedikované hotspare disky - automatický tiering (SSD, SAS a NL_SAS tier) - SSD cache - klony a snapshoty (512 ks) - vzdálené zrcadlení mezi dvěma nebo více poli (alespoň asynchronní) - úložiště musí podporovat správu pomocí GUI z webovského prohlížeče HTML5, - podpora pro VMware vCenter plugin pro správu úložiště prostřednictvím vCenter - podpora SNMP - podpora notifikací pomocí emailu, SNMP trap	ANO	---
Kompatibilita	Nabízená technologie diskového pole musí být kompatibilní s: - RedHat Linux - SuSe Linux - MS Windows 2022, 2019, 2016 - VMware ESX	ANO	---
Záruka	Záruka min. 5 let na kompletní HW, přístup k technické podpoře 24x7, NBD - Oprava v místě instalace - Servis je poskytován certifikovaným servisním partnerem případně přímo výrobcem	ANO	---

<u>Podrobný rozpad diskového pole</u>

1	R0Q82B	HPE MSA 2062 10GbE iSCSI SFF Storage
8	R0Q47A	HPE MSA 1.92TB SAS RI SFF M2 SSD
8	487655-B21	HPE BLc 10G SFP+ SFP+ 3m DAC Cable
1	R0Q39B	HPE MSA 2060 SAS 2U 12d LFF Drv Encl

5	R0Q61A	HPE MSA 12TB SAS 7.2K LFF M2 HDD
1	HU4B2A5	HPE 5Y Tech Care Basic SVC
1	HU4B2A5#ZQE	HPE MSA 2060 LFF Enclosure Support
1	HU4B2A5#ZQB	HPE MSA 2062 Support

BACKUP SERVER:

Požadavky na dodávané řešení		***Splňuje (ANO/NE)***	***Popis/ komentář***
(P54204-B21) 2x HPE DL345 Gen11 8LFF			
Parametr	Požadovaná hodnota		
Form Factor a vnitřní uspořádání	2U, varianta rack	ANO	2U
CPU	jednosocketový systém, osazený jedním procesorem s 16 core, musí mít minimálně 43500 bodů v testu CPU benchmark https://www.cpubenchmark.net/ Z licenčních důvodů musí být počet 16core dodržen.	ANO	AMD EPYC 9124 Benchmark 43.680
RAM	min. 12 slotů, podpora pamětí typu DDR5 4800MT/s RDIMM s minimální celkovou kapacitou 3TB. Požadujeme osadit 2x64GB	ANO	2x 64GB
Diskový subsystém	Požadujeme diskový subsystém pro klasické disky LFF, minimálně 14 slotů. Osazení min 14x 12TB SAS HDD Pro start OS požadujeme diskový prostor v RAID1 o velikosti min 480GB	ANO	14x 12TB SAS RAID1 480GB
Diskový řadič	PCIe 3.0 12Gb/s SAS Raid řadič s RAID 0/1/10/5/50/6/60/ s 4GB battery backed write cache (onboard nebo osazený v PCI Express slotu). Diskový řadič musí podporovat Secure encryption/data at rest Encryption	ANO	HPE MR416i-p Gen11 Storage Cntlr
Interface	- min. 3x externí USB, z toho min. 1x USB 3.0 - dedikovaný USB management port - min. 1x VGA port	ANO	- 3x externí USB, z toho 1x USB 3.0 - dedikovaný USB management port - 1x VGA port
Napájecí zdroje	Dva napájecí zdroje; min. 1000W, účinnost min. 96%	ANO	1.000W Účinnost 96%
Síťové porty	Požadujeme - 1 port 1Gbit RJ-45 pro management - 2 porty 10Gbit SFP+	ANO	---
Kompatibilita	- Canonical® Ubuntu® Server LTS - Microsoft® Windows Server® with Hyper-V - Red Hat® Enterprise Linux - VMware® ESXi®	ANO	---
Management	- Server musí disponovat	ANO	---

a vzdálená správa	vyhrazeným Gb portem pro vzdálený management, port musí mít k dispozici úložiště pro firmware, ovladače a další sw komponenty. Úložiště musí být konfigurovatelné pro vytváření instalačních sad s možností rollback/patch při pádu aktualizace. - Server musí podporovat bez agentový vzdálený management. Vzdálený management musí podporovat standardní webové prohlížeče pro grafickou vzdálenou konzoli spolu s tlačítkem pro Virtual Power a podporovat vzdálený boot z DVD/CD/USB zařízení a být schopen uchovávat historická data o sw upgradech a patchích. - Musí být podporována vícefaktorová autentikace. - Musí být monitorovány změny v hw a systémové konfiguraci, musí být podporována rychlá diagnostika vzniklých problémů. - Pro vzdálenou správu musí být podporována mobilní zařízení Android a Apple OS. Vzdálená konzola musí umožnit současný přístup až 6 uživatelům během pre-OS a OS runtime operací, musí existovat schopnost uchovat video z poslední zásadní poruchy a posledního bootovacího procesu, musí být podporována MS TS integrace včetně 128 bitové SSL enkrypce a Secure Shell Version 2, musí být podporovány AES a 3DES na prohlížeči a vzdálený firmware update a JAVA free pro vzdálenou konzoli. - Musí být podporována současná podpora většího množství serverů, a to v následujících komponentách: Power Control, Power Caping, Firmware Update, konfigurace, Virtual Media, Licence Activation. - Musí být podporována RESTFullAPI integrace a předávání hw událostí přímo na výrobce serveru.		

Podpora a servis	- podpora na 5let, servisní zásah následující pracovní den - oprava v místě instalace serveru - servis je poskytován výrobcem serveru - zdarma aktualizace firmware min. po dobu platné podpory - možnost automatického generování servisního incidentu přímo u výrobce hardware.	ANO	---

Podrobný rozpad serveru

1	P54204-B21	HPE DL345 Gen11 8LFF CTO Svr
1	P53702-B21	AMD EPYC 9124 CPU for HPE
2	P50312-B21	HPE 64GB 2Rx4 PC5-4800B-R Smart Kit
1	P57112-B21	HPE DL345 Gen11 4LFF x1 SAS/SATA Mid Kit
1	P57114-B21	HPE DL345 Gen11 12LFF Upgrade BP Kit
14	881781-B21	HPE 12TB SAS 7.2K LFF LP He 512e HDD
1	P47777-B21	HPE MR416i-p Gen11 SPDM Storage Cntlr
1	P01366-B21	HPE 96W Smart Stg Li-ion Batt 145mm Kit
1	P26256-B21	BCM 57412 10GbE 2p SFP+ OCP3 Adptr
2	P03178-B21	HPE 1000W FS Ti Ht Plg PS Kit
1	BD505A	HPE iLO Adv 1-svr Lic 3yr Support
1	S1A05A	HPE Cmp Cloud Mgmt Srv FIO Enablement
1	P59254-B21	HPE DL345 G11 8LFF SAS/SATA Prim Cbl Kit
6	P58465-B21	HPE DL3X5 Gen11 2U Perf Fan Kit
1	P50400-B21	HPE DL3XX Gen11 2U Com Bezel Kit
1	P48183-B21	HPE NS204i-u Gen11 Ht Plg Boot Opt Dev
1	P52351-B21	HPE DL3XX Gen11 Easy Install Rail 2 Kit
1	P57013-B21	HPE DL3X5 G11 NS204i-u NVMe Boot Cbl Kit
1	P58457-B21	HPE DL3XX Gen11 Perf 1U Heat Sink Kit
1	R7A12AAE	HPE COM Enh 5yr Up ProLiant SaaS
1	HU4B2A5	HPE 5Y Tech Care Basic SVC
1	HU4B2A5#R2M	HPE iLO Advanced Non Blade Support
1	HU4B2A500DF	HPE ProLiant DL345 Gen11 Support

LICENCE PRO KYBEZ INFRASTRUKTURU:

Pro provoz stávajících aplikací a informačních systémů požadujeme dodávku těchto trvalých licencí:

Požadavky na dodávané řešení/licence	***Počet***	***Popis/ komentář***
Serverový operační systém s licencí pro neomezený počet virtuálních strojů, určený pro podnikové aplikace a nasazení v datových centrech. Požadována je nejnovější dostupná verze s aktuálními bezpečnostními aktualizacemi. Řešení musí podporovat pokročilé virtualizační technologie kompatibilní se současným řešením zadavatele. Serverový OS musí: - být kompatibilní s širokou škálou podnikových aplikací pro samosprávu - poskytovat virtualizaci	2ks	Win Server DataCenter Core 2025 16L

- poskytovat správu adresářových služeb MS Active Directory, které jsou aktuálně využívány zadavatelem - zajistit provoz v režimu plnohodnotného řadiče domény adresářových služeb provozovaných Zadavatelem		
Serverový operační systém s licencí pro základní virtualizaci, vhodný pro zálohovací servery. Požadována je nejnovější dostupná verze s aktuálními bezpečnostními aktualizacemi. Serverový OS musí poskytovat kompatibilní prostředí pro provoz management nástroje pro správu nástroje zálohování.	1ks	Win Server Standard Core 2025 16L
Uživatelská přístupová licence pro dodávaný serverový operační systém, která umožňuje uživateli přístup ke službám a funkcím serveru. Požadována je nejnovější dostupná verze.	100ks	Win Server CAL 2025 UCAL
Licence pro vzdálený přístup uživatele k serverovému operačnímu systému pomocí služeb terminálového serveru, která umožňuje přístup z libovolného zařízení. Požadována je nejnovější dostupná verze.	10 ks	Win Remote Desktop Services CAL 2025 UCAL

POŘÍZENÍ KRYPTOGRAFICKÉHO SYSTÉMU ZAJIŠŤUJÍCÍHO OCHRANU INFORMACÍ MEZI DATOVÝMI CENTRY A UŽIVATELSKÝMI PRACOVNÍMI STANICEMI

Požadavky na dodávané řešení	***Splňuje***	***Popis / komentář***
(FWB-VM01) FortiWeb VM01, virtual apliance	***(ANO/NE)***	
Virtuální appliance pro platformu minimálně pro nabízený hypervizor, dále pak VMWARE ESX, Microsoft Hyper-V, KVM	ANO	---
Propustnost minimálně 25Mbit	ANO	25Mbps
Podpora minimálně 10 virtuálních síťových rozhraní	ANO	10
Topologie nasazení:		
Reverzní proxy	ANO	---
Transparentní proxy	ANO	---
Ochrana webového protokolu:		
AI-based Machine Learning	ANO	(dvojúrovňová detekce anomálií a hrozeb za pomoci databáze vzorků výrobce a za pomoci strojového učení (machine learning)
Automatic profiling (white list)	ANO	---
Web server and application signatures (black list)	ANO	---
IP address reputation	ANO	---
IP address geolocation	ANO	---
HTTP RFC compliance	ANO	---
Native support for HTTP/2	ANO	---
WebSocket protection and signature enforcement	ANO	---
Man in the Browser (MiTB) protection	ANO	---
Ochrana aplikací:		
Ochrana/kontrola dle OWASP Top 10	ANO	---
ochrana před Cross Site Scripting	ANO	---
ochrana před SQL Injection	ANO	---
ochrana Cross Site Request Forgery	ANO	---

ochrana před Session Hijacking	ANO	---
vestavěný Vulnerability Scanner	ANO	---
Kontrola nahrávaných souborů vestavěným AV skenerem a pomocí sandboxu.	ANO	---
Bezpečnostní funkce:		
Rozpoznávání aplikací dle signatur	ANO	---
Kontrola shody XML and JSON protokolů se standardem	ANO	---
Detekce Malware	ANO	---
Oprava chybných webových požadavků za běhu (Virtual patching)	ANO	---
Validace síťových a aplikačních protokolů	ANO	---
Ochrana před útoky hrubou silou	ANO	---
Cookie signing and encryption	ANO	---
Syntax-based SQLi detection	ANO	---
Ochrana HTTP hlaviček	ANO	---
Custom error message and error code handling	ANO	---
Ochrana OS rozpoznáváním signatur ohrožení	ANO	---
Ochrana před známými útoky a 0-day útoky	ANO	---
L4 Stateful Network Firewall	ANO	---
Prevence DoS	ANO	---
Rozšířená ochrana korelací více bezpečnostních prvků	ANO	---
Ochrana před únikem dat	ANO	---
Podpora Web aplikací:		
Layer 7 server load balancing	ANO	---
URL Rewriting	ANO	---
Content Routing	ANO	---
HTTPS/SSL Offloading	ANO	---
HTTP Compression	ANO	---
Caching	ANO	---
Podpora autentikace:		
Aktivní a pasivní autentikace web aplikací	ANO	---
Site Publishing and SSO	ANO	---
RSA Access for 2-factor authentication	ANO	---
LDAP, RADIUS, and SAML support	ANO	---
SSL client certificate support	ANO	---
CAPTCHA and Real Browser Enforcement (RBE)	ANO	---
Včetně technologie umožňující realizovat 2-factor přihlášení do publikovaných aplikací, a to pomocí zasílání druhého faktoru na mobilní aplikaci, sms přes sms bránu (sms brána není součástí), kódu do mailu. A to v libovolné kombinaci.	ANO	---
Podpora výrobce v režimu 24x7 pro platformu i její provozní konfiguraci včetně politik na 5 let	ANO	---

Požadavky na dodávané řešení	***Splňuje***	***Popis /***
(FAC-VM-Base) FortiAuthenticator, Virtual Appliance	***(ANO/NE)***	***komentář***
Virtuální appliance pro platformu minimálně pro nabízený hypervizor,	ANO	---

dále pak VMWARE ESX, Microsoft Hyper-V, KVM		
centrální autentizační server s podporou 2FA	ANO	---
Možnost alokovat nejméně 48 virtuálních jader CPU	ANO	Až 64 jader
Počet virtuálních síťových karet – nejméně 4 vNICs	ANO	4 vNIC
alokace virtuálního vnitřního uložiště – nejméně 15 TB	ANO	16TB
alokace virtuální paměť RAM až 1TB	ANO	1TB
Podpora vysoké dostupnosti v režimu Active-Passive, Active-Active	ANO	---
management identit, plnohodnotná AAA funkcionalita, integrované funkce AAA pro připojení z VPN	ANO	---
Podpora nabízených funkcí pro minimálně 90 uživatelů	ANO	100
Možnost automaticky synchronizovat uživatele z Active Directory	ANO	---
Možnost používat bezpečnostní politiky založené na identitách a rolích bez nutnosti dalšího ověřování díky integraci s Active Directory	ANO	---
Možnost vytvářet lokální uživatele a skupiny	ANO	---
Minimální počet uživatelských skupin 8	ANO	10 skupin
Podpora 2FA pomocí tokenů (aplikace pro iOS a Android, HW token)	ANO	---
Podpora 2FA minimálně pro 180 tokenů	ANO	200 tokenů
Podpora 2FA pomocí SMS a emailu	ANO	---
Podpora ověřováni ze sociálních sítí (facebook, linkedin)	ANO	---
Možnost definovat zařízení na základě MAC adresy	ANO	---
Funkce LDAP/LDAPS serveru	ANO	---
Možnost automatického importu identit ze vzdálených LDAP serverů	ANO	---
Funkce TACACS+ serveru	ANO	---
Funkce Radius serveru	ANO	---
Podpora standardu IEEE802.1X pro zabezpečení kabelových a bezdrátových sítí	ANO	---
Podpora radius accountning v proxy režimu	ANO	---
Funkce SAML IdP	ANO	---
Možnost napojení a ověřování z externího Radius, LDAP SAML a OAuth server	ANO	---
Podpora SSO autentizace uživatelů v prostředí domény MS Windows	ANO	---
Podpora Kerberos	ANO	---
podpora EAP metod EAP-MSCHAPv2, EAP-TLS, PEAP, EAP-GTC	ANO	---
Funkce certifikační autority	ANO	---
Podpora minimálně 5 certifikátů CA	ANO	5
Podpora minimálně 300 uživatelských certifikátů	ANO	Až 500
Podpora SCEP a CRL	ANO	---
Podpora captive portálu	ANO	---
Podpora samoobslužných portálů (reset hesla, editace uživatelských údajů, přidělení tokenů)	ANO	---
Podpora 2FA pro Outlook Web Access pomocí nativního klienta	ANO	---
Podpora mechanismu 2FA pro koncové stanice a přihlášení do systému Windows	ANO	---
Podpora FIDO 2 funkcionality, pro ověřování bez hesla	ANO	---
Podpora push notifikací pro 2FA a mobilní aplikaci	ANO	---
Podpora REST API (pokud tato funkce vyžaduje licenci, tak musí být součástí dodávky)	ANO	---
Podpora použití vícefaktorového klientského ověření k přístupu k SSL a IPSec VPN pomocí bezpečnostní brány od stejného výrobce	ANO	---
Možnost definice Captive Portalu k bezdrátovému přístupu	ANO	---

Podpora výrobce v režimu 24x7 pro platformu i její provozní konfiguraci včetně politik na 5 let	ANO	---

20 ks licencí tokenů pro ověření druhým faktorem pro přístup přes VPN

Požadavky na dodávané řešení	***Splňuje (ANO/NE)***	***Popis/ komentář***
(FTM-ELIC-25) FortiToken Software License Key		
Generátor OTP založený na čase a události OATH	ANO	---
Možnost schválení ověření jednou interakcí z mobilního zařízení	ANO	---
Kompatibilita s operačními systémy iOS, Android, Windows	ANO	---
Možnost využít Firewall jako 2FA server	ANO	---
Trvalá licence bez ročních poplatků	ANO	---
Licence minimálně pro 20 uživatelů	ANO	25
Možnost neomezených přenosů zařízení	ANO	---
Podpora a administrace tokenů v centrálním autentizačním serveru od stejného výrobce	ANO	---
Podpora výrobce v režimu 24x7 pro platformu i její provozní konfiguraci včetně politik na 5 let	ANO	---

DROBNÝ MATERIÁL A PROPOJOVACÍ PRVKY:

Požadujeme dodávku propojovacích prvků, kabelů a drobného instalačního materiálu tak, aby vzniklo kompletní, funkční a se stávajícím prostředím propojené dílo. Jedná se především o QSFP+/QSFP28/SFP28/SFP+ DAC kabely pro propojení switchů s firewally a se servery a diskovým polem. A další potřebné metalické a optické kabely.

IMPLEMENTAČNÍ PRÁCE:

1. Nástroj (licence) pro zálohování a archivaci
   - registrace nových licencí
   - úpravy a nastavení nových zálohovacích jobů
   - ověření záloh a testovací obnovy
   - Upravit existující Backup plan + Plán obnovy dle skutečného stavu
2. Zabezpečení sítě pomocí 802.1x
   - Vytvoření segmentu pro zálohování, readresace zálohovacích zařízení, serverů, nastavení přístupu a bezpečnostních politik do tohoto segmentu
   - Readresace koncových zařízení – tiskárny, uživatelské stanice, AV technika, IP kamery atd.
   - Vytvoření definovaných segmentů a bezpečnostních politik pro komunikaci mezi nimi
   - Vytvoření serverového segmentu bez readresace serverů
   - Příprava DMZ segmentu a nastavení komunikačních politik
   - Úprava wifi sítí dle prováděcího dokumentu (redukce stávajících)
   - Dokumentace cílového stavu
3. Firewall
   - Fyzická montáž zařízení a propojení se stávajícími switchi

- konfigurace HA režimu
- analýza, úprava a nastavení politik tak aby byly ve shodě s aktuálními best practice a jejich přenesení na nové firewally
- Přenesení management konfigurace stávajících switchů pod nové firewally

4. WIFI AP

- Fyzická montáž, náhrada stávajících Wifi AP v současných pozicích
- Konfigurace centrální správy, aktualizace firmware AP
- Vytvoření požadovaných sítí a jejich přiřazení do odpovídajících segmentů

5. Nástroj pro analýzu a monitoring síťového provozu

- Instalace virtuální appliance do virtualizačního prostředí
- registrace potřebných licencí
- připojení zdrojů dat – minimálně firewally, switche, nástroj pro řízení přístupu do sítě 802.1x, ochrana publikovaných aplikací
- Tvorba a úprava pohledů na nejfrekventovanější dotazy

6. Nástroj pro log management

- Instalace logovacího systému do virtuálního prostředí
- Instalace log agentů na zdrojové zařízení
- Připojení všech potřebných zdrojů logů
- Nastavení normalizace logů
- Nastavení Dashboardů

7. Služby SOC

- Implementace služby SOC do provozního prostředí Zadavatele

8. Nástroj pro řízení přístupu k privilegovaným účtům

- Dodávka a instalace komponent systému
- Integrace s Active Directory (LDAP) a Email serverem Zadavatele
- Nastavení dvoufaktorové autentizace
- Nastavení politik, workflow, pro PIM/PAM (Nastavení skupin a oprávnění uživatelů a administrátorů PAM, nastavení a přiřazení přístupových politik skupinám uživatelů, nastavení politik hesel podle skupin zařízení).
- Nastavení nahrávání privilegovaných relací, základní popis práce s relacemi, reporty a další.
- Návrh zálohování a obnovy (popisem nastavení pravidelného zálohování a obnovou řešení ze záloh).
- Integrace se systémy provozovaných Zadavatelem:
  - RDP protokol pro Windows platformu
  - SSH protokol pro OS Linux/Unix platformu
  - Vytvoření účtů pro kmenové zaměstnance Zadavatele a přiřazení oprávnění k příslušným serverům.
  - Vytvoření účtů pro externí pracovníky a přiřazení oprávnění k příslušným serverům.
  - Řízený přístup na webové aplikace Zadavatele, například správa Snap-in MS AD, správa webových konzolí hypervizorů, nebo management konzolí bezpečnostních systémů – FW, switche, AV systém.

9. Servery pro Kybez, Diskové pole pro Kybez, Backup servery pro Kybez, Licence pro Kybez infra

- Fyzická montáž zařízení do rozvaděčů
- Propojení se LAN prvky
- Aktualizace firmware
- Instalace virtualizační vrstvy
- Konfigurace diskového pole
- Vytvoření šablony OS
- Přenesení stávajícího backup serveru na nový backup server
- Vytvoření hardened repozitory na druhém hw backup serveru
- Úprava zálohovacích jobů
- Migrace VM ze stávající infra na novou, aktualizace integračních komponent
- Instalace AD DC na poslední vhodné verzi OS Windows Server
- Migrace AD, odstranění původních DC, rozšíření schématu,
- Příprava šablony pro vytváření VM
- Instalace nového File serveru, migrace dat, sdílení a oprávnění
- Instalace nového Terminal serveru
- Vytvoření VM pro další aplikace, součinnost se třetími stranami
- Ochrana publikovaných aplikací včetně podpory pro dvoufaktorovou autentizaci
- Instalace virtuální appliance
- Registrace licencí
- Analýza publikovaných aplikací, návrh konfigurace webového filtru, případné zavedení druhého faktoru
- Ověření funkce, komunikace s dodavateli aplikací
- Součástí dodávky je veškerá potřebná kabeláž pro plné zapojení všech portů do instalovaného prostředí a potřebná napájecí kabeláž kompatibilní s napájecími lištami v RACK skříních.

10. Ochrana publikovaných aplikací včetně podpory pro dvoufaktorovou autentizaci

    - Instalace virtuální appliance
    - Registrace licencí
    - Analýza publikovaných aplikací, návrh konfigurace webového filtru, případné zavedení druhého faktoru
    - Ověření funkce, komunikace s dodavateli aplikací

11. Obecné:

    - Každá kapitola bude doplněna dokumentací o skutečném provedení
    - Bude provedeno zaškolení k nově nasazovaným technologiím

AKCEPTAČNÍ KRITÉRIA:

- Zařízení (Firewaly, switche) jsou namontována v místech určení a propojeny se sítí LAN
- Veškeré Licence jsou aktivovány, přiřazeny na portále výrobce pod účtem zadavatele, délka podpory koresponduje se smlouvou
- Switche a AP jsou připojeny do management nástroje, lze z nich vyčíst provozní údaje a konfigurace.
- Firewally jsou v funkčním HA clusteru.
- Firewally mají zabezpečeny přístupy administrátorů, jsou nastavena bezpečná hesla.
- Firewally mají zapnuté předávání logů do Centrálního úložiště logů a do Analyzátoru síťového provozu.
- Switche jsou v režimu „bezkonfiguračních portů“, probíhá automatické přiřazení VLAN k portu podle připojeného zařízení.
- WIFI AP jsou osazeny, sítě dle dokumentu jsou k dispozici a vedou do správných segmentů.
- SOC – Všechny relevantní posílají své logy do SOC sondy k analýze
- SOC – Simulovaný incident vyvolá odpovídající reakci SOC týmu
- Zařízení bez možnosti suplikanta jsou identifikována a zapojena do systému 802.1x vhodným způsobem (identifikace profilem/MAC adresou a podobně)
- Virtualizační infrastruktura je implementovaná, všechny VM z původního prostředí jsou přesunuty na novou infra, původní je odstavená.
- Při přístupu do VPN je vyžadován druhý faktor pomocí mobilní aplikace
- Publikované aplikace jsou dostupné přes webový filtr, autentizace pomocí druhého faktoru je zapnutá. (pokud dává smysl)
- Logy se shromažďují v centrálním úložišti logů a lze nad nimi vyhledávat a filtrovat je předdefinovanými pohledy.
- Zálohování funguje, jsou zálohovány všechny požadované VM, je ověřená obnova vybrané testovací VM.
- Přístup k privilegovaným účtům je pouze přes nástroj pro jejich správu, k zařízení se nelze přímo přihlásit.
- Předaná dokumentace odpovídá skutečnosti

Předpokládaná součinnost ze strany zadavatele

- Přístup do prostoru zadavatele
- Součinnost správců IT technologií včetně přístupových údajů k dotčeným systémům (servisní účty apod.)
- Poskytnutí dokumentace stávajícího stavu provozu
- Poskytnutí prováděcího dokumentu segmentace sítě LAN (vázáno na podpis NDA)
- Vzdálený přístup pro specialisty – VPN, privilegované účty pro potřebu implementace
- Poskytnutí kontaktů a vytvoření komunikační matice
- Návrh termínů pro systémové odstávky bez zbytečného prodlení

POŽADAVKY NA ZÁRUKY

Zadavatel požaduje záruku na veškeré dodané HW technologie v délce trvání **60 měsíců** od okamžiku předání díla, není-li u konkrétního zařízení či komponenty požadováno jinak v technické specifikaci. Pokrývá-li standardní záruka výrobce/poskytovatele zařízení či komponenty celé období 60 měsíců, bude cena záruky zahrnuta v ceně za dodávku a implementaci plnění. Pokrývá-li standardní záruka výrobce/poskytovatele zařízení či komponenty období kratší než 60 měsíců, pak bude cena za zajištění nadstandardní (prodloužené) záruky do požadované délky trvání vyjádřena samostatně. Obdobně platí pro poskytování těch služeb, které svým obsahem či rozsahem případně přesahují režim poskytování služeb v rámci běžné standardní záruky.

Veškeré záruční opravy / výměny po dobu záruky budou provedeny bez dalších nákladů pro zadavatele bezplatně.

Digitálně podepsal
Mgr. Lukáš Jurča
Datum: 2025.05.08
19:03:15 +02'00'