Spisová značka: S-MI6387/2025 Obsah obrázku Písmo, text, snímek obrazovky, Elektricky modrá

Popis byl vytvořen automatickyObsah obrázku Písmo, text, Grafika, symbol

Popis byl vytvořen automaticky

Registrační číslo projektu: **CZ.31.2.0/0.0/0.0/23\_093/0009398**

**Příloha č. 2 Zadávací dokumentace**

**Specifikace předmětu plnění „Kybernetická bezpečnost Ivančice“**

Obsah:

[1. Předmět veřejné zakázky 2](#_Toc201671903)

[2. Obecné požadavky 2](#_Toc201671904)

[3. Specifikace požadavků řešení – 1. Část 2](#_Toc201671905)

[3.1. Pokročilý NGFW firewall v režimu HA (ID1) 3](#_Toc201671906)

[3.2. Více-faktorová autentizace a Single Sign-On (SSO) – pro 160 uživatelů (ID2) 4](#_Toc201671907)

[3.3. Ochrana před škodlivým kódem (ID3) a Nástroj pro detekci kybernetických bezpečnostních událostí (ID4) 6](#_Toc201671908)

[3.4. Nástroj pro sběr a nepřetržité vyhodnocení kybernetických bezpečnostních událostí – SIEM (Security Information and Event Management) (ID5) 15](#_Toc201671909)

[3.5. Implementace 24](#_Toc201671910)

[4. Specifikace požadavků řešení – 2. Část 25](#_Toc201671911)

[4.1. Server OS datacenter a CAL 160ks, Terminal server a CAL 40 ks. (ID2) 25](#_Toc201671912)

[4.2. Databázový server SQL licence na 4 core (ID2) 25](#_Toc201671913)

[4.3. Zálohovací SW pro 25 virtuálních serverů (ID6) 26](#_Toc201671914)

[4.4. Diskové pole (ID6) 26](#_Toc201671915)

[4.5. Síťové úložiště NAS (ID6) 29](#_Toc201671916)

[4.6. Implementace 31](#_Toc201671917)

[5. Specifikace požadavků řešení – 3. Část 31](#_Toc201671918)

[5.1. Hasicí systém pro serverovnu (ID6) 32](#_Toc201671919)

[5.2. Implementace 32](#_Toc201671920)

[6. Požadavky na servisní podporu provozu a SLA 33](#_Toc201671921)

[7. Podmínky předání a převzetí – akceptace 33](#_Toc201671922)

[8. Harmonogram plnění 33](#_Toc201671923)

[9. Seznam zkratek 33](#_Toc201671924)

Seznam tabulek:

[Tabulka 1: Pokročilý NGFW firewall v režimu HA (ID1) 3](#_Toc201671925)

[Tabulka 2: Více-faktorová autentizace a Single Sign-On (SSO) – pro 160 uživatelů (ID2) 4](#_Toc201671926)

[Tabulka 3: Základní vlastnosti 6](#_Toc201671927)

[Tabulka 4: Konzole pro centrální správu řešení 7](#_Toc201671928)

[Tabulka 5: Vlastnosti a funkce ochrany fyzických koncových bodů 9](#_Toc201671929)

[Tabulka 6: Ochrana virtualizovaných koncových bodů 12](#_Toc201671930)

[Tabulka 7: Rozšířená funkce XDR 14](#_Toc201671931)

[Tabulka 8: Nástroj pro sběr a nepřetržité vyhodnocení kybernetických bezpečnostních událostí – SIEM (Security Information and Event Management) (ID5) 15](#_Toc201671932)

[Tabulka 9: Požadavky – Implementace nabízeného řešení 24](#_Toc201671933)

[Tabulka 10: Server OS datacenter a CAL 160ks, Terminal server a CAL 40 ks. (ID2) 25](#_Toc201671934)

[Tabulka 11: Databázový server SQL licence na 4 core (ID2) 25](#_Toc201671935)

[Tabulka 12: Zálohovací SW Veeam 25 virtuálních serverů (ID6) 26](#_Toc201671936)

[Tabulka 13: Diskové pole (ID6) 26](#_Toc201671937)

[Tabulka 14: Síťové úložiště NAS (ID6) 29](#_Toc201671938)

[Tabulka 15: Požadavky – Implementace nabízeného řešení 31](#_Toc201671939)

[Tabulka 16: Hasicí systém pro serverovnu (ID6) 32](#_Toc201671940)

[Tabulka 17: Požadavky – Implementace nabízeného řešení 32](#_Toc201671941)

# Předmět veřejné zakázky

Předmětem této veřejné zakázky je dodávka a implementace:

1. **část: Posílení KB**
2. Pokročilý NGFW firewall v režimu HA (ID1)
3. Více-faktorová autentizace a Single Sign-On (SSO) – pro 160 uživatelů (ID2)
4. Ochrana před škodlivým kódem (ID3) a Nástroj pro detekci kybernetických bezpečnostních událostí. (ID4)
5. Nástroj pro sběr a nepřetržité vyhodnocení kybernetických bezpečnostních událostí – SIEM (Security Information and Event Management) (ID5)
6. **část: HW a SW**
   1. Server OS datacenter a CAL 160ks, Terminal server a CAL 40 ks. (ID2)
   2. Databázový server SQL licence na 4 core (ID2)
   3. Zálohovací SW pro 25 virtuálních serverů (ID6)
   4. Diskové pole (ID6)
   5. Síťové úložiště NAS (ID6)
7. **část: Hasicí systém pro serverovnu (ID6)**

Včetně zajištění servisní podpory provozu předmětu veřejné zakázky po dobu 60 měsíců od předání předmětu veřejné zakázky.

# Obecné požadavky

Zadavatel požaduje, aby předmět plnění veřejné zakázky (veškeré dodané zboží) měl garantovanou plnou podporu a záruku výrobce. Za účelem prokázání tohoto požadavku předloží dodavatel k nabídce potvrzení výrobce, resp. jeho lokálního zastoupení, nebo jiný rovnocenný doklad ve smyslu § 45 odst. 2 ZZVZ, ze kterého bude jednoznačně vyplývat, že nabízené zboží disponuje plnou podporou a zárukou ze strany výrobce.

Zadavatel požaduje, aby byl předmět plnění veřejné zakázky (veškeré dodané zboží) nový a nepoužitý. Dodavatel tuto skutečnost prokáže nejpozději v rámci součinnosti před podpisem smlouvy ve smyslu § 122 ZZVZ předložením například potvrzení výrobce, oficiálního zastoupení výrobce nebo jiným dokladem ve smyslu § 45 odst. 2 ZZVZ, ze kterého bude jednoznačně vyplývat splnění tohoto požadavku zadavatele.

Je-li v zadávací dokumentaci stanoven požadavek na předložení datasheetu je tím myšleno produktový list vydaný samotným výrobcem zařízení nebo výrobcem předmětné technické komponenty, veřejně dostupný, především internetovým odkazem na www stránkách vlastního výrobce, produktový list či dokument, nejen s přehledovou, ale především podrobnou technickou specifikací vlastností výrobku, v časově aktuální verzi platné pro nabízený model zařízení a region jeho použití a dodání.

Je-li součástí produktů SW či FW, pak se musí jednat o verze, které jsou standardní, běžně dostupné a určené k produkčnímu použití. Není dovoleno použití beta verzí, neoficiálních verzí, ani SW/FW se zákaznickými úpravami.

Nabízený předmět veřejné zakázky, včetně všech interních komponent, musí být pokryt oficiální technickou podporou výrobce tak, aby v případě závady, kterou není dodavatel schopen odstranit, mohl zadavatel tuto závadu eskalovat přímo k technické podpoře výrobce. Servisní zásahy budou prováděny vždy v místě instalace předmětu veřejné zakázky.

Veškeré požadované funkce, vlastnosti, certifikace i výsledky testů, musí být dostupné nejpozději dnem podání nabídky.

# Specifikace požadavků řešení – 1. Část

V následujících podkapitolách je uvedena specifikace parametrů řešení nutných pro plnění této veřejné zakázky.

V době posuzování nabídek musí nabídka řešení účastníka dále splňovat níže specifikované požadavky.

Účastník nakopíruje do nabídky následující tabulku a popis splnění požadavků ve sloupci **„Účastníkem nabízená hodnota, výrobce a typ.“**, tak že tam nakopíruje text ze sloupce „Specifikace požadavků“ a **doplní výrobce a typ**, případně doplní nebo upraví popis nabízené hodnoty, ze kterého bude patrné, že splňuje požadavky.

Sloupec „Specifikace požadavků“ nesmí být účastníkem nijak měněn a účastník je oprávněn vyplnit pouze sloupec „Účastníkem nabízená hodnota, výrobce a typ.“.

Sloupec **„Splněno [ano/ne]“** účastník nevyplňuje, slouží pro zadavatele.

## Pokročilý NGFW firewall v režimu HA (ID1)

Tabulka 1: Pokročilý NGFW firewall v režimu HA (ID1)

|  |  |  |  |
| --- | --- | --- | --- |
| **č.** | **Specifikace požadavků.** | **Účastníkem nabízená hodnota, výrobce a typ.** | **Splněno [ano/ne]** |
| **Základní technické požadavky** | | | |
|  | 2x HW appliance o velikosti 1 RU v režimu vysoké dostupnosti (musí podporovat oba způsoby zapojení active-active i active-passive). |  |  |
|  | Grafické konfigurační rozhraní a příkazový řádek. |  |  |
|  | Min. 12 metalických RJ-45 portů 10/100/1000. |  |  |
|  | Min. 4 optická datová rozhraní SFP+ o rychlosti 10Gb/s. |  |  |
|  | Min. 4 optická datová rozhraní SFP o rychlosti 1Gb/s. |  |  |
|  | 1 dedikovaný port pro správu pomocí konzole pro přístup k CLI a 1 management port. |  |  |
|  | NGFW musí podporovat plnohodnotnou inspekci sítového provozu v režimech:  • NAT/router;  • L2 transparentní režim (dva a více sítových rozhraní);  • L2 interface pair (dvě sítové rozhraní). |  |  |
|  | Redundantní napájení firewallu. |  |  |
| **Výkonové požadavky** | | | |
|  | Minimální požadovaná propustnost stavového firewallu pro IPv4 i IPv6 provoz 35 Gbps (UDP pakety o velikosti 512 B). |  |  |
|  | Nízké vložené zpoždění zařízení (latence) max. 5μs. |  |  |
|  | Minimální počet současně navázaných spojení firewallu 2.5 M. |  |  |
|  | Minimální počet nových spojení za sekundu 120 k. |  |  |
|  | Propustnost firewallu v packetech min. 40 Mpps. |  |  |
|  | Propustnost NGFW (kombinace stavového firewall, IPS, rozpoznávání aplikací na L7, logování) minimálně 3 Gbps. |  |  |
|  | Propustnost ochrany proti hrozbám a škodlivému kódu (kombinace stavového firewall, IPS, rozpoznávání aplikací na L7, ochrana proti škodlivému kódu, logování) min. 2.5 Gbps. |  |  |
|  | Propustnost ochrany proti hrozbám (IPS, ochrana proti sítovým útokům, logování) min. 5 Gbps. |  |  |
|  | Propustnost funkce rozpoznávání sítových aplikací na L7 min. 5 Gbps. |  |  |
|  | Propustnost IPSEC VPN v konfiguraci AES256/SHA256 min. 30 Gbps. |  |  |
|  | Propustnost funkce SSL inspekce provozu min. 2.7 Gbps. |  |  |
|  | Min. počet konfigurovatelných virtuálních kontextů na každém zařízení 10. |  |  |
| **Funkční požadavky** | | | |
|  | Funkce rozpoznávání kancelářských aplikací na L7 – aplikační vrstvě, podpora alespoň 3000 kancelářských aplikací, protokolů či příkazů; jednotlivé aplikace/protokoly uspořádány do kategorií; výrobce automaticky udržuje a aktualizuje databázi podporovaných aplikací. |  |  |
|  | Funkce ochrany před sítovými útoky vycházející z výrobcem udržované a aktualizované databáze, ochrana před útoky typu DoS, verifikace protokolů, min. 10 000 signatur v databázi; podpora zabezpečení kancelářských (IT). |  |  |
|  | Ochrana před výskytem škodlivého kódu v síťovém provozu (antivirus/antimalware) s podporou zabezpečení kancelářských (IT) a škodlivého kódu pro mobilní zařízení; podpora funkce sanitarizace dokumentů (odstranění aktivního obsahu) a předání zkoumaných souborů pro analýzu v prostředí typu sandbox. |  |  |
|  | Funkce kategorizace webových stránek (web filtering) s podporou minimálně 60 kategorií (pracovní zájmy, osobní zájmy, stránky se škodlivým kódem, nově registrované domény atp.), podpora definice časové kvóty, kterou nesmí daný uživatel na dané kategorii za den překročit, výrobcem aktualizovaná a udržovaná databáze. |  |  |
|  | Funkce SSL inspekce pro kontrolu protokolů s možností vytváření výjimek |  |  |
|  | Výjimka z SSL inspekce na základě administrátorem definovaných adres |  |  |
|  | Výjimka z SSL inspekce na základě kategorie URL, brané z URL filtrační databáze (např. kategorie bankovnictví, zdravotnictví atd.) |  |  |
|  | Ověřování identity uživatelů (možnost napojení na MS Active Directory, LDAP, Radius, Kerberos), práce s identitou uživatele v bezpečnostní politice firewallu v režimu tzv. Single Sign-On. |  |  |
|  | Funkce dynamického routingu (min. BGP, OSPF, RIP), pokud jsou tyto funkce licencované, tak licence musí být součástí dodávky. |  |  |
|  | Funkce QoS, traffic shaping. |  |  |
|  | Funkce klientské VPN (přístup do VPN v tunelovém režimu s VPN klientem a přístup do VPN přes webový portál, možnost aplikace identit uživatele ve smyslu definice bezpečnostní politiky VPN uživatelů. |  |  |
|  | Site-to-Site IPsec VPN s podporou statického i dynamického routování. |  |  |
|  | Podpora DLP pro identifikaci, monitorování a ochranu dat. |  |  |
|  | Podpora IoT protokolů (minimálně klasifikace provozu, identifikace zařízení, ochrana zařízení před sítovým útokem). |  |  |
|  | Podpora výrobce v režimu 24x7 a aktualizace všech požadovaných bezpečnostních funkcí po dobu 5 let. |  |  |
|  | Účastník je povinen s dodávkou doložit seznam sériových čísel dodávaných zařízení. |  |  |
|  | **V nabídce účastník doloží katalogový list produktu (datasheet) popisující zadavatelem požadované hardwarové i softwarové parametry.** |  |  |

## Více-faktorová autentizace a Single Sign-On (SSO) – pro 160 uživatelů (ID2)

Tabulka 2: Více-faktorová autentizace a Single Sign-On (SSO) – pro 160 uživatelů (ID2)

| **č.** | **Specifikace požadavků.** | **Účastníkem nabízená hodnota, výrobce a typ.** | **Splněno [ano/ne]** |
| --- | --- | --- | --- |
| **Základní technické požadavky** | | | |
|  | Trvalá licence pro 160 uživatelů s podporou na 60 měsíců, předplatné (subscription, SaaS) je nepřípustné. |  |  |
|  | Kompletně softwarové řešení – bez nutnosti nákupu speciálního hardware. |  |  |
| **Klientská část** | | | |
|  | Možnost získání One-time password,(OTP) aplikací v mobilním zařízení. |  |  |
|  | Možnost získání OTP SMS zprávou. |  |  |
|  | Možnost získání OTP bezpečnostním tokenem. |  |  |
|  | Možnost získání OTP vlastními možnostmi např. min. e-mailem. |  |  |
|  | Aplikace do mobilních zařízení kompatibilní pro stávající platformy zadavatele iOS a Android. (zadavatel umožňuje nabídnout rovnocenné řešení) |  |  |
|  | Mobilní aplikace v hlavních jazykových lokalizacích včetně češtiny. |  |  |
|  | Přístup do mobilní aplikace je možno chránit PIN kódem. |  |  |
|  | OTP nezávislé na internetovém připojení, GSM připojení. |  |  |
|  | Podpora push notifikací kompatibilní pro stávající systémy zadavatele: iOS, watchOS, Android, Android Wear. (zadavatel umožňuje nabídnout rovnocenné řešení) |  |  |
|  | Hardwarové tokeny HOTP nebo TOTP splňující standard OATH. |  |  |
|  | Pro dané řešení musí existovat hardwarové tokeny certifikované výrobcem jako podporované pro nabízený MFA systém. |  |  |
|  | Podpora time based hardwarových tokenů (PSKC). |  |  |
|  | Self-enrollment uživatelů. |  |  |
|  | Součástí dodávky je **110 ks** kompatibilních tokenů bez biometrických parametrů, které mají od výrobce (doložitelné např. datasheetem) deklarovanou podporu pro nabízený MFA systém. |  |  |
| **Ostatní požadavky** | | | |
|  | Ochrana druhým faktorem kompatibilní se stávajícími webovými aplikacemi:   * Microsoft OWA, SharePoint; * RDP; * Exchange Control Panel & Exchange Administrator Center; * VMware Horizon View; * Citrix XenApp; * VPN služeb založených na protokolu RADIUS min. Cisco, Citrix, Fortinet, Microsoft, OpenVPN; * cloudových služeb Office 365, G Suite; * Windows, Linux, macOS účtů.   (zadavatel umožňuje nabídnout rovnocenné řešení) |  |  |
|  | Možnost tvorby výjimek pro vnitřní sítě. |  |  |
|  | Propojení MFA kompatibilní se stávající Active Directory. |  |  |
|  | Možnost implementace do vlastních systémů pomocí SDK výrobce a API výrobce. |  |  |
|  | SDK dostupné minimálně kompatibilní pro následující stávající platformy:   * Java, * PHP, * .NET, * Windows Script Host.   (zadavatel umožňuje nabídnout rovnocenné řešení) |  |  |
|  | Serverová aplikace musí být kompatibilní minimálně se následujícími stávajícími operačními systémy:   * Windows Server 2012 R2 * Windows Server 2016 * Windows Server 2019 * Windows Server 2022 * Windows Server 2025   (zadavatel umožňuje nabídnout rovnocenné řešení) |  |  |
|  | Podpora kompatibilní se stávající Active Directory domény od stávající verze MS Windows 2000.  (zadavatel umožňuje nabídnout rovnocenné řešení) |  |  |
|  | Možnost nasazení v ne-doménových prostředích. |  |  |
|  | Podpora více-doménových prostředí. |  |  |
|  | Podpora alternativních DNS. |  |  |
|  | Podpora cloudových platforem pomocí Active Directory Federation Services. |  |  |
|  | Podpora kompatibilní se stávajícími klientskými operačními systémy zadavatele: Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11.  (zadavatel umožňuje nabídnout rovnocenné řešení) |  |  |
|  | Vzdálená správa pomocí webové konzole nebo kompatibilní se stávající Microsoft Management Console (MMC).  (zadavatel umožňuje nabídnout rovnocenné řešení) |  |  |
|  | Soulad se standardy:   * PCI/DSS - The Payment Card Industry Data Security Standard, * ISAE 3402 – International Standards for Assurance Engagements no. 3402, * HIPAA - Health Insurance Portability and Accountability Act, * FFIEC - Federal Financial Institutions Examination Council compliances, * US Federal Government, * Sarbanes Oxley, * "Code of Connection", * PPI - The Protection of Personal Information Act. |  |  |
|  | Podpora FIDO tokenů. |  |  |
|  | Podpora kompatibilní pro stávající Microsoft Windows Server/SharePoint/Exchange 2019.  (zadavatel umožňuje nabídnout rovnocenné řešení) |  |  |
|  | Možnost definovat maximální počet off-line přihlášení. |  |  |
|  | Centrální správa v cloudu nebo on-premise s možností výběru zadavatele. |  |  |
|  | Součástí dodávky je instalace kompatibilní on-premise řešení do stávajícího VMware prostředí zadavatele.  (zadavatel umožňuje nabídnout rovnocenné řešení) |  |  |
|  | **V nabídce účastník doloží katalogový list produktu (datasheet) popisující zadavatelem požadované softwarové parametry.** |  |  |

## Ochrana před škodlivým kódem (ID3) a Nástroj pro detekci kybernetických bezpečnostních událostí (ID4)

Tabulka 3: Základní vlastnosti

| **č.** | **Specifikace požadavků.** | **Účastníkem nabízená hodnota, výrobce a typ.** | **Splněno [ano/ne]** |
| --- | --- | --- | --- |
| **Základní vlastnosti** | | | |
|  | Licence pro ochranu 120 koncových stanic/uživatelů, celkem 30 serverů (kompatibilní se stávajícím virtuálním prostředí VMware a stávajících fyzických MS Windows serverů). |  |  |
|  | Zabezpečení kompatibilní pro všechny stávající koncové body, včetně fyzických PC s OS MS Windows, Mac a Linux, virtuálních PC (VDI) s OS MS Windows a Linux, fyzických serverů s OS Windows a Linux, virtuálních serverů s OS MS Windows a Linux a mobilních zařízení s OS Android a iOS.  (zadavatel umožňuje nabídnout rovnocenné řešení) |  |  |
|  | **V nabídce doložte katalogový list produktu (datasheet) popisující zadavatelem požadované softwarové parametry.** |  |  |

Tabulka 4: Konzole pro centrální správu řešení

| **č.** | **Specifikace požadavků.** | **Účastníkem nabízená hodnota, výrobce a typ.** | **Splněno [ano/ne]** |
| --- | --- | --- | --- |
|  | Všechny komponenty řešení musejí být v českém jazyce – včetně konzole správy, klientské aplikace a manuálů. |  |  |
|  | Konzole pro správu nasazena v cloudu výrobce, který se stará o její údržbu a vysokou dostupnost veškerých jejích služeb a funkcí. |  |  |
|  | Možnost kdykoli migrovat konzoli pro správu do on-premise prostředí bezplatně, bez změny platnosti licence a za vynaložení minimálního času ze strany administrátora řešení. |  |  |
|  | Konzole pro centrální správu je kompletně multi-tenantní. |  |  |
|  | Podpora produktů výrobcem nástroje bude poskytována v českém jazyce. |  |  |
| **Základní vlastnosti** | | | |
|  | Možnost provádět aktualizace klientů z jiných klientů a tím šetřit šířku přenosového pásma připojení k internetu. |  |  |
|  | Možnost zobrazovat upozornění v konzoli pro správu a posílání upozornění e-mailem. |  |  |
|  | Možnost zasílat upozornění napojením na Syslog server. |  |  |
|  | Možnost využití napojení jakékoli třetí aplikace za pomocí zdokumentované veřejné API, k níž je možné vytvářet klíče přímo z konzole centrální správy bez nutnosti zásahu technické podpory dodavatele či výrobce. |  |  |
| **Úlohy správy bezpečnosti** | | | |
|  | Řešení musí umožnit integraci kompatibilní se stávajícími strukturami zadavatele Microsoft Active Directory za účelem správy ochrany zařízení v těchto inventářích.  (zadavatel umožňuje nabídnout rovnocenné řešení) |  |  |
|  | Řešení musí být schopno odhalit stroje, které nejsou vedeny ve stávající Active Directory pomocí Network Discovery. |  |  |
|  | Filtrování a řazení v inventáři alespoň dle jména hostitele, operačního systému, IP adres, přidělených pravidel a dle času poslední aktivity. |  |  |
|  | Možnost vzdálené instalace a odinstalace EPP klienta přímo z konzole centrální správy. |  |  |
|  | Možnost upravit úroveň skenovacích úloh a jejich spouštění a plánování, přímo z konzole centrální správy. |  |  |
|  | Možnost restartovat serveru nebo desktopu přímo z konzole centrální správy. |  |  |
|  | Centralizované místo pro záznam všech úloh. |  |  |
|  | Přiřazení bezpečnostních pravidel pro koncové stanice možné granulárně na každé úrovni struktury inventáře, včetně kořenu a listů stromu (tzn. jakékoli OU, případně až přímo konkrétní stanici). |  |  |
| **Nastavení úrovně bezpečnosti** | | | |
|  | Více možností přiřazení pravidel:   * podle uživatele či skupiny v Active Directory; * podle síťové lokality; * ve které se zařízení nachází (včetně identifikace podle možné kombinace – inkluze či exkluze - následujících znaků: IP adresa, rozsah IP adres, DNS server, WINS server, výchozí brána, typ sítě, název hostitele, DHCP přípona, zda je možné se připojit ke konkrétnímu hostiteli nebo zda je dostupná konzole centrální správy); * dle OU, ve které se nachází ve stávající AD. |  |  |
|  | Možnost nastavení dědičnosti mezi bezpečnostními pravidly granulárně dle sekcí a subsekcí nastavení bezpečnostních pravidel. |  |  |
| **Reportování** | | | |
|  | Možnost nastavení intervalu, ve kterém jsou reporty generovány, možnost vytvořit report okamžitě. |  |  |
|  | Možnost zasílání vygenerovaných reportů e-mailem. |  |  |
|  | Možnost stáhnout vygenerované reporty minimálně ve formátech .pdf či .csv. |  |  |
|  | Možnost upravení reportů, vybrání cíle (skupina stanic, typ stanic atd.) a časového intervalu, ze kterého je report vytvářen. |  |  |
| **Karanténa** | | | |
|  | Vzdálená obnova či smazání souboru v karanténě. |  |  |
|  | Možnost automaticky přidat soubor do výjimky při obnově z karantény. |  |  |
| **Administrátor řešení** | | | |
|  | Více předdefinovaných rolí: Root, administrátor, reportér:   * 1. Root: spravuje komponenty řešení.   2. Administrátor: spravuje bezpečnostní pravidla a inventář koncových zařízení.   3. Reportér: spravuje a vytváří reporty. |  |  |
|  | Podpora 2-faktorového ověření a možnost jeho vynucení (uživatel se nepřihlásí, dokud si 2-FA nenastaví). |  |  |
|  | Možnost vynutit změnu hesla uživatele po uplynutí určité doby od jeho poslední změny. |  |  |
|  | Možnost automatického zablokování uživatelského účtu při opakovaných neúspěšných pokusech o přihlášení. |  |  |
|  | Detailní možnosti vybrat, jaké služby a jaké typy stanic může uživatel spravovat. |  |  |
| **Logy** | | | |
|  | Zaznamenávání uživatelských akcí. |  |  |
|  | Detailní log pro každou akci. |  |  |
|  | Komplexní vyhledávání v logách. |  |  |
| **Správa a instalace ochrany** | | | |
|  | Administrátor může před instalací vybrat, které moduly ochrany mají být nainstalovány. |  |  |
|  | Instalace může být provedena několika způsoby, alespoň:   1. Stáhnutím instalačního balíčku přímo do pracovní stanice, kde bude nainstalován. 2. Instalace vzdáleně přímo z konzole správy. 3. Distribuce instalačního balíčku pomocí GPO či SCCM. |  |  |
|  | Instalace klienta na koncové stanice ve vzdálené lokalitě může být provedena z existujícího, již nainstalovaného, klienta v této vzdálené lokalitě – účelem je optimalizace přenosu po WAN/VPN. |  |  |
|  | Konzole správy bude reportovat počet chráněných koncových stanic a počet koncových stanic, které chráněné nejsou. |  |  |
|  | Konzole správy obsahuje upravitelné „widgety“ pro okamžitý přehled o stavu ochrany v organizaci. |  |  |
|  | Konzole správy obsahuje detailní informace o chráněných strojích: název, IP adresa, operační systém, instalované moduly, aplikovaná pravidla, informace o aktualizacích. |  |  |
|  | Konzole správy umožňuje získání všech informací potřebných pro řešení potíží s ochranou koncové stanice včetně podrobných logů. |  |  |
|  | Konzole správy umožňuje změnit nastavení hromadně na všech stanicích najednou či třeba jen pro konkrétní skupinu stanic najednou. |  |  |
|  | Pro rozdílné skupiny uživatelů lze granulárně nastavit, jaké skupiny zařízení mají právo spravovat. |  |  |
|  | Možnost vytvářet instalační balíčky pro 32-bit a 64-bit operační systémy, včetně samoinstalačního balíčku, který obsahuje kompletní aplikaci a není nutné pro jeho instalaci přístup k síti. |  |  |
|  | Instalační balíček umožňuje tzn. „tichou“ instalaci (nevyskočí žádné okno, nevyžaduje žádnou uživatelskou interakci). |  |  |
|  | Administrátor bude moci v inventáři správcovské konzole vytvářet skupiny a podskupiny, kam bude moci přesouvat chráněné koncové body. |  |  |
|  | Možnost spustit Network discovery z kteréhokoli již instalovaného klienta. |  |  |

Tabulka 5: Vlastnosti a funkce ochrany fyzických koncových bodů

| **č.** | **Specifikace požadavků.** | **Účastníkem nabízená hodnota, výrobce a typ.** | **Splněno [ano/ne]** |
| --- | --- | --- | --- |
|  | Podpora kompatibilní s následujícími stávajícími OS zadavatele:   * Windows 11 a vyšší * Windows 10 a vyšší * Windows 10 IoT Enterprise * Windows Server 2019 a vyšší * Windows Server 2019 Core * Windows Server 2016 a vyšší * Windows Server 2016 Core * Windows Server 2012 R2 * Windows Server 2012 a vyšší * Ubuntu 14.04 LTS a vyšší * Red Hat Enterprise Linux * CentOS 6.0 a vyšší * SUSE Linux Enterprise Server 11 SP4 a vyšší * OpenSUSELeap 42.x * Fedora 25 a vyšší * Debian 8.0 a vyšší * Oracle Linux 6.3 a vyšší * Amazon Linux AMI 2016.09 a vyšší * Mac OS X El Capitan (10.11) a vyšší   (zadavatel umožňuje nabídnout rovnocenné řešení) |  |  |
|  | Automatické skenování dat, ke kterým je přistupováno – tzn. otevření souboru, kopírování souboru, přenášení souboru (LAN, WAN, sdílené úložiště, přenosná média, pevný disk). |  |  |
|  | Automatické skenování souborů v reálném čase může být nastaveno ke skenování pouze specifických typů souborů. |  |  |
|  | Automatické skenování souborů v reálném čase může být omezeno na maximální velikost souboru |  |  |
|  | Aktualizace bezpečnostního obsahu alespoň jednou za hodinu. |  |  |
|  | Možnost plné ochrany včetně aktualizace pro koncové body trvale bez přístupu k internetu v rámci LAN/WAN sítě. |  |  |
|  | Detekce na základě virových definicí (tzn. signatur). |  |  |
|  | Threat Emulation Technologie (v cloud prostředí dodavatele nebo lokálně). |  |  |
|  | Pokročilá analýza spouštěných procesů ještě před jejich spuštěním a jejich zablokování v případě vykázání škodlivého chování (včetně ochrany proti 0-day útokům). |  |  |
|  | Pokročilá analýza běžících procesů v reálném čase a jejich zablokování v případě detekce škodlivého chování (včetně ochrany proti 0-day útokům). |  |  |
|  | Detekce 0-day útoků na základě cloudového i lokálního (100% funkce i v případě výpadku připojení k internetu) strojového učení. |  |  |
|  | Detekce 0-day útoků na základě odhalování anomálního chování. |  |  |
|  | Detekce s využitím strojového učení. |  |  |
|  | Modul behaviorální analýzy pro detekce chování nových typů ransomware. |  |  |
|  | Aktivní ochrany před útoky hrubou silou na protokol SMB a RDP. |  |  |
|  | Dynamická detekce 0-day útoků, botnetových sítí, Ddos a exploit útoků v cloudových službách dodavatele pomocí umělé inteligence a pokročilých algoritmů strojového učení. |  |  |
|  | Detekce 0-day bezsouborových útoků. |  |  |
|  | Detekce 0-day útoků na úrovni síťového provozu (útoky na RDP, pokusy o zjištění dostupnosti, detekce laterálního pohybu útočníka). |  |  |
|  | Ochrana proti neautorizovanému šifrování s automatickou zálohou dat na nepřístupnou část pevného disku s možností automatické obnovy dat po zastavení útoku. Využití stínová kopie svazku ani jiná řešení statického zálohování nejsou z důvodu možnosti jejich odstranění útočníkem přípustné. |  |  |
|  | Možnost varování před rizikovým chováním uživatele (přihlašování na nezabezpečených webech, používání stejného hesla na mnoha různých webech, používání stejného hesla v interních a externích aplikacích). |  |  |
|  | Uvádění tzn. „Risk score“ uživatelů a koncových stanic umožňující administrátorům určit, kterým stanicím a uživatelům je třeba věnovat pozornost prioritně. |  |  |
|  | Rizika jsou dle závažnosti ohodnocena a pokud se pojí s konkrétním CVE, tak je uvedeno. |  |  |
|  | Schopnost pravidelné automatické detekce bezpečnostně rizikových konfiguračních zranitelností operačního systému koncového bodu pomocí vlastního agenta. |  |  |
|  | Schopnost pravidelné automatické detekce zranitelností instalovaného SW vybavení na koncovém bodě pomocí vlastního agenta chyběj včetně detailního CVE ke každé takové zranitelnosti. |  |  |
|  | Možnost automatické nápravy vybraných rizik, případně uvedení návodu k odstranění rizik, které nelze odstranit automaticky. |  |  |
|  | Možnost automatické detonace podezřelých souborů v Sandboxu s neomezeným počtem detonací. |  |  |
|  | Možnost nastavení Sandboxu – délka pozorování po detonaci, počet opakování detonací, přístup k internetu během detonace ano/ne. |  |  |
|  | Akce automatické nápravy na základě verdiktu po provedené analýze v Sandboxu. |  |  |
|  | Možnost ručního vložení vzorku do Sandboxu. |  |  |
|  | Sandbox po analýze vygeneruje rozsáhlý report o provedené forenzní analýze, včetně: části srozumitelné pro laiky, podrobného shrnutí dění v systému pro experty, časové osy spouštěných procesů a prováděných systémových změn, seznamu a geolokační analýzu síťových připojení, přehledu všech vytvářených, měněných a mazaných souborů a snímky obrazovky případných chybových hlášení. |  |  |
|  | Řešení musí obsahovat funkce EDR / XDR integrované do jedné klientské aplikace spolu s EPP. |  |  |
|  | Řešení musí podporovat možnost izolace infikované koncové stanice. Myšleno tak, že koncová stanice se naprosto odpojí od sítě a bude komunikovat pouze s konzolí centrální správy. |  |  |
|  | Řešení musí být schopno logování systémové, procesové a síťové aktivity v době zachyceného incidentu pro další investigaci. |  |  |
|  | Řešení umožnuje analýzu síťové komunikace, a na základě analýzy detekuje případné incidenty. |  |  |
|  | Řešení generuje detekce na základě automatizovaného hledání IoCs v syrových datech sbíraných EDR senzorem. |  |  |
|  | Řešení u vytvořených incidentů generuje tzv. full execution tree model a časovou osu útoku. |  |  |
|  | Řešení umožňuje analýzu vektoru útoku. |  |  |
|  | Řešení umožňuje logování síťových aktivit v době zachyceného incidentu za účelem dalšího prověřování. |  |  |
|  | Řešení umožňuje tzn. Threat Hunting (hledání IoC v datech sbíraných z EDR). |  |  |
|  | Možnost prověřovat http provoz. |  |  |
|  | Možnost prověřovat provoz šifrovaný pomocí SSL. |  |  |
|  | Možnost nastavení hesla pro odinstalování EPP klientské aplikace z koncových stanic. |  |  |
|  | Možnost šifrovat obsah pevného disku pro notebooky kompatibilní se stávající platformou zadavatele MS Windows.  (zadavatel umožňuje nabídnout rovnocenné řešení) |  |  |
|  | Ochrana agenta před neautorizovanou změnou nastavení, vyřazení z provozu, odinstalací antimalware řešení a kritických nastavení. |  |  |
|  | Automatické skenování emailů na úrovni pracovní stanice, nehledě na použitém emailovém klientu, obojí pro odchozí (SMTP) a příchozí emaily (POP3). |  |  |
|  | Možnost skenovat archivy, možnost nastavení maximální hloubky skenovaných archivů a maximální velikosti skenovaných archivů. |  |  |
|  | Ochrana proti podvodným a phishingovým webovým stránkám. |  |  |
|  | Detekce používaných zařízení (device) na koncové stanici, možnost blokování zařízení dle typu, možnost povolit pouze konkrétní zařízení dle Device ID. |  |  |
|  | Všechny vrstvy ochrany implementovány do jedné aplikace (tzn. není nutnost instalovat více než jednu aplikaci). |  |  |
|  | Řešení musí umožňovat vzdálené připojení na konzoli koncové stanice s možností výpisu procesů, registrů a souborů, vytvoření, změnu či výmaz souborů či registrů a ukončení procesu a to i ve stavu izolace stanice od sítě při použití bezpečnostního řešení. |  |  |
|  | Řešení musí být schopno logování systémové, procesové a síťové aktivity v době zachyceného incidentu pro další investigaci. |  |  |
|  | Podpora offline prostředí, technologie EDR/XDR vyhodnocuje a reaguje na události lokálně, nevyžaduje pro svou činnost připojení k internetu. |  |  |
|  | Grafické zobrazení událostí, které nastaly na koncové stanici při spuštění objektu/procesu (jaký byl sled událostí příkazů, procesů, které procesy, co spouštěly, s jakými komunikovali IP adresami, doménami a tak dále). |  |  |
|  | Přehled všech detekovaných technik/taktik MITRE ATT&CK včetně přímého navázání do zobrazeného kybernetického incidentu a linkem do databáze MITRE. |  |  |
| **Firewall** | | | |
|  | Možnost blokovat skenování portů. |  |  |
|  | Modul musí být možné volitelně kdykoli instalovat a odinstalovat bez nutnosti restartovat OS. |  |  |
|  | Firewall obsahuje systém IDS včetně funkce odhalování neznámých hrozeb. |  |  |
|  | Možnost vypnout IDS. |  |  |
|  | Možnost nastavit profily známých sítí. |  |  |
|  | Možnost blokace Network Discovery kompletně (včetně spojení v LAN) či pouze pro spojení z internetu. |  |  |
| **Karanténa** | | | |
|  | Po každé aktualizaci bezpečnostního obsahu jsou automaticky znovu proskenovány soubory v karanténě. |  |  |
|  | Možnost obnovy souboru do originální či do nově zadané lokality. |  |  |
|  | Automatické mazání souborů v karanténě starších než zadaná maximální doba stáří (maximum nesmí být kratší než 30 dní). |  |  |
| **Kontrola přístupu k internetu** | | | |
|  | Zablokování přístupu na internet pro specifické stanice / skupiny stanic. |  |  |
|  | Zablokování přístupu ke konkrétním webům pro specifické koncové stanice / skupiny stanic. |  |  |
|  | Zablokování přístupu k internetu v určený čas. |  |  |
|  | Zamezení přístupu k typům webových stránek dle výrobcem spravovaných skupin (např. násilí, hazard a jiné). |  |  |
|  | Zamezení přístupu ke kontkrétní webové stránce (včetně podpory tzn. "wildcards" pro možnou inkluzi či exkluzi subdomén). |  |  |

Tabulka 6: Ochrana virtualizovaných koncových bodů

| **č.** | **Specifikace požadavků.** | **Účastníkem nabízená hodnota, výrobce a typ.** | **Splněno [ano/ne]** |
| --- | --- | --- | --- |
|  | Podpora kompatibilní s následujícími stávajícími OS zadavatele:   * Windows * Linux   (zadavatel umožňuje nabídnout rovnocenné řešení) |  |  |
|  | Produkt nepotřebuje stávající VMware vShield či NSX, aby poskytl tzn. bezenginové skenování – režim klienta, kdy na klientském VM běží jen lehký klient a veškeré úlohy skenování jsou prováděny jiným, speciálním „skenovacím“ zařízením; takové „skenovací“ zařízení může být virtualizováno, ale není nutné aby bylo umístěno na tom samém hypervisoru jako chráněné klientské VM. Počet těchto speciálních virtuálních zařízení nesmí být licencí nijak omezen. |  |  |
|  | „Skenovací“ zařízení jsou spravována z konzole centrální správy – aktualizace, restart, přiřazení jednotlivých klientů k těmto „skenovacím“ virtuálním zařízením. |  |  |
|  | „Skenovací“ zařízení musí být možno provozovat v režimu vysoké dostupnosti a rovnoměrného rozložení zátěže. |  |  |
|  | Produkt musí hlásit aktuální stav zabezpečení – VM chráněna/nechráněna, a stav „skenovacího“ zařízení. |  |  |
|  | Řešení musí umožňovat optimalizaci datových přenosů mezi VM a „skenovacím“ zařízením pomocí deduplikace skenovacích procesů – tzn. ten samý soubor (dle hashe) nebude skenován na dvou různých VM (za předpokladu, že se mezitím nezměnila verze bezpečnostní klientské aplikace). |  |  |
|  | Automatické skenování dat, ke kterým je přistupováno – tzn. otevření souboru, kopírování souboru, přenášení souboru (LAN, WAN, sdílené úložiště, přenosná média, pevný disk...). |  |  |
|  | Automatické skenování souborů v reálném čase může být nastaveno ke skenování pouze specifických typů souborů. |  |  |
|  | Automatické skenování souborů v reálném čase může být omezeno na maximální velikost souboru. |  |  |
|  | Aktualizace bezpečnostního obsahu alespoň jednou za hodinu. |  |  |
|  | Detekce na základě virových definicí (tzn. signatur). |  |  |
|  | Threat Emulation Technologie (v cloud prostředí dodavatele nebo lokálně). |  |  |
|  | Pokročilá analýza spouštěných procesů ještě před jejich spuštěním a jejich zablokování v případě vykázání škodlivého chování (včetně ochrany proti 0-day útokům). |  |  |
|  | Pokročilá analýza běžících procesů v reálném čase a jejich zablokování v případě detekce škodlivého chování (včetně ochrany proti 0-day útokům). |  |  |
|  | Detekce 0-day útoků na základě cloudového i lokálního (100% funkce i v případě výpadku připojení k internetu) strojového učení. |  |  |
|  | Detekce 0-day útoků na základě odhalování anomálního chování. |  |  |
|  | Dynamická detekce 0-day útoků, botnetových sítí, Ddos a exploit útoků v cloudových službách dodavatele pomocí umělé inteligence a pokročilých algoritmů strojového učení. |  |  |
|  | Detekce 0-day bezsouborových útoků. |  |  |
|  | Detekce 0-day útoků na úrovni síťového provozu (útoky na RDP, pokusy o zjištění dostupnosti, detekce laterálního pohybu útočníka). |  |  |
|  | Možnost automatického hlídání, zda není koncová stanice špatně nakonfigurována a zda nemá nezáplatované aplikace se známou zranitelností. |  |  |
|  | Možnost varování před rizikovým chováním uživatele (přihlašování na nezabezpečených webech, používání stejného hesla na mnoha různých webech, používání stejného hesla v interních a externích aplikacích). |  |  |
|  | Uvádění tzn. „Risk score“ uživatelů a koncových stanic umožňující administrátorům určit, kterým stanicím a uživatelům je třeba věnovat pozornost prioritně. |  |  |
|  | Rizika jsou dle závažnosti ohodnocena a pokud se pojí s konkrétním CVE, tak je uvedeno. |  |  |
|  | Možnost automatické nápravy vybraných rizik, případně uvedení návodu k odstranění rizik, které nelze odstranit automaticky. |  |  |
|  | Možnost automatické detonace podezřelých souborů v Sandboxu. |  |  |
|  | Možnost nastavení Sandboxu – délka pozorování po detonaci, počet opakování detonací, přístup k internetu během detonace ano/ne. |  |  |
|  | Akce automatické nápravy na základě verdiktu po provedené analýze v Sandboxu. |  |  |
|  | Možnost ručního vložení vzorku do Sandboxu. |  |  |
|  | Sandbox po analýze vygeneruje rozsáhlý report o provedené forenzní analýze, včetně: části srozumitelné pro laiky, podrobného shrnutí dění v systému pro experty, časové osy spouštěných procesů a prováděných systémových změn, seznamu a geolokační analýzu síťových připojení, přehledu všech vytvářených, měněných a mazaných souborů a snímky obrazovky případných chybových hlášení. |  |  |
|  | Řešení musí obsahovat funkce EDR integrované do jedné klientské aplikace spolu s EPP. |  |  |
|  | Řešení musí podporovat možnost izolace infikované koncové stanice. Myšleno tak, že koncová stanice se naprosto odpojí od sítě a bude komunikovat pouze s konzolí centrální správy. |  |  |
|  | Řešení musí být schopno logování systémové, procesové a síťové aktivity v době zachyceného incidentu pro další investigaci. |  |  |
|  | Řešení umožnuje analýzu síťové komunikace, a na základě analýzy detekuje případné incidenty. |  |  |
|  | Řešení u vytvořených incidentů generuje tzv. full execution tree model a časovou osu útoku. |  |  |
|  | Řešení umožňuje analýzu vektoru útoku. |  |  |
|  | Řešení umožňuje logování síťových aktivit v době zachyceného incidentu za účelem dalšího prověřování |  |  |
|  | Možnost prověřovat http provoz. |  |  |
|  | Možnost prověřovat provoz šifrovaný pomocí SSL. |  |  |
|  | Možnost nastavení hesla pro odinstalování EPP klientské aplikace z koncových stanic. |  |  |
|  | Modul pro ochranu mailboxů lokálně provozované Microsoft Exchange proti malwaru, spamu a phishingovým útokům. |  |  |
|  | Automatické skenování emailů na úrovni pracovní stanice, nehledě na použitém emailovém klientu, obojí pro odchozí (SMTP) a příchozí emaily (POP3). |  |  |
|  | Možnost skenovat archivy, možnost nastavení maximální hloubky skenovaných archivů a maximální velikosti skenovaných archivů. |  |  |
|  | Ochrana proti podvodným a phishingovým webovým stránkám. |  |  |
|  | Detekce používaných zařízení (device) na koncové stanici, možnost blokování zařízení dle typu, možnost povolit pouze konkrétní zařízení dle Device ID. |  |  |
|  | Řešení umožňuje tzn. Threat Hunting (hledání IoC v datech sbíraných z EDR). |  |  |
|  | Řešení umožňuje ukládat data o bezpečnostních incidentech až 90 dní. |  |  |
|  | Všechny vrstvy ochrany implementovány do jedné aplikace (tzn. není nutnost instalovat více než jednu aplikaci). |  |  |

Tabulka 7: Rozšířená funkce XDR

| **č.** | **Specifikace požadavků.** | **Účastníkem nabízená hodnota, výrobce a typ.** | **Splněno [ano/ne]** |
| --- | --- | --- | --- |
| **Sonda XDR pro analýzu stávající Microsoft Active Directory** | | | |
|  | Rozšiřující modul pro XDR – Sonda pro analýzu OnPremise Active Directory. |  |  |
|  | Rozšiřující modul pro XDR – Provádí monitorování a zpracování informací o uživatelích z OnPremise kompatibilní se stávající Microsoft Active Directory. |  |  |
|  | Rozšiřující modul pro XDR – analyzuje a doplňuje incidenty bezpečnostního řešení o informace získané ze stávající Microsoft Active Directory. |  |  |
|  | Rozšiřující modul pro XDR – sonda kompatibilní pro stávající MS Active Directory musí auditovat bezpečnostní politiky v AD, minimálně Account Logon, Account Management, Object Access, Policy Change a Privilege Use. |  |  |
|  | Rozšiřující modul pro XDR – Sonda pro analýzu kompatibilní se stávající Microsoft Active Directory musí být plně integrována do řešení ochrany koncového bodu. |  |  |
|  | Rozšiřující modul pro XDR – Sonda kompatibilní pro stávající Microsoft Active Directory nesmí zasahovat do chodu MS AD. |  |  |
|  | Z konzole bezpečnostního řešení je možno zakázat uživatelský účet nebo vynutit reset hesla kompatibilní se stávající Microsoft AD, který byl použit v rámci bezpečnostního incidentu. |  |  |
| **Sonda XDR pro analýzu síťové vrstvy** | | | |
|  | Rozšiřující modul pro XDR – Síťová sonda analyzující provoz na síťové vrstvě, která je plně integrovaná do nabízeného řešení. |  |  |
|  | Rozšiřující modul pro XDR – Síťová sonda musí monitorovat a analyzovat datové toky v rámci počítačové sítě. |  |  |
|  | Rozšiřující modul pro XDR – Síťová sonda obohacuje incidenty bezpečnostního řešení o informace získané z datové sítě. |  |  |
|  | Rozšiřující modul pro XDR – Síťová sonda je samostatná appliance kompatibilní minimálně pro stávající Vmware ESXi a stávající Microsoft Hyper-V. |  |  |
|  | Rozšiřující modul pro XDR – Síťová sonda obsahuje minimálně jeden port pro zpracování síťového provozu. |  |  |
|  | Rozšiřující modul pro XDR – Síťová sonda umožňuje připojení prostřednictvím TAP/SPAN portu. |  |  |
|  | Rozšiřující modul pro XDR – Nabízená síťová sonda nesmí být na monitorovacím portu detekovatelná, nesmí zasahovat do síťového provozu. |  |  |
| **Sonda XDR pro analýzu stávajícího MS Office365 prostředí** | | | |
|  | Rozšiřující modul pro XDR – MS Office365 sonda analyzující provoz kompatibilní se stávajícím prostředí zadavatele MS Office365, která je plně integrovaná do nabízeného řešení. |  |  |
|  | Rozšiřující modul pro XDR – Síťová sonda musí monitorovat a analyzovat aktivity v rámci stávajícího MS Office365. |  |  |
|  | Detekce účtů s vypnutou anti-phishing ochranou. |  |  |
|  | Detekce phishing kampaní. |  |  |
|  | Detekce vytváření nových účtů bez požadavků na multifaktor autentikaci. |  |  |
|  | Detekce a analýza ukládání dokumentů s makry kompatibilní ve stávajícím prostředí MS Office365 (OneDrive, Sharepoint). |  |  |
|  | Monitoring stávajícího MS Exchange Online emailové aktivity. |  |  |

## Nástroj pro sběr a nepřetržité vyhodnocení kybernetických bezpečnostních událostí – SIEM (Security Information and Event Management) (ID5)

Tabulka 8: Nástroj pro sběr a nepřetržité vyhodnocení kybernetických bezpečnostních událostí – SIEM (Security Information and Event Management) (ID5)

| **č.** | **Specifikace požadavků.** | **Účastníkem nabízená hodnota, výrobce a typ.** | **Splněno [ano/ne]** |
| --- | --- | --- | --- |
|  | Trvalá licence pro 120 uživatelů s podporou na 60 měsíců, předplatné (subscription, SaaS) je nepřípustné. |  |  |
|  | Systém provádí zpracování událostí z předdefinovaných následujících zdrojů logů stávajících aplikací, operačních systémů a síťového hardware:   1. Apache web server, 2. Apache Tomcat, 3. Dell IDRAC (Integrated Dell Remote Access Controller), 4. Dell iDRAC 9 (Integrated Dell Remote Access Controller), 5. Dell PowerConnect, 6. ESET Remote Administrator, 7. FortiAuthenticator, 8. FortiADC, 9. FortiGate, 10. FortiMail, 11. FortiSandbox, 12. FortiWeb, 13. FreeRADIUS, 14. HP iLO 4, HP iLO 5, 15. HP Intelligent Management Center (IMC), 16. HP ProCurve, 17. HP Comware, 18. Linux Rsyslog,Linux Syslog-NG, 19. Microsoft Exchange, 20. Microsoft DHCP, 21. Microsoft DNS, 22. Microsoft SQL Server, 23. Microsoft Windows Event Sender (WES) (Deprecated), 24. Microsoft Windows File Share Audit, 25. Microsoft Windows Firewall, 26. Microsoft Windows IIS, 27. MikroTik, 28. MySQL database server, 29. Office 365, 30. QNAP, 31. Samba, 32. SQL agents, 33. Squid, 34. Sysmon, Systemd, Synology, Syslog over TLS, 35. Veeam Backup & Replication, VMware. |  |  |
|  | 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 uživatelem bez nutnosti spolupráce s výrobcem nebo dodavatelem (vč. subdodavatelů) 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.  **Zadavatel** **požaduje předložit příslušnou dokumentaci k vytváření parserů a testování jejich funkčnosti v nabídce.** |  |  |
|  | 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. **Zadavatel požaduje v nabídce předložit 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 kompatibilní pro stávající databáze zadavatele MS SQL a to bez nutnosti instalovat na databázový server doplňkový software nebo agenta. U sběru dat z databází musí systém umět nastavit interval čtení.  **Zadavatel požaduje v nabídce předložit 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). |  |  |
|  | 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.  **Zadavatel požaduje v nabídce předložit 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. Všechny operace uživatelů včetně prohledávání dashboardů jsou logované a lze je auditovat přímo v systému. |  |  |
|  | 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.  **Zadavatel požaduje v nabídce předložit link na dokumentaci popisující nastavení systému v jednotném grafickém rozhraní tak, aby získával logy ze stávajícího systému zadavatele MS 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). |  |  |
|  | 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 ve stejném rozsahu 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.  **Zadavatel požaduje v nabídce předložit link na online dokumentaci nebo připojit pdf aktuální kompletní dokumentace k ověření jednotlivých vlastností nabízeného 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. |  |  |
|  | 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.  **Zadavatel požaduje v nabídce předložit dokumentaci, ze které je zřejmé, jakým způsobem je realizována konfigurace v rámci jednotné konzole.** |  |  |
|  | Systém umožňuje jednotné vytváření uživatelských rolí definujících přístupová práva k uloženým událostem na základě typu zdrojů a značek a k jednotlivým ovládacím komponentům systému.  **Zadavatel požaduje v nabídce předložit 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 stávajících systémů zadavatele MS 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. |  |  |
| **Minimální 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. |  |  |
|  | 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.  **Zadavatel požaduje doložit v nabídce 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. |  |  |
| **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.  **Zadavatel požaduje v nabídce předložit 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. |  |  |
|  | 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. Systém musí zobrazovat aktuální i historické informace vytížení vlastních systémových prostředků včetně velikosti fronty na zpracování dat, odezvy DNS serveru, indexovací rychlosti, IOps diskových operací a dostupného diskového prostoru. |  |  |
|  | 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. Vizuální programovací jazyk není prezentován textově, ale graficky formou schémat-symbolů, které reprezentují aplikační logiku a kontrolují syntaxi. **Zadavatel požaduje v nabídce doložení 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. |  |  |
|  | 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.  **Zadavatel požaduje v nabídce doložení 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, úspěšné ověření uživatele, neúspěšné ověření uživatele, zpráva přišla ze stávajícího OS zadavatele MS Windows, zpráva byla vygenerována firewallem. |  |  |
|  | 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.  **Zadavatel požaduje v nabídce doložení 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. **Zadavatel požaduje V nabídce popis použité technologie 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. **Zadavatel požaduje v nabídce doložit 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.  **Zadavatel požaduje doložit 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 umět zobrazovat počet odesílaných emailů ve frontě. |  |  |
|  | 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.  **Zadavatel požaduje v nabídce doložit 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.  **Zadavatel požaduje v nabídce doložit 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).  **Zadavatel požaduje v nabídce doložit 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 ze stávajícího Microsoft prostředí zadavatele** | | | |
|  | Události ze stávajícího Microsoft prostředí zadavatele jsou vyčítány pomocí agenta instalovaného přímo v koncových systémech. Windows agent musí současně podporovat jak monitoring interních stávajících windows logů, tak monitoring textových souborových logů. Agent se nesmí instalovat individuálně, ale prostřednictvím stávajícího MS AD Group Policy a nesmí vyžadovat žádnou konfiguraci na cílovém systému.  **Zadavatel požaduje doložit odkaz na dokumentaci popisující požadované vlastnosti integrovaného Windows agenta.** |  |  |
|  | Agent sběru ze stávajícího Microsoft prostředí zadavatele podporuje globální i lokální nastavení filtrace odesílaných událostí pomocí centrální správcovské konzole. Například, zašli pouze logy z adresářů eventview Systém, Security 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.  **Zadavatel požaduje v nabídce doložit 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 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 400 na dobu předpokládané morální životnosti produktu – 5 let. Předpokládáme instalaci agentů na všechny systémy současně, proto je nutné potvrdit zda systém výkonnostně splňuje tento požadavek. |  |  |
| **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.  **Zadavatel požaduje v nabídce doložit 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.  **Zadavatel požaduje v nabídce doložit odkazem na dokumentaci, jak vypadá komunikační matice pro připojení řešení 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 kompatibilní pro stávající virtualizaci zadavatele 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** | | | |
|  | Zadavatel požaduje podporu pro nasazení ve vysoké dostupnosti. |  |  |
|  | HW – Požadovaná min. 5letá 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. |  |  |
|  | Dodávka musí obsahovat veškeré potřebné licence pro splnění požadovaných vlastností a parametrů. |  |  |
|  | Účastník je povinen s dodávkou doložit seznam sériových čísel dodávaných zařízení. |  |  |
|  | **V nabídce doložte katalogový list produktu (datasheet) podrobně popisující hardwarové i softwarové parametry.** |  |  |

## Implementace

Tabulka 9: Požadavky – Implementace nabízeného řešení

|  |  |  |  |
| --- | --- | --- | --- |
| **č.** | **Specifikace minimálních požadavků** | **Účastníkem nabízená hodnota** | **Splněno [ano/ne]** |
|  | Součástí je zajištění instalace a konfigurace předmětu veřejné zakázky v návaznosti na stávající infrastrukturu zadavatele (tj. včetně dopravy, montáže, instalace a implementace do stávající IT infrastruktury) v sídle zadavatele. |  |  |
|  | Účastník do své nabídky zahrne veškerý instalační materiál a kabeláž nutnou k plnohodnotnému zprovoznění předmětu veřejné zakázky jako logického a funkčního celku. |  |  |
|  | Součástí instalace musí být i zaškolení administrátorů (správců) – 2 osoby minimálně v rozsahu nutném pro samostatnou administraci předmětu zakázky. Administrací se rozumí zejména: konfigurace, monitoring činnosti, aktualizace, řešení problémů, zálohování konfigurace.  Trvání zaškolení administrátorů je minimálně 40 hodin pro každého administrátora v sídle zadavatele. |  |  |
|  | Konzultační práce pro předmět veřejné zakázky v minimálním rozsahu 48 hodin, poskytnuté do konce realizace. |  |  |
|  | Testování implementovaného předmětu veřejné zakázky na zkušebních datech. |  |  |
|  | Vypracování a předání dokumentace popisující konečný skutečný stav předmětu veřejné zakázky ve 3 tištěných vyhotoveních.  Dokumentace bude zahrnovat:   * popis všech prvků/zařízení, * popis způsobu zálohy a obnovy konfigurace všech prvků/zařízení * veškeré požadavky na zachování záruky/podpory (např. kompatibilita) * informaci o způsobu řešení servisních požadavků. |  |  |
|  | Provedení všech předepsaných zkoušek a revizí včetně vystavení dokladů o jejich provedení, doložení atestů, certifikátů, prohlášení o shodě, vlastnostech a ostatních dokladů potřebných pro možnost řádného provozování ve smyslu platných právních a ostatních předpisů apod. a jejich předání zadavateli ve 3 vyhotoveních. |  |  |
|  | Dodání všech potřebných dokladů, zajištění návodů k obsluze, návodů na provoz a údržbu díla.  Těmito doklady rozumí např. i potvrzení o provedení zkoušek na všech rozvodech a instalacích dotčených stavebními a montážními pracemi, kompletní zprávy o výchozích revizích elektrických zařízení. |  |  |
|  | Zahájení ostrého provozu (převedení předmětu veřejné zakázky do produkčního prostředí). |  |  |

# Specifikace požadavků řešení – 2. Část

V následujících podkapitolách je uvedena specifikace parametrů řešení nutných pro plnění této veřejné zakázky.

V době posuzování nabídek musí nabídka řešení účastníka dále splňovat níže specifikované požadavky.

Účastník nakopíruje do nabídky následující tabulku a popis splnění požadavků ve sloupci **„Účastníkem nabízená hodnota, výrobce a typ.“**, tak že tam nakopíruje text ze sloupce „Specifikace požadavků“ a **doplní výrobce a typ**, případně doplní nebo upraví popis nabízené hodnoty, ze kterého bude patrné, že splňuje požadavky.

Sloupec „Specifikace požadavků“ nesmí být účastníkem nijak měněn a účastník je oprávněn vyplnit pouze sloupec „Účastníkem nabízená hodnota, výrobce a typ.“.

Sloupec **„Splněno [ano/ne]“** účastník nevyplňuje, slouží pro zadavatele.

## Server OS datacenter a CAL 160ks, Terminal server a CAL 40 ks. (ID2)

Tabulka 10: Server OS datacenter a CAL 160ks, Terminal server a CAL 40 ks. (ID2)

| **č.** | **Specifikace požadavků.** | **Účastníkem nabízená hodnota, výrobce a typ.** | **Splněno [ano/ne]** |
| --- | --- | --- | --- |
|  | Nové, nepoužité licence pro 36 core kompatibilní s MS Windows Server 2025 Datacenter Edition (zadavatel umožňuje nabídnout rovnocenné řešení)   1. Podpora min. 64 procesorových socketů. 2. Podpora běhu v on-premise, hybrid a cloudovém prostředí. 3. Podpora TPM 2.0 čipů. 4. Podpora ochrany firmware před neoprávněným přepsáním. 5. Podpora replikace úložišť. 6. Vestavěná technologie serverové i desktopové virtualizace. 7. Nativní podpora virtualizace sítí. 8. Neomezený počet virtuálních serverů. 9. Počet licencí bude určen počtem jader procesorů ve všech navržených virtualizačních serverech. |  |  |
|  | Nové, nepoužité licence 160ks kompatibilní s MS Windows Server 2025 User CAL  (zadavatel umožňuje nabídnout rovnocenné řešení) |  |  |
|  | Nové, nepoužité licence 40 ks kompatibilní s MS Windows Server 2025 Remote Desktop Services User CAL  (zadavatel umožňuje nabídnout rovnocenné řešení) |  |  |

## Databázový server SQL licence na 4 core (ID2)

Tabulka 11: Databázový server SQL licence na 4 core (ID2)

| **č.** | **Specifikace požadavků.** | **Účastníkem nabízená hodnota, výrobce a typ.** | **Splněno [ano/ne]** |
| --- | --- | --- | --- |
|  | Nová, nepoužitá, trvalá licence pro 4 core kompatibilní s Microsoft SQL Server 2022 Standard včetně SA (Software Assurance) na 36 měsíců (zadavatel umožňuje nabídnout rovnocenné řešení) |  |  |
|  | Databázový SW systému v aktuální verzi pro GOV. Licence musí umožnit provoz neomezeného počtu uživatelů. Databázový SW bude provozován ve virtuálním prostředí a licenčně musí umožnovat přiřazení min 4 core ve virtuálním prostředí. |  |  |

## Zálohovací SW pro 25 virtuálních serverů (ID6)

Tabulka 12: Zálohovací SW Veeam 25 virtuálních serverů (ID6)

| **č.** | **Specifikace požadavků.** | **Účastníkem nabízená hodnota, výrobce a typ.** | **Splněno [ano/ne]** |
| --- | --- | --- | --- |
|  | Trvalá (perpetuální) Licence kompatibilní s SW Veeam Data Platform Essentials Universal pro 25 instancí.  (zadavatel umožňuje nabídnout rovnocenné řešení) |  |  |
|  | Zálohovací řešení musí být kompatibilní a podporovat stávající infrastrukturu VMware ve verzích 6.x, 7.x a 8.0, včetně VMware Cloud Foundation, VMware Cloud on AWS, VMware cloud on Dell a Azure VMware Solution. |  |  |
|  | Řešení musí být kompatibilní a podporovat stávající hostitele spravované serverem VMware vCenter ve verzích 6.x, 7.x a 8.0 i samostatné ESXi hostitele. |  |  |
|  | Zálohovací řešení musí být kompatibilní a podporovat stávající MS Windows Server Hyper-V 2012 až 2022 včetně Server Core, Azure Stack HCI i Microsoft Hyper-V Server. |  |  |
|  | Řešení musí být kompatibilní a podporovat stávající hostitele spravované pomocí Microsoft System Center Virtual Machine Manager 2012 R2 až 2019, klastrové i samostatné hostitele Hyper-V. |  |  |
|  | Řešení musí podporovat zálohování všech operačních systémů, které jsou podporovány pro provoz na těchto hypervizorech. |  |  |
|  | Řešení musí být kompatibilní a podporovat zálohování stávající platformy Red Hat Virtualization 4.4 SP1. |  |  |
|  | Řešení musí podporovat zálohování celých zařízení NAS, jednotlivých sdílených složek SMB a NFS a souborových serverů Windows a Linux. |  |  |
|  | Podpora (maitenance) na dobu 60 měsíců. |  |  |

## Diskové pole (ID6)

Tabulka 13: Diskové pole (ID6)

| **č.** | **Specifikace požadavků.** | **Účastníkem nabízená hodnota, výrobce a typ.** | **Splněno [ano/ne]** |
| --- | --- | --- | --- |
|  | Architektura: modulární, minimálně dvou řadičové hybridní diskové pole active-active designu, řešení je koncipováno jako HW, SW a FW od jednoho výrobce |  |  |
|  | Diskové pole musí umožňovat synchronní replikaci pomocí nativní funkcionalitou stávajícího diskového pole: MTM 4680-3P4 S/N:7813BA8 a to v konfiguraci aktivně-aktivní mezi dvěma lokalitami, kdy umožňuje mít dvě synchronizované kopie diskového svazku umístěné ve dvou různých geografických lokalitách. Obě kopie jsou aktivní, což znamená, že hostitelé mohou číst a zapisovat na obě kopie. |  |  |
|  | Rozšiřitelnost, podporované disky a moduly:   * celková velikost cache/RAM v jednom řadiči je minimálně 32GB; * celková nativní rozšiřitelnost je minimálně 400 disků, v případě nasazení více řadičů až dvakrát tolik disků. To nelze řešit pomocí externí virtualizace nebo podvěšením dalšího pole a řadičů; * podpora 2,5” nebo 3,5” disků technologie SSD/flash včetně rotačních disků a to současně; * enterprise úrovně tzn. minimálně eMLC, 3D TLC, SLC nebo eSLC nebo enterprise flash modulů s hodnotou DWPD 1 a vyšší; * rotační disky minimálně na SAS 3.0 architektuře; * podpora minimálně následujících režimů RAID - 1, 5, 6 nebo DRAID 1, 5 a 6 |  |  |
|  | Minimální požadovaná hrubá kapacita:  Tier 0: minimálně 39 TB čisté kapacity s paritní ochranou ekvivalentní k RAID6 s Hot Spare disku na SSD, maximální velikost jednoho disku je 4TB. |  |  |
|  | Požadavky na velikost řešení a rozšiřitelnost: nabízené řešení nesmí přesáhnout 2U |  |  |
|  | Konektivita k hostitelským serverům (front-end):   * diskové pole obsahuje připojení diskového pole blokovým přístupem minimálně pomocí 16Gbit FC a 10Gbit iSCSI; * jsou požadovány min. 4 porty 16Gb -- FC a 2 porty 10Gb iSCSI na řadič, tzn. minimálně 8x 16Gbit FC portů a 4x 10Gbit iSCSI portů na jedno dvouřadičové diskové pole. |  |  |
|  | Typ přístupu k datům:   * blokový, standard FCP a iSCSI, možnost použít více protokolů najednou. |  |  |
|  | Funkcionality pro efektivní ukládání a správu dat:   * vytváření virtuálních logických disků; * thin provisioning (včetně detekce a reklamace prázdného prostoru) komprese dat v reálném čase bez nutnosti dedikování dodatečného diskového prostoru pro post-processing pro celou nabízenou kapacitu; * deduplikace dat v reálném čase bez nutnosti dedikování dodatečného diskového prostoru pro post-processing pro celou požadovanou kapacitu včetně SW licence; * možnost budoucího šifrování dat pro jakýkoliv typ disků a nabízenou kapacitu (licence nemusí být součástí dodávky); * možnosti budoucího nasazení inteligentní správy výkonnostních charakteristik (pro minimálně 3) virtualizovaných diskových prostorů (automatická migrace více utilizovaných dat na rychlejší disky nebo SSD), licence nemusí být součástí dodávky; * podpora externí storage virtualizace a možnost dalšího připojení externích diskových polí od různých výrobců min. pro účely migrace. Seznam podporovaných diskových systému musí být veřejně dostupný; * podpora nástrojů pro sledování historických dat o vytížení datového úložiště (minimálně počet IOps, latence, propustnost, alokovaná kapacita, využití keší) s granularitou na hosta či LUN s historií minimálně 1 rok (možnost řešit externích SW nástrojem v rámci dodávky); * podpora kompatibilní se stávající Microsoft VSS * podpora kompatibilní se stávající VMware VAAI, VVOL, dále je požadován VASA provider přímo ve FW nabízeného diskového pole. |  |  |
|  | Kopírovací funkce - licence musí být součástí nabídky a musí být na neomezenou kapacitu, počet disků, expanzích jednotek:   * zrcadlení virtuálního disku tzn. ochrana virtualizovaných dat v režimu RAID1 (s možností zdvojení dat virtuálního disku i na dvě pole) * možnost vytváření snapshotů (CoW a RoW) a klonů v následujících režimech:   + snapshot se po určité době může automaticky stát klonem   + inkrementální snapshoty, tzn. kopírují se jen rozdílová data mezi dvěma okamžiky iniciace klonu   + reverzní snapshoty, tzn. lze provést zpětné přesunutí dat z klonu do původního originálního Volume * interní/externí zrcadlení logického (virtuálního) disku z jednoho zdroje do dvou cílů pro zvýšení dostupnosti v případě výpadku jednoho cíle |  |  |
|  | Bezpečnost:   * ochrana proti ransomware útokům nativní funkcionalitou nabízeného pole v rámci jeho funkcionalit – řešení z aplikační vrstvy pomocí aplikací třetích stran není přípustné. Řešení musí být pro tento účel jasně popsané a určené, např. ochrana LUNu pouze nastavením do read-only modu není dostatečná pro splnění tohoto požadavku. * řešení musí umožňovat detekci ransomware v reálném čase na blokové úrovni. |  |  |
|  | Zajištění kontinuální dostupnosti dat (DR a HA řešení) - licence musí být součástí nabídky a musí být na neomezenou kapacitu, počet disků, expanzích jednotek:   * upgrade software a hardware u řadičů je proveditelné za chodu a bez ztráty přístupu hostitelských serverů k datum; * diskové musí být možné spojit do clusteru, který umožňuje vytvoření jednoho funkčního celku, zrcadlení dat mezi jednotlivými poli; * vytvoření HA řešení s automatickým failover bez dalších vícenákladů, které je navíc nezávislé na běžných OS nebo virtualizační platformě včetně příslušných licencí; * podpora replikace do třetí lokality; * SW pro redundantní datové cesty v ceně řešení * Nabízené řešení musí být plně kompatibilní se stávajícím VMware Metro Storage Cluster funkcionalitou, tzn. musí být dohledatelné v matici kompatibility na stránkách VMware. |  |  |
|  | Migrace dat:   * transparentní migrace (tzn. možnost zdarma migrovat data ze stávajících diskových polí na nová disková úložiště) s možnosti rozšíření o synchronní a asynchronní zrcadlení logických (virtuálních) disků v případě více lokalit. |  |  |
|  | Počet hostitelských serverů připojovaných k diskovému poli:   * řešení obsahuje licence na neomezený počet připojení hostitelských serverů |  |  |
|  | Management virtualizačního controleru, další požadavky:   * software pro plnohodnotnou správu diskového pole a diskových subsystémů, možnost ovládání přes CLI, GUI (ze std. web browseru) Remote Service (call home) v ceně řešení; * příkazy prováděné v GUI jsou uchovávány v tzv. "AuditLogu" v podobě standardních CLI příkazů, které lze později snadno zkopírovat a aplikovat při programování uživatelských skriptů např. pro podporu automatizace zálohování; * Servisní podpora výrobce bude v českém jazyce. |  |  |
|  | Provedení služeb jako součást nabídky o doprava a instalace HW a SW na místě:   * ekologická likvidace obalového materiálu * úvodní inicializace HW * konsolidace FW jednotlivých zařízení, v souladu doporučením výrobců pro daný virtualizační software a aktuální verzi (týká instalace diskového Clusteru, dle požadavků výše * migrace stávajícího provozovaného prostředí zadavatele na nový HW * rekonfigurace zálohovacího clusteru |  |  |
|  | Příslušenství:  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. |  |  |
|  | Servisní podpora:  Minimálně 5 let; v online režimu 24x7 s odezvou tentýž pracovní den včetně software podpory, která umožňuje např. přístup k novým verzím FW, opravným patchům apod. |  |  |

## Síťové úložiště NAS (ID6)

Tabulka 14: Síťové úložiště NAS (ID6)

| **č.** | **Specifikace požadavků.** | **Účastníkem nabízená hodnota, výrobce a typ.** | **Splněno [ano/ne]** |
| --- | --- | --- | --- |
|  | Provedení: Server pro osazení do standardního 19" racku, velikost 2U, bez nástrojové kolejnice pro montáž do racku. |  |  |
|  | CPU: 1 procesor s 16 jádry s možností osazení druhého procesoru.  Spotřeba procesoru maximálně 270W.  Výkon plně osazené konfigurace dle benchmarku SPEC CPU2017 - hodnoty musí být uvedené na spec.org, sloupec Baseline, Integer Rates – 380, Floating Point Rates – 535. |  |  |
|  | RAM: 256GB DDR5 operační paměti, rychlost paměti aspoň 5600MHz.  Osazení všech kanálů paměťového řadiče.  Rozšiřitelnost na 8 TB DDR5 RAM, minimálně 32 paměťových slotů. |  |  |
|  | HDD: Osazeno 12x 16TB 7.2k SATA hot-swap HDD.  Podpora až 20x 3,5" disků.  Dvojice interních M.2 SATA SSD v RAID1, umožňující bootování OS nebo hypervizoru, o kapacitě 240GB a alespoň 1 DWPD. |  |  |
|  | RAID Řadič: 12 Gb interní RAID řadič s podporou Tri-Mode (možnost obsluhovat disky typu SATA, SAS a NVMe U.3), 4GB zálohované cache, možnost připojení až 16 disků. |  |  |
|  | IO Rozhraní: 4 portová síťová karta 1Gb Base-T ve standardu OCP 3.0.  2 portová síťová karta 10Gb Base-T PCIe.  2 portový 16Gb Fiber Channel Host Bus Adapter. |  |  |
|  | PCIe sloty: Podpora až 10 PCIe slotů generace PCIe 5.0 + 1x slot OCP 3.0.  Možnost osazení až osmi grafických adaptérů (GPU). |  |  |
|  | Porty: VGA port, 3x USB minimálně generace 3.1 na zadní straně serveru.  Minimálně 2x USB z čelní strany serveru, jedno z čelních USB může sloužit také pro přístup na servisní procesor serveru.  Minimálně 1x interní USB s možností bootu OS. |  |  |
|  | Napájení: Plně redundantní za chodu měnitelné napájecí zdroje.  Minimálně certifikace Titanium, účinnost až 96%.  Výkon minimálně 1100 W. |  |  |
|  | Správa serveru:   1. Vzdálené správa s dedikovaným vlastním portem RJ-45 a možností převzít plně vzdálené ovládání serveru. 2. Možnost redundantního plně dedikovaného 1Gb RJ-45 management portu. 3. Podpora standardů IPMI (minimálně verze 2.0), SNMP (verze 3), CIM-XML, REST a RedFish. 4. Možnost nahrávání záznamu bootu serveru a pádu serveru. 5. Možnost vzdáleného mountu ISO a IMG image souborů (minimálně pomocí protokolů: HTTPS, SFTP, CIFS, a NFS). 6. Možnost sdílet jednu virtuální konzoli až šesti uživateli. 7. Podpora standardních Webových prohlížečů a HTML5. 8. Možnost blokovat konkrétní IP adresy. 9. Real time sledování vytíženosti CPU, paměti a spotřeby, možnost Power cappingu (včetně historických dat). 10. Možnost asistované instalace OS bez dalších nástrojů, médií, ISO apod. 11. Nejvyšší licence pro správu serveru bez jakéhokoli omezení funkcionalit/doby/provozu/počtu spravovaných serverů. 12. Možnost osadit server diagnostickým displejem (interním, nebo externím) zobrazující základní informace o serveru a jeho stavu (IP adresy, teploty atd.). 13. Možnost připojit se lokálně na servisní procesor pomocí mobilního telefonu (podpora minimálně pro stávající OS Android a Apple). Minimální funkcionalita aplikace: stav serveru, včetně chybových hlášení a možnost správy serveru. 14. Podpora proaktivních upozornění využívající technologii S.M.A.R.T. a PFA. 15. Slot pro micro SD kartu o kapacitě alespoň 4GB. 16. Možnost správy a synchronizace konfigurace a úrovně firmware pro několik serverů najednou. |  |  |
|  | Zabezpečení: TPM 2.0 chip a podpora SED disků.  Možnost osazení čelního zamykatelného panelu a intrusion switche.  Splňující standardy NIST SP800-131A, SP800-193, SP800-147B, FIPS 140-2 a CNSA Suite 1 Quantum-resistant.  Podpora Advanced Encryption Standard (AES). |  |  |
|  | Chlazení: Plně redundantní, za chodu měnitelné ventilátory.  Regulovaný chod jednotlivých ventilátoru na základě aktuálních teplot. |  |  |
|  | Vybavení racku: Bez nástrojové vysouvací lyžiny s možností CMA (ramena pro vedení kabelů). |  |  |
|  | Záruka: Záruka serveru minimálně 5 let s odezvou technika následující pracovní den, Onsite.  Možnost rozšíření záruky na minimálně 7 let.  Hlášení servisních požadavků výrobci serveru musí být možné 24x7 v českém jazyce. |  |  |
|  | Podporované stávající OS (minimálně):  Microsoft Windows Server 2019, 2022 a 2025  Red Hat Enterprise Linux 8.8, 8.9, 8.10, 9.2 - 9.5  SUSE Linux Enterprise Server 15 SP5, SP6 a Xen SP5  Ubuntu 18.04, 20.04 a 22.04 LTS 64-bit  VMware ESXi 7.0 U3, 8.0 U |  |  |
|  | Software pro monitoring:  Časově neomezená licence na hromadnou správu serverů, inventarizace a alerting.  Možnost hromadného sledováni a upgrade úrovní FW jednotlivých komponent serverů.  Call Home funkce.  Plug-in do management nodů virtualizačních hypervizorů (minimálně pro stávající VMware vCenter, vRealize, Microsoft Admin Center, Microsoft System Center, SPLUNK, AIOps, PagerDuty a ServiceNow).  Podpora REST-API a Redfish standardů.  Podpora pro správu stávající serverové infrastruktury zadavatele na platformě Lenovo.  Podpora minimálně 1000 zařízení.  Podpora standardních Webových prohlížečů a HTML5.  Software musí být tzv. bez-agentový. |  |  |

## Implementace

Tabulka 15: Požadavky – Implementace nabízeného řešení

|  |  |  |  |
| --- | --- | --- | --- |
| **č.** | **Specifikace minimálních požadavků** | **Účastníkem nabízená hodnota** | **Splněno [ano/ne]** |
|  | Součástí je zajištění instalace a konfigurace předmětu veřejné zakázky v návaznosti na stávající infrastrukturu zadavatele (tj. včetně dopravy, montáže, instalace a implementace do stávající IT infrastruktury) v sídle zadavatele. |  |  |
|  | Účastník do své nabídky zahrne veškerý instalační materiál a kabeláž nutnou k plnohodnotnému zprovoznění předmětu veřejné zakázky jako logického a funkčního celku. |  |  |
|  | Součástí instalace musí být i zaškolení administrátorů (správců) – 2 osoby minimálně v rozsahu nutném pro samostatnou administraci předmětu zakázky. Administrací se rozumí zejména: konfigurace, monitoring činnosti, aktualizace, řešení problémů, zálohování konfigurace.  Trvání zaškolení administrátorů je minimálně 40 hodin pro každého administrátora v sídle zadavatele. |  |  |
|  | Konzultační práce pro předmět veřejné zakázky v minimálním rozsahu 48 hodin, poskytnuté do konce realizace. |  |  |
|  | Testování implementovaného předmětu veřejné zakázky na zkušebních datech. |  |  |
|  | Zahájení ostrého provozu (převedení předmětu veřejné zakázky do produkčního prostředí). |  |  |
|  | Vypracování a předání dokumentace popisující konečný skutečný stav předmětu veřejné zakázky.  Dokumentace bude zahrnovat:   * popis všech prvků/zařízení, * popis způsobu zálohy a obnovy konfigurace všech prvků/zařízení * veškeré požadavky na zachování záruky/podpory (např. kompatibilita) * informaci o způsobu řešení servisních požadavků. |  |  |

# Specifikace požadavků řešení – 3. Část

V následujících podkapitolách je uvedena specifikace parametrů řešení nutných pro plnění této veřejné zakázky.

V době posuzování nabídek musí nabídka řešení účastníka dále splňovat níže specifikované požadavky.

Účastník nakopíruje do nabídky následující tabulku a popis splnění požadavků ve sloupci **„Účastníkem nabízená hodnota, výrobce a typ.“**, tak že tam nakopíruje text ze sloupce „Specifikace požadavků“ a **doplní výrobce a typ**, případně doplní nebo upraví popis nabízené hodnoty, ze kterého bude patrné, že splňuje požadavky.

Sloupec „Specifikace požadavků“ nesmí být účastníkem nijak měněn a účastník je oprávněn vyplnit pouze sloupec „Účastníkem nabízená hodnota, výrobce a typ.“.

Sloupec **„Splněno [ano/ne]“** účastník nevyplňuje, slouží pro zadavatele.

## Hasicí systém pro serverovnu (ID6)

Tabulka 16: Hasicí systém pro serverovnu (ID6)

| **č.** | **Specifikace požadavků.** | **Účastníkem nabízená hodnota, výrobce a typ.** | **Splněno [ano/ne]** |
| --- | --- | --- | --- |
|  | Stabilní hasicí zařízení musí být vhodné pro hašení elektronických zařízení a hasivo nesmí poškodit zdraví přítomných osob. |  |  |
|  | Hasivo musí být environmentálně netečné a hasivo nesmí podléhat registraci na Ministerstvu životního prostředí. |  |  |
|  | SHZ nesmí obsahovat tlakové nádoby a musí být umístěno přímo v chráněném prostoru. |  |  |
|  | Koncentrace zdrojové směsi min. 1kg/10m3. |  |  |
|  | Aspirační (nasávací) systém detekce. |  |  |
|  | Životnost zařízení minimálně 12 let a servis musí být zajištěn po dobu 20 let. |  |  |
|  | Stabilní hasicí zařízení certifikováno pro použití na území ČR, musí být doloženo Stavebně technické osvědčení, Certifikace České autorizované osoby, TZUS, PAVUS. |  |  |
|  | Musí být schopno v případě potřeby přenést výstupní stavy na další PBŘ případně GSM nebo síťový modul, musí být bezobslužné a musí sdělovat své stavy. |  |  |
|  | Likvidace zařízení zvláště hasiva nesmí být zpoplatněno. |  |  |
|  | Servisní odezva 24/7. |  |  |

## Implementace

Tabulka 17: Požadavky – Implementace nabízeného řešení

|  |  |  |  |
| --- | --- | --- | --- |
| **č.** | **Specifikace minimálních požadavků** | **Účastníkem nabízená hodnota** | **Splněno [ano/ne]** |
|  | Dodávka a instalace systému Stabilního hasicího zařízení (dále jen SHZ) v budově Palackého náměstí 196/6 v místnosti v přízemí č. 104 (serverovna). |  |  |
|  | Součástí je zajištění instalace a konfigurace předmětu veřejné zakázky v návaznosti na stávající infrastrukturu zadavatele (tj. včetně dopravy, montáže, instalace a implementace do stávající IT infrastruktury) v sídle zadavatele. |  |  |
|  | Účastník do své nabídky zahrne veškerý instalační materiál a kabeláž nutnou k plnohodnotnému zprovoznění předmětu veřejné zakázky jako logického a funkčního celku. |  |  |
|  | Součástí instalace musí být i zaškolení administrátorů (správců) – 2 osoby minimálně v rozsahu nutném pro samostatnou administraci předmětu zakázky. Administrací se rozumí zejména: konfigurace, monitoring činnosti, aktualizace, řešení problémů, zálohování konfigurace.  Trvání zaškolení administrátorů je minimálně 8 hodin pro každého administrátora v sídle zadavatele. |  |  |
|  | Vypracování a předání dokumentace popisující konečný skutečný stav předmětu veřejné zakázky ve 3 tištěných vyhotoveních.  Dokumentace bude zahrnovat:   * popis všech prvků/zařízení, * veškeré požadavky na zachování záruky/podpory * informaci o způsobu řešení servisních požadavků. |  |  |
|  | Provedení všech předepsaných zkoušek a revizí včetně vystavení dokladů o jejich provedení, doložení atestů, certifikátů, prohlášení o shodě, vlastnostech a ostatních dokladů potřebných pro možnost řádného provozování ve smyslu platných právních a ostatních předpisů apod. a jejich předání zadavateli ve 3 vyhotoveních. |  |  |
|  | Dodání všech potřebných dokladů, zajištění návodů k obsluze, návodů na provoz a údržbu díla.  Těmito doklady rozumí např. i potvrzení o provedení zkoušek na všech rozvodech a instalacích dotčených stavebními a montážními pracemi, kompletní zprávy o výchozích revizích elektrických zařízení. |  |  |
|  | Zahájení ostrého provozu (převedení předmětu veřejné zakázky do produkčního prostředí). |  |  |

# Požadavky na servisní podporu provozu a SLA

Požadavky na servisní podporu provozu a SLA jsou uvedeny ve smlouvě o dílo a poskytování servisní podpory v ZD **v příloze č. 3 pro 1. část, v příloze č. 4 pro 2. část a v příloze č. 5 pro 3. část**.

# Podmínky předání a převzetí – akceptace

Podmínky předání a převzetí – akceptace jsou stanoveny ve smlouvě o dílo a poskytování servisní podpory v ZD v **příloze č. 3 pro 1. část, v příloze č. 4 pro 2. část a v příloze č. 5 pro 3. část.**

# Harmonogram plnění

Harmonogram plnění je uveden ve smlouvě o dílo a poskytování servisní podpory v ZD v **příloze č. 3 pro 1. část, v příloze č. 4 pro 2. část a v příloze č. 5 pro 3. část**.

# Seznam zkratek

API Rozhraní pro programování aplikací (Application Programming Interface)

DHCP Protokol pro správu sítě vyžadovaný v sítích IP (Dynamic Host Configuration Protocol)

DNS Domain Name System

EDR Detekce a odpověď koncového bodu (Endpoint Detection and Response)

FC Fibre Channel

HA High Availability

HTTP Hypertext Transfer Protocol

HTTPS Hypertext Transfer Protocol Secure

HW Hardware

IS Informační systém

IT Informační technologie

LAN lokální síť (Local Area Network)

NFS Network File System

MP Management Packs

OOB Out-Of-Band

OS Operační systém

RAID Redundant Array of Independent Disks

SAS Serial Attached SCSI

SLA Dohoda o úrovni služeb servisní podpory (Service Level Agreement)

SSD Solid State Drive

SSH Secure Shell

SSL Secure Sockets Layer

SW Software