# Město Holešov

# **TECHNICKÁ SPECIFIKACE**

**KYBERBEZPEČNOST**

Veškeré produkty, které dodavatel dodává v rámci plnění zadavateli, musí splňovat následující podmínky a dodavatel splnění těchto podmínek potvrdí samostatným čestným prohlášením:

* 1. jsou nové, byly oprávněně uvedeny na trh v EU nebo pochází z autorizovaného prodejního kanálu výrobce,
	2. mají plnou záruku od výrobce,
	3. jsou podporovány výrobcem a jsou součástí servisního a podpůrného programu výrobce,
	4. obsahují všechny nezbytné licence na používání příslušného softwaru,
	5. jsou určeny pro provoz v České republice (EU).

Tyto skutečnosti dodavatel doloží:

1. potvrzením výrobce daného zařízení, nebo
2. čestným prohlášením distributora, nelze-li prohlášení výrobce získat, nebo
3. jiným rovnocenným dokladem (doklady) v případě, že doklady dle předchozích písm. a) a b) není dodavatel z důvodů, které mu nelze přičítat, schopen předložit (takové důvody musí dodavatel doložit).

Zadavatel si vyhrazuje právo na ověření všech dodaných informací od výrobce daného zařízení a zjištění původu výrobků nejpozději při jejich předávání, a to dle příslušných sériových čísel a právo podpisu akceptačního protokolu, osvědčujícího převzetí dodávky, až po ověření původu výrobku.

Dodavatel doloží toto potvrzení dle předchozího odstavce ke všem nabídnutým technologiím v níže uvedeným kapitolám technické specifikace:

**1) Nástroj pro zajišťování úrovně dostupnosti informací**

* **Server 2 ks**
* **Server OS + CAL**
* **Software Defined Storage**

**2) Nástroj pro ochranu integrity komunikačních sítí**

**3) Systém pro analýzu síťového provozu a bezpečnostní monitoring**

**4) NAS** - [**Network Attached Storage**](https://www.synology.com/cs-cz/dsm/solution/what-is-nas/for-home)

### **5) Nástroj pro ochranu koncových stanic**

**6) Nástroj pro ověřování identity uživatelů**

### **7) Nástroj pro ochranu a zabezpečení e-mailů**

### **8) Nástroj pro centralizované zaznamenávání událostí z libovolných zdrojů, s možností analýzy a řešení provozních i bezpečnostních událostí/incidentů ze systémů a aplikací zadavatele.**

### **9) Ochrana počítačové sítě před malwarem a zneužíváním zařízení na úrovni DNS překladu, řešení poskytujícího plnou kontrolu nad DNS provozem**

## 1) Nástroj pro zajišťování úrovně dostupnosti informací

### Server 2 ks

|  |  |
| --- | --- |
| **Parametr** | **Minimální požadavek** |
| Výrobce a model | **[bude doplněno dodavatelem]** |
| Provedení, příslušenství | * Rackové provedení, max 2U
 |
| CPU | * Min. 1x procesor o výkonu minimálně 24800 bodů dle <http://cpubenchmark.net/>, min počet jader 8
 |
| RAM + HDD | * minimálně 256 GB RAM v provedení min. DDR5, min. 4800 MHz
* Server musí disponovat alespoň 8x diskovou hotswap šachtou pro disky přístupnou zpředu. Požadujeme osazení:
* min. 3x NVMe SSD 7,68TB RI Hot Plug disky
* bootovací zařízení 2x 480GB Raid 1
 |
| Řadič disků: | * Řadič min. 4GB cache  s ochranou proti výpadku napájení
* podpora hot-plug disků SAS, SATA, NVMe
* podpora min. RAID - 0, 1, 5, 6, 10, 50, 60
 |
| Síťové karty: | * 4 x 10/25GbE SFP28
* 4x 1Gbit Base T
 |
| Napájecí zdroje: | * 2x napájecí zdroj minimálně 1000W
 |
| Management: | * Plný vzdálený management umožňující plnou vzdálenou konzoli (html5), připojení lokálních médií
 |
| Ostatní: | * Zásuvné ližiny pro rack

Podpora systémů:* Microsoft Windows Server
* Red Hat® Enterprise Linux
* SUSE Linux Enterprise Server
 |
| Záruka, servis | * Záruka na 5 let typu NBD, oprava v místě instalace serveru, servis je poskytován výrobcem serveru.
 |
| Kompatibilita | * Všechny servery budou od jednoho výrobce z důvodu zajištění maximální kompatibility a jednotného servisního místa a managementu
 |
| Další informace či odkazy dodavatele k nabízenému plnění (nepovinné pole) |  |

SERVER OS + CAL

|  |  |
| --- | --- |
| **Parametr** | **Minimální požadavek** |
| Výrobce a model | **[bude doplněno dodavatelem]** |
| Parametry | 2 ks licencí 64-bitového serverového operačního systému v aktuální verzi * Podpora min. 64 procesorových socketů
* Podpora běhu v on-premise, hybrid a cloudovém prostředí
* Podpora TPM 2.0 čipů
* Podpora ochrany firmware před neoprávněným přepsáním
* Podpora replikace úložišť
* Vestavěná technologie serverové i desktopové virtualizace
* Nativní podpora virtualizace sítí
* Neomezený počet virtuálních serverů
* Počet licencí bude určen počtem jader procesorů ve všech navržených serverech – min 2x16CORE
* Operační systém musí být kompatibilní s již provozovanými aplikacemi. Aktuálně zadavatel provozuje operační systémy od společnosti MICROSOFT.
* licence pro nabízené operační systémy umožňující využívat těchto systémů minimálně pro **85** zařízení + **5** uživatelů
 |
| Další informace či odkazy dodavatele k nabízenému plnění (nepovinné pole) |  |

Software Defined Storage

|  |  |
| --- | --- |
| **Parametr** | **Minimální požadavek** |
| Výrobce a model | **[bude doplněno dodavatelem]** |
| Parametry | * Nabízené řešení Software Defined Storage (SDS) bude využívat SAN infrastrukturu na protokolu iSCSI.
* SDS musí umět virtualizovat kapacitu z vnitřních úložišť a tuto kapacitu poskytovat pomocí standardního protokolu.
* Kromě SDS musí být v nodech storage clusteru provozovatelné  také virtuální servery.
* Nabízené řešení musí být široce škálovatelné
* SDS musí podporovat min. OS Windows 2008 R2, a vyšší, Linux, VMware 6.0 a vyšší, Hyper-V,  včetně „multi-path“ připojení
* Podpora autentizace uživatelů přes Active Directory
* Řešení musí podporovat SSD, SAS i NL-SAS disky v jednom nodu současně.
* SDS musí umět vytvořit logický disk (LUN) o velikosti min.64TB
* Čistá kapacita storage clusteru musí být nelimitovaná
* Řadiče diskového pole musí podporovat režim active/active a automaticky rozkládat zátěž každého LUNu na všechny disky v dané vrstvě.
* Nabízené řešení musí využívat min. 10 Gbit technologii
* Storage musí podporovat No Single Point of Failure řešení tak, aby při havárii libovolného storage nodu/řadiče provoz plynule pokračoval bez odstávky. Rovněž upgrade systému storage clusteru (HW, firmware ...) musí být možné provést bez přerušení provozu.
* Řešení umožní synchronní replikaci dat mezi uzly clusteru pro zvolené datové oblasti na úrovni nodů clusteru a synchronní replikaci LUNů mezi dvěma lokalitami.
* Podpora protokolu NVMe-oF minimálně na platformě Hyper-V
* Řešení musí podporovat min.tyto protokoly: ISCSI, SMB 3.0, NFS V4
* Podpora VVols pro VMware prostředí
* Podpora Write-Back Cache pro ukládání dat do mezipaměti, která je uzpůsobená pro intenzivní virtualizovaná pracovní vytížení.
* Požadujeme licence pro následující funkce:
* kompletní management/GUI a command line. Grafické rozhraní pro správu musí být intuitivní a jednoduše ovladatelné.
* snapshpot – až 64 snapshootů z jednoho logického disku
* thin provisioning
* synchronní replikace mezi NODy
* podpora multipathing a Microsoft MPIO DSM
* Podpora VMware VAAI
* Řešení musí umožňovat detailní reporting o okamžité i historické vytíženosti SDS
* Podpora produktu poskytovaná výrobcem na dobu 5 let (v ceně licence)
 |
| Další informace či odkazy dodavatele k nabízenému plnění (nepovinné pole) |  |

### 2) nástroje pro ochranu integrity komunikačních sítí

INFRASTRUKTURA – 2 core a 1 přístupový SWITCH

|  |  |
| --- | --- |
| **Parametr** | **Minimální požadavek** |
| Výrobce a model | **[bude doplněno dodavatelem]** |
| Základní vlastnosti | * Záruka výrobce na výměnu vadného HW platná po celou dobu životnosti zařízení, minimálně 5 let od ukončení prodeje daného zařízení
* Podpora výrobce pro řešení technických problému platná po celou dobu životnosti zařízení, minimálně 5 let od ukončení prodeje daného zařízení.
* IEEE 802.3ad (Link Aggregation)
* IEEE 802.3ad přes více přepínačů ve stohu nebo více šasis
* Minimálně 8 linek jako součást Link Aggregation Group trunku
* Minimální počet konfigurovatelných Link Aggregation Group trunků: 16
* IEEE 802.1Q
* Minimální počet aktivních VLAN: 4093
* IEEE 802.1x
* Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací)
* Podpora instance spanning-tree protokolu per VLAN
* IEEE 802.1w - Rapid Spanning Tree Protocol
* Protokol MVRP/GVRP nebo VTP pro definici a správu VLAN sítí
* Podpora jumbo rámců (min. 9000 bytes)
* Detekce protilehlého zařízení (např. CDP nebo LLDP)
* Směrování protokolů IPv4 a IPv6 v hardware
* IGMPv2, IGMPv3
* IGMP snooping
* MLD snooping
* Minimální počet HW QoS front: 8
* QoS classification – ACL, DSCP, CoS based
* IPv6 First Hop Security (RA guard, DHCPv6 snooping, IPv6 source guard)
* Možnost definovat povolené MAC adresy na portu
* Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové MAC a IP adresy
* Bezpečnostní funkce umožňující ochranu proti připojení neautorizovaného DHCP serveru
* Bezpečnostní funkce umožňující inspekci provozu protokolu ARP
* HW trusted modul využíván pro bezpečné uložení hesel a šifrovacích klíčů
* IEEE 802.3az.
* Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu.
* SSHv2.
* CLI rozhraní.
* SNMPv2/v3.
* TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting).
* Záruka dohledatelná na webových stránkách výrobce, stahování aktualizací a řešení servisních případů přímo na webových stránkách výrobce zařízení
 |
| Technické požadavky na agregační přepínače LAN - 2ks | • L2/L3 přepínač• Rackmount provedení pro 19’’ rozvaděč • Stohovatelný switch, minimálně 8 zařízení v jednom stohu • Rozměr 1 RU • 10x 10GE SPF+ porty • 2x combo 10G SFP+/ 10GbitBase-T• 1x RJ45 1Gbit Management port• Minimální kapacita přepínání 240 Gbps • Minimální paketový výkon přepínače 178 Mpps• minimálně 4093 aktivních VLAN• Minimální počet záznamů MAC tabulky 16 000 • Minimální počet MST Spanning tree instancí 8• Minimální počet záznamů v routovací tabulce 900 (pro IPv4)• Packet buffer minimálně 1,5MB |
| Technické požadavky na přístupový přepínač LAN - 1ks | • L2/L3 přepínač• Rackmount provedení pro 19’’ rozvaděč • Stohovatelný switch, minimálně 8 zařízení v jednom stohu • Rozměr 1 RU • 48x 10/100/1000Mbit RJ45 porty • 4x 10G SFP+ porty• Minimální kapacita přepínání 176 Gbps • Minimální paketový výkon přepínače 130 Mpps• minimálně 4093 aktivních VLAN• Minimální počet záznamů MAC tabulky 16 000 • Minimální počet MST Spanning tree instancí 8• Minimální počet záznamů v routovací tabulce 900 (pro IPv4)• Packet buffer minimálně 1,5MB |
| Spojovací materiál | * 30x 10G SFP+ Transceiver SM
* 2x DAC kabel 10Gbit, 1M
* 10x DAC kabel 10Gbit, 3M
* 6x DAC kabel 10Gbit, 5M
* Optické moduly a DAC kabely musí podléhat stejné záruce jako switche
* Další drobný a propojovací materiál nutný k plnohodnotné realizaci díla jednotlivě nespecifikovaný (optické propojovací kabely, metalické propojovací kabely, napájecí kabely atd)
 |
| Certifikace dodavatele, původ zboží | * Jsou splněny „Požadavky na certifikaci dodavatele HW a původ zboží“
 |
| Další informace či odkazy dodavatele k nabízenému plnění (nepovinné pole) |  |

3 - Systém pro analýzu síťového provozu a bezpečnostní monitoring

TECHNICKÁ SPECIFIKACE :

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

Nabízená technologie musí být určená pro provoz v ČR. Podpora na licence ve všech úrovních musí být zajištěna přímo jejich výrobcem, kterého může zadavatel přímo kontaktovat.

Při definici technických požadavků jsou všechny uvedené požadavky závazné. Je-li definice požadavku „umožňuje, lze, je možné, možnost, …“ je uvedený parametr závazný a požadovaná funkcionalita musí být v rámci Systému dodána/naimplementována a případně licencována. Tyto technické požadavky jsou minimální možné, dodavatel může nabídnout charakteristiky (funkce) lepší.

Řešení musí splňovat **VŠECHNY** níže uvedené požadavky:

|  |  |
| --- | --- |
| **Požadované funkcionality/vlastnosti**  | **Nabízené řešení splňuje/nesplňuje,** vč. vysvětlení, jak je zadání splněno |
| **Systém pro analýzu síťového provozu** |
| Systém složený z hardwarových zařízení musí monitorovat síťovou aktivitu v reálném čase a identifikovat potenciální kybernetické hrozby, bezpečnostní rizika a anomální chování a musí o nich v reálném čase vytvářet upozornění.  |  |
| Dodaný systém musí analyzovat síť na základě zrcadleného síťového provozu ze SPAN portů nebo TAPů (nikoliv jen na základě statistických protokolů typu NetFlow) a zároveň bez potřeby nasazovat agenty na koncové stanice nebo další zařízení v síti. |  |
| Systém musí analyzovat obsah datových paketů v reálném čase a detekovat protokol nebo aplikaci na základě obsahu provozu prostřednictvím DPI (Deep Packet Inspection), nikoli pouze čísla portu. |  |
| Dodaný systém musí být schopen analyzovat síť také na základě zpracování statistických protokolů typu NetFlow, IPFIX, NetStream, Cisco NSEL a případně dalších. |  |
| Systém musí být plně funkční v offline prostředí objednatele bez využití cloudového prostředí pro sběr, ukládání a zpracování dat a veškeré konfigurace a reporting jsou k dispozici přímo v systému. |  |
| Aktualizace systému musí být možné provádět uživatelsky v offline režimu. |  |
| **Zpracování a ukládání síťových toků** |
| Systém ukládá síťové toky ve formátu, který umožní analýzu síťové komunikace na úrovni jednotlivých toků, včetně dohledání informací o aplikačních transakcích a jejich metadatech z L2 až L7, obsažených v daném síťovém toku. |  |
| Požadované protokoly pro ukládání aplikačních metadat z jednotlivých transakcí jsou: DHCP, DNS, SMB, HTTP, HTTPS, SMTP, SMTPS, POP3, IMAP, SSH, LDAP, LDAPS, KERBEROS, SNMP, CIFS, MSSQL, RDP, SIP, TELNET, FTP, FTP-DATA, TFTP, TFTP-DATA, NFS, ARP, SSL/TLS zapouzdření. |  |
| Je požadováno vysokorychlostní úložiště pro uchování historie datových toků na dobu minimálně 3 měsíců složené z SSD nebo NVMe disků. |  |
| **Analýza aplikačních a systémových logů**Systém musí být schopen sbírat a analyzovat aplikační a systémové logy ve formátu syslog z dohledovaných zařízení a identifikovat nebezpečné nebo potenciálně škodlivé aktivity. |  |
| **Uživatelské rozhraní** |
| Systém musí poskytovat jednotné grafické uživatelské rozhraní pro veškerou práci uživatelů, včetně všech detekcí, analýzy síťových statistik, nastavení systému, konfiguraci alertů, reportů a dashboardů. |  |
| Systém musí být schopen vytváření profilů a skupin uživatelů pro omezení funkcionality produktu a viditelnosti uložených dat s podporou minimálně: |  |
| * granulárního nastavení přístupu k analytickým i konfiguračním/administrativním komponentám systému s definovanými úrovněmi přístupu (alespoň read, write, execute),
 |  |
| * granulárního nastavení přístupu k datům z různých segmentů sítě organizace s definovanými úrovněmi přístupu (alespoň read, write, execute),
 |  |
| * vytváření vlastních filtrů veškerých dat a jejich sdílení mezi uživateli a skupinami uživatelů,
 |  |
| * vytváření vlastních uživatelských pohledů, reportů, dashboardů apod.
 |  |
| **Automatické hlášení (alerty) a reporting** |
| Systém musí být schopen upozorňovat uživatele prostřednictvím minimálně emailu a logu o všech identifikovaných událostech a dále o událostech filtrovaných minimálně dle IP a MAC adresy, podsítě, závažnosti události, kategorie události, země, uživatele, síťové služby, čísla portu, provozu do/z internetu. |  |
| Tyto alerty musí být systém schopen dodávat i ve strojově čitelném formátu pro vyžití v nástrojích typu SIEM a musí obsahovat minimálně kompletní informace o detekované události včetně URL odkazu na danou událost v reportovaném období do grafického rozhraní systému. |  |
| Systém musí mít možnost vytváření automatizovaných manažerských reportů o stavu kybernetické bezpečnosti z pohledu zprávy kybernetických incidentů ideálně dle oblastí jejich vzniků (např.: doména, web, email apod.). |  |
| Je požadováno vytváření automatizovaných reportů v českém jazyce. |  |
| **Integrace systému** |
| Systém musí poskytovat hotové nástroje umožňující integraci se softwarem třetích stran bez použití API systému, a to minimálně: |  |
| * syslog, CEF a LEEF pro export událostí včetně plné podpory filtrů (exportování pouze požadovaných dat)
 |  |
| * přímé url odkazy na libovolnou obrazovku grafického uživatelského rozhraní a filtrovaná zobrazení v grafickém uživatelském rozhraní
 |  |
| * export informací o toku ve formátu IPFIX nebo podobném formátu včetně plné podpory filtrů (exportovat lze pouze požadovaná data) včetně aplikačních metadat alespoň pro protokoly HTTP, HTTPS a SMTP
 |  |
| * integrace se službami identity uživatelů bez nutnosti konfigurace zasílání logů do systému – minimálně Microsoft Active Directory
 |  |
| * integrace s firewall řešením pro automatické a manuální reakce vyvolané systémem
 |  |
| * integrace s nástroji pro řízení přístupu k síti pro automatickou a manuální reakci systému.
 |  |

## Požadavky na architekturu nasazení

|  |  |
| --- | --- |
| **Požadované funkcionality/vlastnosti**  | **Nabízené řešení splňuje/nesplňuje,** vč. vysvětlení, jak je zadání splněno |
| **Obecné požadavky pro nasazení** |
| Pro všechny HW komponenty senzor a kolektor je požadován formát 1U nebo 2U server o velikosti 19“. |  |
| Pro všechny HW komponenty senzor a kolektor je požadován duální zdroj napájení se schopností hot-swap. |  |
| Pro všechny HW komponenty senzor a kolektor je požadováno samostatné síťové rozhraní pro vzdálenou správu serveru v případě výpadku systému typu IPMI, IDRAC, ILO apod.  |  |
| **Požadavky pro pokrytí IT prostředí** |
| Je požadován 1x HW datový kolektor/sensor o celkové propustnosti minimálně 100Mbps pro 200 monitorovaných IP adres s monitorovacím rozhraním 2x1GbE. |  |

## Požadavky na schopnost detekce bezpečnostních událostí

|  |  |
| --- | --- |
| **Požadované funkcionality/vlastnosti** | **Nabízené řešení splňuje/nesplňuje,** vč. vysvětlení, jak je zadání splněno |
| **Monitorování zařízení, segmentů sítě a využívaných síťových služeb** |
| Dodaný systém musí identifikovat všechna zařízení připojená do sítě včetně koncových zařízení, serverů, IoT zařízení apod. Zároveň musí být systém schopen identifikovat změny v síti – minimálně:  |  |
| * změna IP/MAC adresy hosta,
 |  |
| * duplicitní IP/MAC adresa,
 |  |
| * změna VLAN,
 |  |
| * vytvoření nové podsítě,
 |  |
| * připojení nového zařízení,
 |  |
| * použití nebo vznik nové služby,
 |  |
| * nedostupnost dříve dostupné a komunikující služby nebo dříve dostupného a komunikujícího zařízení,
 |  |
| * přístup nového zařízení ke službě či zařízení
 |  |
| * ověřování platnosti interních certifikátu pro validní TLS šifrování u HTTPS a upozornění před datem jejich vypršení.
 |  |
| Systém musí uživateli umožnit pomocí těchto detekčních metod nastavovat bezpečnostní politiky pro různé segmenty sítě a pro různá zařízení a na porušení těchto politik reagovat upozorněním. |  |
| **Samostatné učení behaviorálních aktivit a detekce anomálií** |
| Systém musí používat matematické metody samostatného učení pro analýzu síťové aktivity, vytvářet a v čase automaticky modifikovat modely chování na základě běžného chování jednotlivých zařízení a na nich provozovaných služeb v rámci celé organizace.  |  |
| Systém musí mít schopnost na základě matematického modelu daného zařízení a jeho služeb identifikovat nestandardní síťové chování, a to zejména odchylky od modelu normálního chování pro:  |  |
| * odchylku od modelu pro přenos dat, toků a paketů,
 |  |
| * odchylku od modelu pro počet komunikačních partnerů,
 |  |
| * odchylku od modelu entropie na komunikačních portech,
 |  |
| * odchylku od modelu pro počet síťových toků a využitých síťových služeb,
 |  |
| * odchylku od modelu výkonnosti sítě (rychlost přenosu) a aplikací (doba odezvy).
 |  |
| Samostatné učení je požadováno na všech síťových zařízeních a na nich provozovaných službách (port číslo 0 až 65535 u TCP i UDP) na IPv4 a IPv6 a dalších protokolech L3 a L4 síťové vrstvy. |  |
| **Identifikace neznámých hrozeb a podezřelých chování** |
| Systém musí být schopen detekovat neznámé hrozby, které nelze identifikovat prostřednictvím detekčních signatur, jako jsou trojské koně, botnety apod. Zejména musí být identifikovány tyto příznaky potenciálně škodlivého chování: |  |
| * průzkumné aktivity v síti,
 |  |
| * detekce podezřelého strojového chování, které nevytvářejí lidští uživatelé sítě,
 |  |
| * detekce repetitivních vzorců chování na síti,
 |  |
| * detekce botnetů a ovládání kompromitované stanice,
 |  |
| * detekce příznaků těžení kryptoměn,
 |  |
| * útoky hrubou silou a enumerace dat,
 |  |
| * rozpoznání tunelovaného síťového provozu – alespoň IPv4 prostřednictvím IPv6 a DNS tunely.
 |  |
| **Detekce na základě databáze známých hrozeb** |
| Systém musí být schopen identifikovat hrozby a reportovat události na základě |  |
| * detekční databáze známých hrozeb, tj. malware (trojské koně, viry, červy, rootkity, apod.), známých útoků (exploity) a zranitelností, porušení bezpečnostních pravidel a „best practices“ a dalších rizik,
 |  |
| * reputační databáze známých škodlivých IP adres, TLS certifikátů, záznamů DNS a hostname, URL adres a hashů souborů.
 |  |
| Tyto databáze musí být aktualizované minimálně na hodinové bázi. Nesmí se jednat pouze o volně dostupné/open-source databáze, ale musí se jednat o komerční databázi renomovaného vendora nebo poskytovatele těchto služeb. |  |
| Uživatel musí být schopen importovat vlastní záznamy. |  |
| Systém musí využívat tuto detekci pro veškerý monitorovaný provoz (na perimetru i v interní síti mezi všemi segmenty), nikoliv pouze pro omezený segment nebo podmnožinu celkové komunikace.  |  |
| Databáze detekčních pravidel (signatur) musí být založena na pokročilých regulárních výrazech pro zpracování řetězců, které dokáží provádět inspekci veškeré síťové komunikace od L2 (Ethernet apod.) po L7. Systém musí detekovat události na základě vysokého počtu signaturních pravidel (minimálně několik desítek tisíc).  |  |
| Uživatel musí být schopen prostřednictvím webové aplikace přidávat vlastní detekční pravidla v praktickém a obecně využívaném formátu bez nutnosti znalosti syntaxe a sémantiky pravidel.Příklad možné syntaxe detekčního pravidla:*alert tcp $HOME\_NET any -> any any (msg:”Command Shell Access”; content:”C:\\Users\\Administrator\\Desktop\\hfs2.3b”;)*  |  |
| **Analýza šifrované komunikace**Vedle samostatného učení musí systém používat další metody pro analýzu šifrované komunikace, minimálně TLS fingerprinting a s ní spojenou detekci známých hrozeb. |  |
| **Asistované učení** |
| Je požadován uživatelsky přívětivý proces vytváření pravidel pro zpřesnění detekce a eliminaci falešně pozitivní detekce, a to na základě minimálně následujících parametrů: |  |
| * IP adresa,
 |  |
| * MAC adresa,
 |  |
| * hostname,
 |  |
| * segment sítě / podsíť,
 |  |
| * lokalita – ASN, země apod.
 |  |
| * směr komunikace – určení klienta, nebo serveru,
 |  |
| * detekovaná událost – kategorie, název apod.
 |  |
| * použité služby, protokolu, portu,
 |  |
| * libovolné kombinaci výše popsaných.
 |  |
| Systém musí být schopen eliminovat falešné alarmy i pro události detekované v historii. |  |

## Požadavky na zajištění síťové viditelnosti

|  |  |
| --- | --- |
| **Požadované funkcionality/vlastnosti** | **Nabízené řešení splňuje/nesplňuje,** vč. vysvětlení, jak je zadání splněno |
| **Vyhledávání, filtrování a vizualizace dat**  |
| Systém musí být schopen okamžitého (v řádu vteřin) vyhledávání a vizualizace pro forenzní analýzu a podporu threat hunting bez zvláštního dotazovacího jazyka. |  |
| Jedná se o možnost okamžitě filtrovat a vyhledávat v plné historii všech uložených dat, tj. bezpečnostních událostí, síťových toků a agregovaných síťových statistikách (tabulky a grafy), a to minimálně:  |  |
| * podle parametrů IP a MAC adresa, hostname, username (identita uživatele), příchozí a odchozí provoz, síťová služba, lokální nebo vzdálená služba (služba z pohledu klient nebo server), číslo portu, VLAN, země, ASN,
 |  |
| * prostřednictvím full-textového vyhledávání v datech a vyhledávání na základě definice směru (zdroj, cíl) a logických výrazů and, or, not.
 |  |
| Systém musí pro vyhledávání poskytovat již předpočítané hodnoty výkonnostních a behaviorálních charakteristik pro každé zařízení v síti a pro všechny na něm provozované služby, bez nutnosti zpracování surových dat ze síťových logů.  |  |
| Systém musí být schopen filtrovat a vizualizovat výsledky v grafech, výčtových tabulkách s možností řazení a TOP N statistikách.  |  |
| Systém musí být schopen ukládat a následně vyhledávat aplikační metadata (vždy dotaz i odpověď všech transakcí v toku) minimálně z následujících protokolů, které jsou nebo mohou být využívány ve vnitřní síti organizace: FTP, FTP-DATA, TFTP, TFTP-DATA, SSH, Telnet, SMTP, SMTPS, DNS, DHCP, HTTP, HTTPS, NTP, SMB, SNMP, LDAP, NFS, RDP, ARP, MS-SQL, SIP, Kerberos, SSL/TLS.Metadata jsou v tomto případě chápána jako přenášená aplikační metadata nebo vlastní data servisních protokolů. U protokolu HTTP například http hlavička s metodou, URI, host, user-agent, cookies apod. V odpovědi pak návratový kód a další http parametry. |  |
| Systém umožnuje provádět uživatelsky jednoduché a okamžité vizualizace síťových prostupů mezi zařízeními a podsítěmi. Využitím uživatelského datového filtru lze vizualizační pohledy libovolně modifikovat. |  |
| **Kontextuální informace** |
| Systém musí být schopen pro každé zařízení získávat, vizualizovat a v jednom grafickém pohledu zobrazovat kontextuální informace:  |  |
| * jméno uživatele a další jeho parametry z doménového řadiče (MS Active Directory), včetně její historie
 |  |
| * hostname zařízení a jeho historie na základě zpracování relevantních dat z DNS a DHCP provozu
 |  |
| * IP geolokace
 |  |
| * IP reputace, vč. údaje, jestli je IP adresa na blacklistu nebo podezřelá
 |  |
| * historie použitých MAC adresa a výrobce zařízení
 |  |
| * operační systém a jeho historie na zařízení
 |  |
| * uživatelem zadané poznámky a informace k zařízení
 |  |
| * automaticky přiřazené značky/tagy zařízení, které popisují jejich účel a chování – alespoň server doménového řadiče, webový server, poštovní server, server DNS, server SSH, databázový server, tiskárna, administrátorské zařízení, datové úložiště, aktivní dohledy, skenery zranitelností a technologické systémy.
 |  |
| * seznam provozovaných a využívaných služeb (klient a server) u daného zařízení a množství na nich přenesených dat.
 |  |
| * seznam detekovaných bezpečnostních a provozních událostí daného zařízení.
 |  |
| **Zaznamenávání, ukládání a zpětná analýza plného provozu** |  |
| Je požadováno volitelné nahrávání plného síťového provozu (full packet capture) ve formátu PCAP na všech dodaných zařízeních minimálně na základě parametrů: cílová a zdrojová IP/MAC adresa, podsíť, využitý protokol, IPv4 nebo IPv6. Zaznamenávání je možno zapínat automaticky dle detekovaných událostí, nebo uživatelskou aktivací. |  |
| Je požadována schopnost importu vlastního PCAP souboru prostřednictvím webového rozhraní a jeho zpětná analýza všemi detekčními a analytickými prostředky kolektoru. |  |
| Je požadována schopnost zobrazení plného obsahu PCAP souboru v prostředí webového rozhraní aplikace a dále pak automatizovaná analýza surových dat za účelem identifikace provozních nedostatků zachycených pouze v datovém PCAP souboru.  |  |

## Další požadované oblasti využití

|  |  |
| --- | --- |
| **Požadované funkcionality/vlastnosti**  | **Nabízené řešení splňuje/nesplňuje,** vč. vysvětlení, jak je zadání splněno |
| **Monitorování politik kybernetické bezpečnosti** |
| Systém musí umožňovat vytváření komplexních komunikačních a bezpečnostních politik, a to minimálně: |  |
| * monitorovat definovanou komunikační matici a detekovat, kdy jsou tyto matice porušeny – alespoň jaké zařízení smí komunikovat s jakým zařízením, přes jaký protokol, v jakém čase.
 |  |
| * detekce změn v síti – přinejmenším nové komunikační vektory, nová nebo změněná zařízení a podsítě, obcházení perimetru.
 |  |
| Pro účely monitorování politik kybernetické bezpečnosti musí systém poskytovat uživatelský rámec pro definování pravidel pomocí: |  |
| * uživatelem definované podsítě na základě rozsahů IP adres
 |  |
| * uživatelsky libovolně definovaných skupin zařízení
 |  |
| * automaticky přiřazené značky/tagu zařízení, které popisují jejich účel a chování – alespoň server doménového řadiče, webový server, poštovní server, server DNS, server SSH, databázový server, tiskárna, administrátorské zařízení, datové úložiště, aktivní dohledy, skenery zranitelností a technologické systémy.
 |  |
| **Management bezpečnostních událostí a incidentů**  |
| Systém musí poskytovat funkcionalitu pro reporting bezpečnostních incidentů (prohlášení identifikované události za bezpečnostní incident), včetně: |  |
| * spolupráci a sdílení informací při analýze identifikovaných bezpečnostních incidentů včetně potřebného workflow mezi jednotlivými uživateli s podporou automatizovaných oznámení o změně stavu události či přiřazení řešitele,
 |  |
| * jednoduché sdílení informací o bezpečnostních incidentech, včetně uživatelem zadaných komentářů,
 |  |
| * možnost vyhledávání a filtrování nad všemi událostmi z pohledu workflow bezpečnostního incidentů (reportovaná událost, událost v řešení, vyřešená událost, události v řešení daného uživatele apod.),
 |  |
| * možnost exportování dat do emailu, csv, pdf, syslogu a podobně,
 |  |
| * možnost exportu bezpečnostních událostí a incidentů do systémů typu ticket management třetích stran.
 |  |
| **Detekce úniku dat** |
| Systém musí být schopen detekovat přenosy citlivých souborů a dat definovaných pomocí jejich názvů, hashů, specifického binárního obsahu (vodoznaku) nebo regulárních výrazů (např. rodné číslo). |  |
| Systém musí být schopen detekovat přenosy citlivých souborů a dat alespoň u následujících protokolů: HTTP, FTP, SMTP, SMB, NFS. |  |
| V rámci historických metadat u HTTP, FTP, SMTP, SMB a NFS je požadováno ukládání informací o všech po síti přenášených souborech alespoň v rozsahu:  |  |
| * název souboru,
 |  |
| * velikost souboru,
 |  |
| * HASH souboru.
 |  |
| **Monitoring výkonu aplikací a sítě** |
| Systém v celé monitorované síti, mezi všemi zařízeními a na všech službách měří a vytváří automaticky (bez nutnosti nastavovat manuálně limitní hodnoty) model normálního chování pro výkonnostní parametry minimálně:  |  |
| * přenosová rychlost sítě,
 |  |
| * rychlost odezvy aplikace,
 |  |
| * odezva systému z pohledu uživatele.
 |  |
| Výpočet uvedených výkonnostních parametrů a automatické detekce anomálií na základě odchylky od modelu normálního chování musí být prováděna pro:  |  |
| * všechny porty a služby TCP,
 |  |
| * pro všechny kombinace služeb a zařízení.
 |  |
| Systém musí v celé monitorované síti, mezi všemi zařízeními a na všech službách měřit informace o retransmission paketech, out of order paketech, TTL, QoS a komunikaci blokované firewally. |  |
| **Monitoring cloudových služeb**  |
| Systém musí být schopen monitorovat přístupy zařízení a uživatelů ke cloudovým službám, a to minimálně Google Workspace a Microsoft Office 365, vč. monitoringu operací se soubory, změn oprávnění a nastavení a neúspěšných přístupů. |  |
| Systém musí být schopen tyto informace autonomně a průběžně získávat z aplikačních rozhraní těchto cloudových služeb bez nutnosti využití řešení třetích stran. |  |
| **Inventarizace sítě a grafická vizualizace topologie** |
| Systém musí být schopen zobrazit celý inventář monitorované sítě s počtem zařízení v jednotlivých lokalitách, segmentech, nebo podsítích. Včetně detailního přehledu zařízení.  |  |
| Systém musí být schopen graficky vykreslit celou topologii sítě, dle zaznamenané komunikace.  |  |
| Systém musí být schopen zobrazit inventář jednotlivých lokalit, přehledy zařízení, přehledy výrobců, tagy zřízení, uživatele.  |  |
| Systém umožňuje všechny inventarizační informace řadit dle různých parametrů.  |  |

**Implementační služby**

Všechna dodavatelem instalovaná zařízení budou zabezpečena a nebudou obsahovat zjevná rizika a zranitelnosti, a to po celou dobu provozu služby.

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

**Produktová podpora výrobce**

Dodavatel musí zajistit:

* softwarovou produktovou podporu řešení v délce 60 měsíců od podepsání akceptačního protokolu po předáním monitorovacího systému.
* záruku na veškerá dodaná HW zařízení minimálně v rozsahu 5 let NBD ode dne akceptace (Next Business Day) On-Site.

**Administrátorské školení**

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

Dále je požadováno opakované proškolení uživatelů jednou ročně v rozsahu minimálně 1MD, včetně revize analýzy bezpečnostních událostí ve všech lokalitách.

4 - NAS

|  |  |
| --- | --- |
| **Parametr** | **Minimální požadavek** |
| Výrobce a model | **[bude doplněno dodavatelem]** |
| Parametry | * NAS, rackmount provedení včetně lyžin
* Čtyřjádrový procesor v architektuře x86 64 bit
* Systémová paměť 8 GB DDR4 2666 MHz, rozšiřitelná do 32GB
* Pozice pro diskové jednotky
	+ 12 x 3,5" nebo 2,5" SATA HDD/SSD
* Kompatibilita diskových jednotek
	+ 3,5" SATA jednotky pevných disků
	+ 2,5" SATA SSD
* Diskové jednotky vyměnitelné za provozu
* Min.2x Gigabitový Ethernet port (RJ45)
* 2x 10GbE Base-T (RJ45)
* 2x pozice pro M.2 SSD NVMe, Podporovaný rozměr: 22110 / 2280
* 2x disk SSD M.2 800GB, TWB 1022TB, stejný výrobce jako NAS
* USB port
	+ 2x USB 3.0
* Disky:
	+ 4x16T HDD stejný výrobce jako NAS a určen pro provoz v NAS
	+ rozhraní SATA III (6 Gb/s),
	+ rychlost 7 200 ot./min.
* Záruka 5LET NBD
 |
| *Další informace či odkazy dodavatele k nabízenému plnění* *(nepovinné pole)* |  |

### 5) nástroj pro ochranu koncových stanic

### Ochrana koncových stanic a SVR

## Specifikace pokročilé ochrany koncových bodů včetně ochrany virtualizačních platforem a EDR.

Zadavatel požaduje zabezpečit komplexně všechny koncové body, včetně fyzických PC s OS Windows, Mac a Linux, virtuálních PC (VDI) s OS Windows a Linux, fyzických serverů s OS Windows a Linux, virtuálních serverů s OS Windows a Linux s možností rozšíření ochrany pro mobilních zařízení. Požadovaný počet licencí je 150.

# Základní požadavky na řešení

Řešení pro komplexní ochranu PC, Linux, Mac, fyzické a virtuální serverové infrastruktury musí být spravováno z jedné webové konzole. Výrobce nesměl získat na av-comparatives (https://www.av-comparatives.org/awards/) za poslední 2 roky ani jednou méně než 3 hvězdy v kategorii „Real World Protection“ u firemních řešení.

Detailní požadavky na správu a funkcionalitu naleznete podle kategorií a funkcí níže.

Následující funkce jsou bezvýhradně nutné k splnění podmínek výběrového řízení:

### Konzole pro centrální správu řešení:

|  |  |  |
| --- | --- | --- |
| Požadovaná funkce | Splňuje ANO/NE | Popis, jak je řešeno (volitelné) |
| 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 zmigrovat 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 |  |  |
| **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 se strukturami Microsoft Active Directory za účelem správy ochrany zařízení v těchto inventářích. |  |  |
| Řešení musí být schopno odhalit stroje, které nejsou vedeny v 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) či dle OU, ve které se nachází v 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 |  |  |
| **Uživatelé**  |  |  |
| Více předdefinovaných rolí:Root, administrátor, reportér1. 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: mimo jiné 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 |  |  |

### Vlastnosti a funkce ochrany fyzických koncových bodů (Windows, Mac, Linux):

|  |  |  |
| --- | --- | --- |
| Požadovaná funkce | Splňuje ANO/NE | Popis, jak je řešeno (volitelné) |
| Podpora operačních systémů:Windows 10 1507 a vyššíWindows 8.1Windows 8Windows 7Windows 10 IoT EnterpriseWindows Embedded 8.1 IndustryWindows Embedded 8 StandardWindows Embedded Standard 7Windows Embedded Compact 7Windows Embedded POSReady 7Windows Embedded Enterprise 7Windows Server 2019Windows Server 2019 CoreWindows Server 2016Windows Server 2016 CoreWindows Server 2012 R2Windows Server 2012Windows Small Business Server 2011Windows Server 2008 R2Ubuntu 14.04 LTS a vyššíRed Hat Enterprise LinuxCentOS 6.0 a vyššíSUSE Linux Enterprise Server 11 SP4 a vyššíOpenSUSELeap 42.xFedora 25 a vyššíDebian 8.0 a vyššíOracle Linux 6.3 a vyššíAmazon Linux AMI 2016.09 a vyššíMac OS X El Capitan (10.11) a vyšší |  |  |
| 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, apod.) |  |  |
| 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 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) |  |  |
| Řešení umožňuje ukládat data o bezpečnostních incidentech až 90 dní |  |  |
| Možnost prověřovat http provoz |  |  |
| Možnost prověřovat provoz šifrovaný pomocí SSL |  |  |
| Možnost nastavení hesla pro odinstalování EPP klientské aplikace z koncových stanic |  |  |
| 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 |  |  |
| Možnost rozšíření o správu patchů aplikací třetích stran |  |  |
| Možnost rozšíření o správu šifrování pevných disků |  |  |
| Všechny vrstvy ochrany implementovány do jedné aplikace (tzn. není nutnost instalovat více než jednu aplikaci) |  |  |
| **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)
 |  |  |

### Ochrana virtualizovaných koncových bodů (Windows, Linux)

|  |  |  |
| --- | --- | --- |
| Požadovaná funkce | Splňuje ANO/NE | Popis, jak je řešeno (volitelné)  |
| Produkt nepotřebuje 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, apod.) |  |  |
| 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 |  |  |
| 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) |  |  |
| Podpora 60 měsíců |  |  |
| Akceptační podmínky:* Veškeré komponenty systému jsou řádně licencované
* Bylo dodáno zařízení dle požadované technické specifikace
* Všechny komponenty systému jsou nainstalovány a napojeny na infrastrukturu zadavatele.
* Byla vytvořena a dodána provozní dokumentace.
* Bylo provedeno školení v požadovaném rozsahu
 |  |  |
| **Produkty, které dodavatel dodává v rámci plnění zadavateli, musí splňovat následující podmínky** * jsou nové, byly oprávněně uvedeny na trh v EU nebo pochází z autorizovaného prodejního kanálu výrobce,
* mají plnou záruku od výrobce,
* mohou být podporovány výrobcem a mohou být součástí servisního a podpůrného programu výrobce,
* obsahují všechny nezbytné licence na používání příslušného softwaru,
* jsou v databázi výrobce uvedeny jako prodaná kupujícímu a určeny pro tento konkrétní projekt
* jsou určeny pro provoz v České republice.
* Tyto skutečnosti dodavatel doloží potvrzením výrobce nebo oficiálního distributora tohoto zařízení
 |  |  |

6) nástroj pro ověřování identity uživatelů

|  |  |
| --- | --- |
| **Parametr** | **Minimální požadavek** |
| Výrobce a model | **[bude doplněno dodavatelem]** |
| Parametry | * Trvalá licence pro mobilní platformy (Android, IOS)
* Podpora stávajícího firewallu FortiGate 60F
* Plná integrace s uvedeným Firewalem
* Licence použitelná pro realizaci 2FA pro přihlášení minimálně na VPN
* Podpora time-based i event-based autentifikačních tokenů
* Push notifikace
* Licence pro 100 koncových uživatelů
 |
| Další informace či odkazy dodavatele k nabízenému plnění (nepovinné pole) |  |

### 7) nástroj pro ochranu a zabezpečení e-mailů

|  |  |
| --- | --- |
| **Parametr** | **Minimální požadavek** |
| Výrobce a model | **[bude doplněno dodavatelem]** |
| Parametry | * Řešení na ochranu emailové komunikace (bezpečná emailová brána) fungující jako VM appliance (proprietární operační systém výrobce včetně všech funkcí) v prostředí Vmware/HyperV/KVM. Řešení HW appliance, anebo jako software není přípustné. Součástí musí být podpora výrobce v režimu 24x7 zahrnující aktualizaci a udržování všech požadovaných funkcí, technickou podporu, to vše po dobu 5 let
* Podpora až 4 sítových rozhraní v rámci síťového prostředí hypervisoru
* VM appliance alokuje min. 1 vCPU
* VM appliance alokuje min. 4 GB paměti
* VM appliance alokuje min. 2 TB diskového prostoru
* Možnost nasazení v režimu MTA gateway nebo transparetní režim
* Možnost nasazení v režimu vysoké dostupnosti (včetně sdílení fronty) pro budoucí rozšíření
* Obousměrná a výrobcem podporovaná integrace s dalšími nabízenými bezpečnostními prvky (NG Firewall, sandbox) za účelem sdílení provozně telemetrických informací a informací o odhalených hrozbách (škodlivém kódu) sandboxovací technikou.
* Ochrana proti škodlivému kódu, nevyžádané elektronické poště a uniku citlivých dat
* Podpora víceúrovňové detekce nevyžádané pošty (IP, domény, reputační databáze, ověření příjemce, DMARC, SPF, DKIM, proprietární funkce rozpoznávání nevyžádané pošty technikou výrobce, vyhledávání a kategorizace URI/URL, vyhledávání klíčových slov, behaviorální analýza)
* reakce na detekovaný spam minimálně: přidání tagu, přidání hlavičky, přeposlání emailu na jiný SMTP server, odmítnutí (reject), zahození (discard), uložení do karantény, přepsání adresy příjemce
* Možnost limitace v rámci SMTP navázané relace (počet zpráv od jednoho klienta za určitou dobu, maximální počet spojení od jednoho klienta za určitou dobu, podpora endpoint reputace, napojení na LDAP za účelem verifikace uživatelů; možnost omezení počtu HELO/EHLO v rámci jedné SMTP relace, možnost omezit počet emailových zpráv v rámci SMTP relace, možnost omezit počet příjemců v rámci adresátů emailu, možnost manipulace s hlavičkou mailu (odstranění Received hlavičky)
* Antivirová kontrola (antimalware, funkce ochrany proti rychle se šířícím kampaním škodlivého kódu, heuristická funkce detekce škodlivého kódu, detekce dalších variant škodlivého kódu, odstranění aktivního obsahu PDF a kancelářských dokumentů, karanténa, odstranění škodlivých odkazů z emailů, AV kontrola musí být plně integrována s platformou Sandbox (viz níže), umožňující pokročilou ochranu před pokročilými typy hrozeb včetně tzv. zero- day útoků. Na rozdíl od firewallu tato integrace musí být v režimu pozdržení emailu ve frontě až do konce analýzy na sandboxu, sdílení signatur dynamicky vytvářených na platformě sandbox
* Podpora IPv6
* Podpora VLAN
* Plnohodnotná integrace s LOG serverem a SIEM platformou.
* Plnohodnotná integrace se síťovým dohledem (podpora SNMP (v2c, v3) včetně dostupnosti MIB souboru dodávaného výrobcem).
* Výkonové požadavky
* Propustnost min. 50 000 emailů za hodinu při průměrné velikosti email ~100 kB a prováděné kontrole na přítomnost škodlivého kódu a spamu
* Podpora ochrany minimálně 100 emailových domén
* Licenčně nezávislý model na počtu uživatelů, mailových schránek nebo IP adres (pokud jsou tyto funkce licencované, požadujeme dodání licence pro neomezený počet schránek)
* Certifikace VB verified spam +
* Certfikiace VB 100 Virus
* Certifikace ICSA labs
* Certifikace AAA SE Labs
 |
| Další informace či odkazy dodavatele k nabízenému plnění (nepovinné pole) |  |

# 8 - Dodávka a implementace nástroje pro centralizované zaznamenávání událostí z libovolných zdrojů, s možností analýzy a řešení provozních i bezpečnostních událostí/incidentů ze systémů a aplikací zadavatele.

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Minimální požadavek** |  |
| Výrobce a model | **[bude doplněno dodavatelem]** | **Splňuje Ano/Ne** |
| Základní vlastnosti | * Navrhnout, dodat a implementovat nástroj na zaznamenávání událostí. Tento nástroj bude sloužit pro sběr a analýzu logů s možností následné analýzy a řešení bezpečnostních událostí/incidentů ze systémů a aplikací zadavatele určeným hodnocením aktiv a bezpečnostních potřeb organizace. Navržený nástroj musí zachovávat originál logů za účelem bezpečnostního auditu a umožňovat splnění legislativních norem a požadavků, vyplývajících zejména z připravované vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšší povinnosti (NIS2). Nástroj proto musí být schopen zaznamenat všechny bezpečnostní a relevantní provozní události a tyto uchovat nejméně po dobu 18 měsíců. Nástroj musí být dále schopen zajistit přesné časové razítko ke všem pořízeným událostem a umožnit zachování důvěrnosti a integrity pořízených dat po celou dobu jejich životního cyklu. Pro efektivní využití musí nástroj umět generovat reporty o aktivitách systémů i uživatelů, včetně auditních reportů na vyžádání, nebo se stanovenou periodicitou s definovatelným obsahem.
* Cílem je mít jednotné úložiště logů s pokročilými nástroji analýzy a upozorňování, ke kterému budou mít přístup pouze autorizovaní pracovníci zadavatele. Nezbytnou nutností je vyloučit možnost modifikace logů ze strany administrátorů nebo uživatelů. Nástroj musí dále umožňovat snadnou klasifikaci dat, tvorbu uživatelsky definovaných parserů, filtrů, upozornění a korelací bez účasti výrobce nebo dodavatele ve snadno pochopitelném grafickém rozhraní bez nutnosti používat znalostí programátora. Dokumentace musí poskytnout jednoznačný návod, jak takovéto činnosti provádět, a to včetně široké škály vzorových příkladů.
* Zálohování konfigurace i dat a jejich obnova je nezbytnou nutností, kterou musí dodaný systém podporovat. Protože není předem známo přesné množství logů vznikajících v naší organizaci, požadujeme, aby dodaný nástroj podporoval možnost horizontálního i vertikálního rozšíření formou clusteru a dále plánované i ad-hoc zálohování vzniklých dat na externí zálohovací systém. Zálohováním dat na externí systém musí umožnit dosáhnout požadavku na délku uložení logovaných událostí po dobu minimálně 18 měsíců. Platí však, že požadujeme, aby systém umožňoval on-line zobrazit hodnoty nad všemi interně uloženými daty za libovolné časové období bez nutnosti nejprve modifikovat konfiguraci systému nebo parametry uložených dat.
* Součástí dodávky musí být úplná a podrobná dokumentace systému v češtině. Ne všichni naši administrátoři a budoucí operátoři systému dokonale ovládají angličtinu, proto požadujeme, aby součástí dodávky byla i dokumentace v českém jazyce, obsahem i kvalitou srovnatelná s aktuální dokumentací v angličtině. Proto v rámci odpovědi na výběrové řízení požadujeme předložit kompletní dokumentaci k celému systému a poznámky k vydání (release notes) k systému i všem návazným komponentům. Není přípustné předložit českou dokumentaci, která bude odkazovat do dokumentace, která bude v jiném jazyce, než je čeština. Dodaný systém plánujeme provozovat vlastními lidskými zdroji, proto by nabízený systém měl umožňovat našim pracovníkům IT provádět základní i středně pokročilé konfigurace bez nutnosti konzultovat dodavatele nebo výrobce. Nabízený nástroj proto musí splňovat očekávané parametry uživatelské přívětivosti a integrity uživatelského rozhraní a vyhnout se nutnosti používaní skriptů, maker, konfigurací v příkazové řádce nebo terminálu. Dále by dokumentace měla poskytnout jednoznačné návody, jak konfigurovat nejčastější zdrojová zařízení pro spolupráci s nabízeným systémem.
* Pokud jsou v nabízeném řešení zahrnuty jakékoliv licence, jejich legální používání nesmí být časově omezeno. Nabízené řešení tedy musí být plně funkční i po uplynutí doby placené podpory.
* V případě pochybností o vlastnostech nabízeného nástroje si vyhrazujeme právo vyžádat funkční vzorek nabízeného řešení pro ověření funkčních vlastností a provést ověřovací testy ještě před ukončením výběrového řízení. V tomto případě je dodavatel povinen dodat funkční vzorek s technickými parametry nabízeného řešení do 1 týdne od výzvy zadavatele a poskytnout součinnost s testováním. Dále si vyhrazujeme právo vyžádat kontakty alespoň na 3 referenční zákazníky z našeho sektoru pro účely zjištění zkušeností s nabízeným systémem.
 | Anno/Ne |
| Technická specifikace | Zadavatel vyžaduje, aby nabízené řešení mělo níže požadované funkce již v době podání nabídky, nikoliv aby se jednalo o budoucí funkce plánovaných verzí software pro nabízené řešení. | Ano/Ne |

|  |  |  |
| --- | --- | --- |
|  | **Obecné požadavky na systém pro centralizovanou správu logů, událostí a strojových dat** | **Splňuje** |
| 1 | Systém pracuje jako hardwarová appliance s jedním uceleným webovým rozhraním pro všechny administrátorské i operátorské činnosti. Nevyžaduje instalaci dalších systémů a aplikací, vyjma podpory sběru na pobočkách a agenta pro sběr Windows logů. Doložte katalogový list produktu (datasheet) podrobně popisující hardwarové i softwarové parametry nabízeného systému. | Ano/Ne |
| 2 | Systém provádí zpracování událostí z předdefinovaných zdrojů logů napříč výrobci aplikací, operačních systémů a síťového hardware. | Ano/Ne |
| 3 | 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. | Ano/Ne |
| 4 | Systém umožňuje dopsání parserů pro výše neuvedená zařízení 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 viz bod č. 1. Vytváření a testování parserů nesmí mít vliv na provoz systému. Pro psaní parserů nesmí být použito textové psaní programového kódu ale tzv. vizuální programování, které automaticky opravuje uživatele a upozorňuje ho na chyby. Požadujeme předložit příslušnou dokumentaci k vytváření parserů a testování jejich funkčnosti. | Ano/Ne |
| 5 | Systém umožňuje v grafickém rozhraní vizuálního programovacího jazyka snadno provádět třídění a značkování vstupních dat pro jejich další zpracování. Nepřipouští se nastavování třídění vstupních dat ve formě skriptu/makra zobrazeného v textovém okně. Předložte příslušný odkaz na dokumentaci popisující funkčnost třídění vstupních dat. | Ano/Ne |
| 6 | Systém přijímá a zpracovává logy, události a další strojově generovaná data prostřednictvím minimálně následujících protokolů: SYSLOG (dle RFC3164, RFC5424, RFC5425) a RELP. Systém musí umožňovat příjem logů i na rozsahu alespoň 50 UDP a TCP portů pro zjednodušené třídění vstupních zpráv. Dále požadujeme podporu sběru strojových dat z databází s nastavením v grafickém menu systému minimálně pro databáze MSSQL, MySQL, Oracle a PostgreSQL a to bez nutnosti instalovat na databázový server doplňkový software nebo agenta. Předložte detailní komunikační matrici s popisem všech použitých protokolů a portů pro nabízený systém a dokumentaci k nastavení sběru z databází v grafickém rozhraní systému. | Ano/Ne |
| 7 | 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 přidávájí 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. | Ano/Ne |
| 8 | Hodnoty jednotlivých parsovaných polí je možné v definici parseru přetypovat a standardizovat alespoň na tyto základní druhy: číslo, IP adresa, MAC adresa, URL. Nad uloženými čísly je pak možné při prohledávání dat provádět matematické operace (součty všech hodnot, průměry, nejmenší/největší hodnota apod.). | Ano/Ne |
| 9 | 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. | Ano/Ne |
| 10 | Všechna pole a položky přijaté systémem jsou automaticky indexovány. Nad všemi položkami je možné ihned provádět vyhledávání bez nutnosti dodatečného ručního indexování administrátorem. | Ano/Ne |
| 11 | Možnost sběru událostí minimálně ve formátech RAW, Syslog RFC5424, CEF, LEEF, JSON RFC8259. | Ano/Ne |
| 12 | 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.  | Ano/Ne |
| 13 | 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.  | Ano/Ne |
| 14 | Systém provádí konsolidaci logů na interním storage logovacího systému. | Ano/Ne |
| 15 | Systém umožňuje snadné vyhledávání událostí a okamžité vytváření grafických reportů (ad hoc) bez nutnosti dodatečného programování nebo aplikování dotazů v SQL jazyce. Reportovací nástroj musí být integrální součástí navrhovaného systému a musí se obsluhovat v jednotném rozhraní nabízeného produktu. Předložte link nebo pdf popisující způsob vytváření reportů.  | Ano/Ne |
| 16 | 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. | Ano/Ne |
| 17 | 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. | Ano/Ne |
| 18 | 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. | Ano/Ne |
| 19 | Systém podporuje nativní získávání logů z Office365/Microsoft365 prostředí bez ohledu na použitou licenci 365 prostředí a bez nutnosti instalovat dodatečné externí komponenty. Požadujeme předložit link na dokumentaci popisující nastavení systému v jednotném grafickém rozhraní tak, aby získával logy z Office365/Mircosoft365. | Ano/Ne |
| 20 | 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. | Ano/Ne |
| 21 | Systém musí umožňovat unifikované vyhledávání napříč všemi typy dat a zařízeními dle normalizovaných polí (uživatelské jméno,zdrojová IP, značka/tag apod.). | Ano/Ne |
| 22 | Systém musí mít možnost uložení uživatelem vytvořených pohledů na data (dashboardů) pro budoucí zpracování. | Ano/Ne |
| 23 | Továrně dodané pohledy na data nesmí jít administrátorem ani uživatelem systému nevratně modifikovat nebo smazat. |  Ano/Ne |
| 24 | Systém obsahuje předpřipravené pohledy na uložená data dle jednotlivých kategorií zdrojových zařízení i dle logického členění. | Ano/Ne |
| 25 | 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. | Ano/Ne |
| 26 | Konfigurační a Systémové rozhraní a dokumentace k těmto rozhraním musí být identické v anglickém i v českém jazyce. Nepřipouští se omezená dokumentace v českém jazyce nebo zjednodušená dokumentace odkazující na další dokumentaci v anglickém jazyce, případně na dokumentaci třetích stran.  | Ano/Ne |
| 27 | Požadujeme předložit link na online dokumentaci nebo připojit pdf aktuální kompletní dokumentace k ověření jednotlivých vlastností navrhovaného systému. | Ano/Ne |
| 28 | Čistá kapacita úložného prostoru (kapacita diskového pole) dostupná pro uložená data nabízeného systému musí být minimálně 12TB. | Ano/Ne |
| 29 | Požadujeme, aby ze systému bylo možné za běhu vytáhnout libovolný disk, bez ztráty dat a vlivu na funkčnost řešení.  | Ano/Ne |
| 30 |  Redundance disků nesmí ovlivňovat požadovanou kapacitu úložiště. | Ano/Ne |
| 31 | Jednotná centrální webová konzole s jednotným grafickým rozhraním pro přístup k logům, alertům, reportům a pro správu systému. Z této konzole se provádí veškerá konfigurace, správa i analýza logů. Není přípustné, aby navrhovaný systém měl více rozdílných konzolí od různých výrobců s rozdílným ovládáním nebo aby se konfigurace musela provádět mimo jednotné webové rozhraní. Požadujeme předložit dokumentaci, ze které je zřejmé, jakým způsobem je realizována konfigurace v rámci jednotné konzole.  | Ano/Ne |
| 32 | Požadujeme, aby systém umožňoval jednotné vytváření uživatelských rolí definujících přístupová práva k uloženým událostem na základě typu zdrojů a značek a k jednotlivým ovládacím komponentům systému. Připojte odkaz na dokumentaci popisující vytváření uživatelských rolí v grafickém rozhraní systému. | Ano/Ne |
| 33 | Dodaný systém musí obsahovat ucelené all-in-one řešení pro parsování a normalizaci přijatých událostí bez nutnosti dodatečné instalace externích aplikací nebo systémů. Jedinou přípustnou výjimkou je monitorování systémů Windows pomocí agentů.  | Ano/Ne |
| 34 | 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. | Ano/Ne |
|  | **Minimální HW parametry požadovaného systému** |  |
| 38 | Jedna hardwarová appliance o velikosti max. 1U, včetně lyžin umožňujících vysunutí zapnutého systému z racku pro servisní účely. | Ano/Ne |
| 39 | HW appliance obsahuje veškeré potřebné komponenty (CPU, RAM, diskový prostor) pro svoji činnost a je nezávislá na dalších systémech. | Ano/Ne |
| 40 | 1 procesor, min. 16 jader, s podporou HyperThreadingu nebo Multi-Threadingu. | Ano/Ne |
| 41 | RAM Min. 64GB DDR-4. | Ano/Ne |
| 42 | Minimálně 12TB pro integrovanou databázi podporovanou HW akcelerovaným SAS RAID řadičem. Řadič diskového pole musí obsahovat zálohovací baterii nebo být vybaven flash pamětí. | Ano/Ne |
| 43 | 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. | Ano/Ne |
| 44 | 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. | Ano/Ne |
| 45 | Ventilátory redundantní a vyměnitelné za provozu. | Ano/Ne |
| 46 | Napájecí zdroje redundantní a vyměnitelné za chodu (hotplug). | Ano/Ne |
| 47 | Virtuální KVM (tj. převzetí textové i grafické konzole serveru a zajištění přenosu povelů z klávesnice a myši vzdáleného počítače. | Ano/Ne |
| 48 | Systém pro vzdálenou správu serveru včetně potřebné licence, pokud je třeba (obdoba HP iLO, Dell iDRAC apod). | Ano/Ne |
|  | **Výkonnostní a SW parametry systému** |  |
| 49 | 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). | Ano/Ne |
| 50 | Aktualizace systému jsou distribuovány v jednotném balíku a jejich instalace je prováděna uživatelsky přes centrální webovou správcovskou konzoli. Všechny aktualizace musí být prováděny z webového prostředí bez potřeby asistence dodavatele/výrobce dodávaného systému. Požadujeme předložení posledních 4 poznámek k novému vydání (release notes) pro kontrolu parametrů navrhovaného systému.  | Ano/Ne |
| 51 | Systém musí podporovat downgrade v jednom kroku, pro případ problémů s novou verzí systému po upgrade. Není přípustný downgrade pouze za součinnosti výrobce. Popište podrobně způsob realizace downgrade, nebo přiložte odkaz na dokumentaci s detailním popisem. | Ano/Ne |
| 52 | 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.  | Ano/Ne |
| 53 | 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. | Ano/Ne |
| 54 | 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. | Ano/Ne |
| 55 | Uživatelská konfigurace klasifikace dat, parserů, filtrů a alertů se provádí pomocí vizuálního programovacího jazyka v centrální správcovské webové konzoli. Vizuální programovací jazyk musí uživateli umožnit psát konfigurace bez nutnosti znalosti programování (např. Node-RED, Microsoft VPL, Blockly apod). Vizuální programovací jazyk není prezentován textově, ale graficky formou schémat-symbolů, které reprezentují aplikační logiku a kontrolují syntaxi. Doložte odkazem na dokumentaci systém vizuálního programování a popisu jednotlivých použítých komponent vizuálního programování nástroje.  | Ano/Ne |
| 56 | Konfigurace uživatelských parserů musí umožňovat automatické doplňování DNS reverzních záznamů, čísel a jmen autonomních sítí, geolokační informace a identifikace výrobce zařízení podle MAC adresy. | Ano/Ne |
| 57 | Možnost on-line ladění uživatelsky definovaných parserů - při jejich vytváření je možné vložit skupinu testovacích zpráv, při změně je okamžitě zobrazena výsledná podoba rozparsovaných dat a případná chybová hlášení s upozorněním na chybná místa vytvářeného parseru. Pro snadnější vytváření parserů požadujeme mít možnost vložení minimálně 20 testovacích zpráv současně. Doložte odkazem na dokumentaci, ze které je zřejmé, jakým způsobem se vkládají testovací zprávy během psaní nového uživatelského parseru a jakým způsobem je prezentován výstup testu. | Ano/Ne |
| 58 | V centrální správcovské konzoli je možné přidávat k jednotlivým zdrojům dat, aplikacím, zařízením nebo IP subnetům tzv. značky, označující například umístění zařízení, typ zařízení, kritičnost zařízení apod. Systém obsahuje předdefinované značky, které automaticky přidává k přijímaným zprávám. Příklady značek: konfigurační změna, úspešné ověření uživatele, neúspěšné ověření uživatele, zpráva přišla z windows, zpráva byla vygenerována firewallem atd... | Ano/Ne |
| 59 | Všechny přidávané značky jsou ukládány s každou přijatou událostí, na základě značky je možné filtrovat data nebo omezovat oprávnění uživatelů systému k jednotlivým událostem. | Ano/Ne |
| 60 | Pro budoucí nasazení ve vysoké dostupnosti a výkonnostní rozšíření je vyžadována podpora sestavení ve vysoké dostupnosti – požadujeme podporu minimálně 4 nodů v clusteru. Nastavení clusteru se musí kompletně realizovat v grafickém rozhraní správcovské konzole v jednom kroku, není přípustné konfigurovat sestavení scripty, makry nebo úpravou textové konfigurace systému a pomocí ručních restartů služeb. Systém ve vysoké dostupnosti musí přehledně informovat o stavu clusteru a procesu synchronizace databází. Dokumentace k realizaci vysoké dostupnosti musí být kompletní a popisovat všechny kroky sestavování a obnovení v případě výpadku komponenty clusteru. Doložte odkazem na dokumentaci, jakým způsobem se cluster vytváří a jakým způsobem se provádí obnovení po možném výpadku jednotlivých zúčastněných komponent. | Ano/Ne |
| 61 | Vícenodový cluster se chová i ovládá jako jednotný systém, nutnost nezávislé konfigurace na každé jednotce v clusteru je vyloučena. Vícenodový cluster umožnuje geolokační oddělení a pro komunikaci v rámci clusteru musí využívat definovaný TCP/UDP port pro snadné nastavení prostupy firewallu. Veškerá komunikace v rámci clusteru musí být šifrovaná s vysokým kryptografickým standardem pro bezpečné vytvoření privátní virtuální sítě na síťové vrstvě. Popište použitou technologii zabezpečení komunikace v rámci clusteru.  | Ano/Ne |
| 62 | V případě využití více nodů v clusteru se automaticky zrychluje zpracování vstupních dat a vyhledávání v již uložených datech. | Ano/Ne |
| 63 | V případě rozšíření systému na cluster musí navrhovaný systém zajistit bezvýpadkovost sběru logů. | Ano/Ne |
| 64 | 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. | Ano/Ne |
| 65 | Podpora zálohování nebo obnovení konfigurace v jednom kroku a jednom souboru pro celý systém. Doložte odkazem na dokumentaci, jakým způsobem se provádí zálohování a obnova konfigurace systému.  | Ano/Ne |
| 66 | Podpora důvěryhodného zálohování dat na externí systém. Požadováno plánované i ad-hoc zálohování. Zálohy dat musejí být vhodně kompresovány a umožnit v budoucnosti obnovení bez ohledu na verzi systému, ve které byla záloha pořízena. Doložte odkazem na dokumentaci, jakým způsobem se realizuje zálohování a obnova záloh.  | Ano/Ne |
|  | **Alerty** |  |
| 67 | Systém je schopen na základě uživatelsky zadaných podmínek splněných v přijatých datech vygenerovat alert. | Ano/Ne |
| 68 | Text emailu vygenerovaného alertem musí být uživatelsky definovatelný s proměnnými, které jsou vyplněny z přijaté rozparsované události. | Ano/Ne |
| 69 | Systém musí obsahovat výrobcem předpřipravené sety/vzory alertů a korelací. | Ano/Ne |
| 70 | Systém musí provádět konfigurace alertů a korelací pomocí vizuálního programovacího jazyka. Vizuální programovací jazyk není prezentován čistě textově, ale textově-grafickou formou, která vizualizuje aplikační logiku vytvářeného alertu. Konfigurace alertů musí umožňovat okamžitou kontrolu funkčnosti výstupu alertu nebo korelace vložením příslušné testovací zprávy, včetně zobrazení upozornění na případné uživatelské chyby. Doložte odkazem na dokumentaci, jakým způsobem realizujete konfiguraci a testovaní alertů a korelací. | Ano/Ne |
| 71 | Jako výstupní pravidlo Alertu musí systém umět odeslat událost, která alert vyvolala, na externí systém minimálně prostřednictvím SMTP nebo Syslogu přes TCP protokol. U Syslog protokolu požadujeme možnost definice formátu odesílaných dat pro snazší integraci se systémy třetích stran. Doložte odkazem na dokumentaci, jakým způsobem se zpráva, která vyvolala spuštění alertu, odesílá na externí systém a jak se definuje formát odesílání dat.  | Ano/Ne |
| 72 | V alertech je možné nejen využívat, ale i přiřazovat značky (příklad: pošli alert jen v případě, že se událost stala na kritickém serveru a je označen názvem lokality, nebo pokud událost obsahuje podmínku, přiřaď novou značku). Doložte odkazem na dokumentaci, jakým způsobem lze v jednotném grafickém rozhraní systému definovat a přiřazovat značky. | Ano/Ne |
| 73 | 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. | Ano/Ne |
|  | **Sběr událostí z Microsoft prostředí** |  |
| 74 | Události z Microsoft prostředí jsou vyčítány pomocí agenta instalovaného přímo v koncových systémech. Windows agent musí současně podporovat jak monitoring interních windows logů, tak monitoring textových souborových logů. Agent se nesmí instalovat individuálně, ale prostřednictvím MS AD Group Policy a nesmí vyžadovat žádnou konfiguraci na cílovém systému. Doložte odkaz na dokumentaci popisující požadované vlastnosti integrovaného Windows agenta. | Ano/Ne |
| 75 | Agent sběru z Microsoft podporuje globální i lokální nastavení filtrace odesílaných událostí pomocí centrální správcovské konzole. Například, zašli pouze logy z adresářů eventview Systém, Security, Sysmon a Terminal Services a zahoď logy s EventId 7036. | Ano/Ne |
| 76 | Filtrace odesílaných událostí agenty se konfiguruje pomocí vizuálního programovacího jazyka z centrální správcovské konzole systému. Logy nastavené k filtraci jsou filtrovány na straně windows agenta a nejsou nijak odesílány po síti. Vizuální programovací jazyk není prezentován textově, ale textově-grafickou formou, která vizualizuje aplikační logiku vytvářeného alertu. Doložte odkazem na dokumentaci, jakým způsobem se vytváří a přiřazují filtry pro Windows agenty pro sběr logů a jakým způsobem se testuje účinnost filtru.  | Ano/Ne |
| 77 | 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.  | Ano/Ne |
| 78 | Komunikace Windows agenta a centrálního systému musí být zabezpečena TLS 1.2 a výše a musí podporovat ověřování certifikátem. | Ano/Ne |
| 79 | Windows agent podporuje sběr nejen ze základních systémových logů (Aplikace, Zabezpečení, Instalace, Systém), ale je možné z centrální konzole v grafickém rozhraní nastavit i sběr všech ostatních logů ve složce Protokoly aplikací a služeb a logy rozšířené Sysmonem. Dále musí Windows agent podporovat centralizované nastavení z administrátorské konzole systému pro sběr textových logů včetně možnosti výběru jejich formátu. Doložte odkazem na dokumentaci, jakým způsobem se nastavují parametry sběru logů globálně a jakým způsobem u konkrétního agenta.  | Ano/Ne |
| 80 | 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 **200** na dobu předpokládané morální životnosti produktu – 7 let. Předpokládáme instalaci agentů na všechny systémy současně, proto je nutné potvrdit zda systém výkonnostně splňuje tento požadavek. Jedná se o klíčovou funkci, proto budeme před uzavřením smlouvy požadovat předvedení požadovaných funkcí, stability i výkonnostní kapacity nabízeného systému pro sběr logů z prostředí Microsoft. | Ano/Ne |
|  | **Podpora pro sběr událostí z poboček** |  |
| 81 | Systém musí podporovat centrálně spravované řešení, které sbírá události na pobočkách a umožní jejich odeslání po saturované lince bez ztráty dat. Doložte odkazem na dokumentaci, jakým způsobem realizujete sběr událostí z poboček. | Ano/Ne |
| 82 | 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. | Ano/Ne |
| 83 | 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.  | Ano/Ne |
| 84 | Řešení musí komunikovat po definovaném TCP/UDP portu, aby mohl být snadno nastaven prostup přes firewally a řešena kvalita služby (QoS) pro přenos událostí. Doložte odkazem na dokumentaci, jak vypadá komunikační matice pro připojení rešení pro sběr událostí na pobočkách.  | Ano/Ne |
| 85 | Řešení musí poskytovat kapacitu vyrovnávací paměti pro minimálně 100GB událostí, které na pobočce mohou vzniknout během výpadku spojení mezi pobočkou a datovým centrem. | Ano/Ne |
| 86 | Řešení pro sběr dat z poboček musí mít výkon minimálně 5 tisíc událostí/s, a to i v trvalé zátěži. | Ano/Ne |
| 87 | Řešení musí poskytnout podporu pro sběr událostí na identických UDP i TCP portech jako hlavní dodaný systém. | Ano/Ne |
| 88 | Řešení musí být k dispozici jako fyzický systém nebo jako virtuální systém pro VMware ESXi a Hyper-V. | Ano/Ne |
| 89 | Řešení musí být schopno komunikovat z pobočky na centrálu i přes vícenásobný překlad adres (NAT). | Ano/Ne |
|  | **Vysoká dostupnost, SW Podpora a záruka na hardware** |  |
| 90 | Požadujeme volitelnou podporu pro nasazení ve vysoké dostupnosti. | Ano/Ne |
| 91 | HW - Požadovaná minimálně 5letá servisní podpora na hardware appliance s opravou v místě instalace serveru a s garantovanou odezvou následující pracovní den od nahlášení případné závady. | Ano/Ne |
| 92 | Systém musí podporovat vygenerování TSR (technického support reportu) pro možnost diagnostiky bez vzdáleného přístupu.  | Ano/Ne |
| 93 | SW - Podpora výrobce na aktualizaci systému a parserů na **5 let.** Podpora musí obsahovat aktualizaci SW minimálně 4x ročně, opravy chyb a telefonickou a emailovou podporu s diagnostikou vzdáleným přístupem.  | Ano/Ne |

|  |  |
| --- | --- |
| Akceptační podmínky | * Veškeré komponenty systému jsou řádně licencované
* Bylo dodáno fyzické zařízení dle požadované technické specifikace.
* Všechny HW i SW komponenty systému jsou nainstalovány a napojeny na infrastrukturu zadavatele.
* Byla vytvořena a dodána provozní dokumentace.
* Bylo provedeno školení v požadovaném rozsahu
 |

9 Ochrana počítačové sítě před malwarem a zneužíváním zařízení na úrovni DNS překladu, řešení poskytujícího plnou kontrolu nad DNS provozem.

|  |  |
| --- | --- |
| **Parametr** | **Minimální požadavek** |
| Výrobce a model | **[bude doplněno dodavatelem]** |
| Základní vlastnosti | * Produkt poskytuje ochranu na úrovni DNS proti:
* Malware
* Detekce Zero-day pomocí generátoru domén (DGA)
	+ Homografické phishingové útoky
	+ Komunikace C&C
	+ Exploit, Backdoor, Trojan, Keyloggerům
	+ Spamu
	+ Škodlivému coinminingu
	+ DNS tunnelingu
	+ DNS cache poisoningu
	+ DNS rebinding útokům
	+ Detekce anomálií DNS a upozorňování na ně
* Nevyžaduje modifikaci na koncových stanicích
* Není třeba instalovat SW na koncové stanice
* Bez nutnosti ruční rekonfigurace, vše musí být provedeno automaticky
* Není třeba instalovat certifikáty ani resetovat bezpečnostní politiky
 |
| Dodavatel stručně popíše způsob naplnění jednotlivých požadavků základních vlastností |  |
| Požadavky na administrační portál | * Webové rozhraní pro správce je plně přístupné prostřednictvím moderních webových prohlížečů bez nutnosti instalace doplňků nebo místního softwaru potřebného pro přístup k rozhraní.
* Možnost aktivovat dvoufaktorovou autentizaci a vynutit jo pro všechny správce v organizaci
* Možnost omezit přístup k rozhraní správce pouze z místní sítě nebo z definovaných veřejných IP rozsahů
* Různá nastavení autorizace (pro jednotlivé skupiny) dostupná pro operátory v minimálně 2 rolích:
* Administrátor
* Uživatel s právy pouze pro čtení
* K dispozici je log provozu DNS ze všech resolverů s možností fulltextového filtrování v rozhraní.
* Podrobnosti o všech unikátních požadavcích/odpovědích budou přístupné a exportovatelné pro další analýzu ve formátu csv
* Webové rozhraní poskytuje přístup ke následujícím funkcím:
* Analýza hrozeb
* Analýza provozu DNS
* Analýza content filteringu
* Konfigurace nastavení filtrace a bezpečnostních politik:

ZKonfigurace bezpečnostních politik* + Konfigurace blokace regulatorních feedů
	+ možnost vytváření vlastních whitelistů a blacklistů
	+ Konfigurace white-label blokačních stránek
	+ Konfigurace nastavení resolveru
* Správa DNS resolveru:
	+ Přehled resolverů
	+ Přiřazení bezpečnostních politik konkrétním rozsahům IP adres
	+ Možnosti upgradu / aktualizace verze resolveru
	+ Možnosti pokročilé konfigurace
	+ Procházení auditních logů o aktivitách uživatelů v portálu
* Alerting
 |
| Dodavatel stručně popíše způsob naplnění jednotlivých požadavků na administrační portál |  |
| Požadavky na další funkce a komponenty | * **On-premise řešení:**
* Plně autonomní DNS resolver s bezpečnostní vrstvou, která provádí filtraci a překlad DNS bez nutnosti komunikace s externí službou v cloudu.
* V souladu se standardy RFC
* Bezpečnostní vrstva umožňuje přesměrování požadavků u nebezpečných domén na blokační stránku.
* Vyžaduje DNSSEC validaci včetně negativního ukládání do mezipaměti NSEC3
* Změny konfigurace a aktualizace resolveru jsou prováděny za plného provozu - bez výpadku služby a bez výpadku provozu DNS, během aktualizací a rekonfigurací
* Podpora DNS přes TLS (DoT) a DNS přes HTTPS (DoH)
* **Blokační stránka:**
* Webová stránka, na kterou je uživatel přesměrován, když se on nebo jeho zařízení pokusí o přístup k inkriminované webové stránce.
* Blokační stránku lze libovolně upravit podle přání zákazníka tak, aby respektovala firemní identitu a vizuální stránku (písmo, barvy, logo, kontakty)
* Funkce „ByPass“ pro definované sítě - uživatel může pokračovat na cílovou doménu, aniž by vyžadoval spolupráci správce (např. pro sítě hostů).
* **Správa provozu DNS a brány firewall:**
* Konkrétní zóny lze přesměrovat na vybrané IP adresy
* Požadavky na interní domény lze přesměrovat na řadiče domén nebo jiné autoritativní servery.
* Přednačítání mezipaměti DNS - záznamy v mezipaměti jsou obnovovány před vypršením jejich platnosti.
* Záznamy DNS jsou uchovávány v paměti déle, než by autoritativní nameservery pro danou zónu měly být nedostupné z důvodu ttl periody (např. doména.com je nedostupná po dobu jedné hodiny, resolver bude moci použít poslední odpověď, kterou pro tuto doménu měl).
* DNS firewall - možnost definovat pravidla přístupu pro konkrétní domény - povolení přístupu pouze k vybraným doménám v rámci jedné IP podsítě. Příklad použití - povolení přístupu klientských počítačů pouze k doménám Office365, ostatním vracet odpověď NXDOMAIN.
* Automatická aktualizace seznamu domén Office365 a dalších služeb Microsoft Azure používaných v bráně firewall DNS.
* **Centrální management:**
* Zobrazuje provoz DNS v reálném čase
* Možnost vyloučit určité domény z logování (např. interní domény z důvodu dodržování předpisů).
* Poskytuje a provádí:
	+ Aktualizace databáze na základě filtrování zabezpečení
	+ správu aktualizací resolveru a softwaru
	+ Centrální úložiště protokolů a incidentů a poskytuje možnosti jejich vyhodnocení.
* Protokoly o provozu DNS včetně podrobností o všech unikátních požadavcích/odpovědích pro další analýzu jsou přístupné a exportované ze všech resolverů ve společnosti a dostupné včetně fulltextového filtrování v jednom rozhraní (např. ve formátu csv)
* Možnost analyzovat doménu z hlediska bezpečnosti a obsahu, včetně integrace s bezpečnostními službami třetích stran.
* Upozornění upozorňující na anomálie zjištěné v provozu DNS pomocí:
	+ e-mailu
	+ Syslog (TLS)
	+ Slack
	+ REST API
* Přehled provozu DNS umožňuje komplexní analýzu komunikace DNS, včetně podrobné:
	+ Drilldown jednotlivých událostí
	+ filtrování
	+ fulltextové vyhledávání
	+ export dat
	+ přehled trendů v provozu
 |
| Dodavatel stručně popíše způsob naplnění jednotlivých požadavků na další funkce a komponenty |  |
| Požadavky na Threat intelligence engine | * Pro uživatele má nulovou latenci. Vyhodnocení bezpečnosti je poskytováno v reálném čase bez požadavků mimo síť.
* Nasazení softwaru bez nutnosti nasazení na speciálně upravený hardware, s možností funkce ve virtuálním prostředí.
* Ochrana proti útokům typu DNS spoofing na základě DNSSEC včetně podpory NSEC3 a negativního ukládání do mezipaměti.
* Možnost definovat různé bezpečnostní politiky a přiřazovat je idndividuálně dle CIDR anotace nebo přiřazení na základě IP adresy resolveru.
* Detekce hrozeb typu Zero-day bez nutnosti předchozí znalosti dané domény
* Detekce a upozorňování na anomálie v provozu DNS
* Možnost upozornit / zablokovat z vnitřní sítě přístup k doménám, které vypadají podobně jako definovaná doména společnosti/organizace, pro ochranu před cílenými phishingovými útoky
* Možnost blokovat přístup k doménám podle kategorie obsahu alespoň v rozsahu:
* Coinminers
* P2P připojení (např. torrenty)
* DNS přes HTTPS (DoH)
* Pornografie
* Hazardní hry
* Násilí
* Tracking
* Reklama
* Sociální sítě
	+ Hry
* Měl by zajistit ochranu proti zneužití provozu DNS k tunelování jiné komunikace v technicky platných paketech DNS a komunikaci s externími servery (zabezpečení tunelování DNS).
* Vrstva tunelování DNS proaktivně narušuje tunelování DNS na několika úrovních:
* Resolver
* Neuronová síť
* Bezpečnosntí politiky umožňují nastavení:
* Úrovně ochrany (blokace)
* Úroveně detekce (audit)
* Kategorie hrozeb, které jsou zahrnuty v konkrétních zásadách
* Vlastní blacklisty a whitelisty
* Kategorie blokovaného obsahu
 |
| Dodavatel stručně popíše způsob naplnění jednotlivých požadavků na Threat intelligence engine |  |
| DNS resolver management | * Poskytuje vzdálenou diagnostiku
* Monitorování problémů s hardwarem
* Monitorování softwaru
* Shromažďování protokolů
* Vyhodnocení latence překladu
* Aktualizace softwaru a zpětné obnovení
* Možnost okamžitého vrácení provedené aktualizace do předchozího stavu
* Místní správa
* Plný přístup k protokolům pro místní správce
* Místní rozhraní CLI

  |
| Dodavatel stručně popíše způsob naplnění jednotlivých požadavků na DNS resolver management |  |
| Požadavky na Alerting | * Konfigurovatelné filtry pro domény, sítě a akce
* Možnosti způsobu doručení alertů včetně:
* E-mail
* Syslog (TLS)
* Slack
* Webhook (REST API)
* Další místa doručení výstrah (na vyžádání)
* Alerting je založen na:
* Prahové hodnoty událostí zabezpečení a provozu DNS
* Detekce dynamických anomálií
* Whitelisty a blacklisty
 |
| Dodavatel stručně popíše způsob naplnění jednotlivých požadavků na Alerting |  |
| Požadavky na Ochranu pro zařízení mimo korporátní síť | * Součástí řešení je také aplikace instalovaná lokálně na mobilních zařízeních, která zajistí stejnou úroveň ochrany zařízení, jako by bylo v místní síti pod ochranou lokálního resolveru.
* Podporované operační systémy:
	+ Windows
	+ Android
	+ iOS
* Možnost hromadného nasazení prostřednictvím zásad skupiny na počítačích spravovaných v doméně (Active directory)
* Možnost hromadné instalace na Android / iOS prostřednictvím MDM
* Mezi podporované MDM se řadí:
	+ Microsoft Intune
	+ Sophos
	+ A další
 |
| Dodavatel stručně popíše způsob naplnění jednotlivých požadavků na Ochranu pro zařízení mimo korporátní síť |  |
| Požadavky na reporting | * Zprávy jsou doručovány e-mailem na předem definované adresy.
* Možnost nastavení periodicity (7/14/30 dní) a dne v týdnu
* Průběžné zprávy shrnují:
	+ Objemy DNS provozu
	+ Počet hrozeb podle jednotlivých kategorií
	+ Podezřelá a infikovaná klientská zařízení
	+ Převažující rodiny škodlivých kódů a škodlivých domén
 |
| Dodavatel stručně popíše způsob naplnění jednotlivých požadavků na reporting |  |
| Požadavky na ochranu domény - Identity protection | * Produkt zajišťuje ochranu identit pod vlastní doménou.
* hlášení e-mailových adres, které jsou zahrnuty do veřejně známých případů narušení bezpečnosti dat
* seznam historických úniků, v nichž figurovaly e-mailové adresy dané domény.
* sledování nových úniků a upozorňování na nové úniky
* hlášení obsahuje seznam typů citlivých údajů, které figurovaly v úniku (hesla, telefonní čísla, osobní údaje, e-mail, pohlaví, bankovní informace).
* Produkt umožňuje správu incidentů na elementární úrovni - tj. označení incidentu jako vyřešeného/řešitelného.
* Produkt obsahuje doporučení, jak daný únik citlivých údajů řešit.
 |
| Dodavatel stručně popíše způsob naplnění jednotlivých požadavků na ochranu domény - Identity protection |  |
| Požadavky na integraci | * Dostupnost rozhraní REST API pro vyhledávání informací pro
* statistiky provozu DNS
* Využití REST API požadavků pro filtrování na základě
	+ zdrojové IP adresy
	+ cílové domény
	+ Typ požadavku
	+ Typ hrozby
	+ na IP adresu odpovědi
	+ čas
* Monitoring pomocí SNMP
* Dostupné šablony pro rychlou integraci s monitoringem Zabbix nebo jiným hostitelem SNMP
* Integrace protokolu Syslog (SIEM, správa protokolů, provozní monitorování atd.)
* Konfigurovatelný datový tok prostřednictvím syslogu obsahující zjištěné hrozby
* Konfigurovatelný datový tok prostřednictvím syslogu obsahující provoz DNS
* Konfigurovatelná horní část dat prostřednictvím syslogu obsahující bloky z filtrování obsahu
* Konfigurovatelná top data prostřednictvím syslogu obsahující metriky resolveru a systému
 |
| Dodavatel stručně popíše způsob naplnění jednotlivých požadavků na integraci |  |
| Podpora | * 60 měsíců.
 |
| Akceptační podmínky | * Veškeré komponenty systému jsou řádně licencované
* Bylo dodáno zařízení dle požadované technické specifikace
* Všechny komponenty systému jsou nainstalovány a napojeny na infrastrukturu zadavatele.
* Byla vytvořena a dodána provozní dokumentace.
* Bylo provedeno školení v požadovaném rozsahu
 |
| Další informace či odkazy dodavatele k nabízenému plnění (nepovinné pole) |  |

## Implementační služby

### Obecné požadavky

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

Zajištění projektového vedení realizace předmětu plnění.

Dodávku nabízených prvků a kompletní implementaci řešení provedenou podle prováděcí dokumentace a splňující povinné parametry technického řešení, implementace musí respektovat a využívat osvědčené praktiky (tzv. Best Practice) a doporučení výrobců nabízených technologií.

Provedení školení,

Zajištění zkušebního provozu,

Provedení akceptačních testů,

Zpracování provozní dokumentace v rozsahu detailního popisu skutečného provedení a popisu činností běžné údržby a administrace systémů a činností pro spolehlivé zajištění provozu.

Předání do ostrého provozu,

Dodavatel je dále povinen zahrnout do nabídky i další související potřebné služby nutné pro úspěšnou realizaci díla.

Veškerá dokumentace musí být zhotovena výhradně v českém jazyce, bude dodána v elektronické formě ve standartních formátech (MS Office) používaných zadavatelem.

### Harmonogram realizace

Dodavatel zajistí projektové vedení po celou dobu realizace zakázky osobou odpovědnou za realizaci předmětu plnění, která bude hlavní kontaktní osobou a která bude přítomna při všech jednáních týkajících se projektu.

Zadavatel vyžaduje dodržení následujícího harmonogramu plnění – zde jsou uvedeny maximální možné lhůty pro jednotlivé kritické milníky.

|  |  |
| --- | --- |
| **HARMONOGRAM** |  |
| Aktivita | Začátek | Termín |
| Předání místa plnění | D | D |
| Zahájení projektu – úvodní projektová schůzka - detailní harmonogram včetně návaznosti implementačních prací | D | D+4 |
| Realizace předmětu plnění - implementace kyberbezpečnostních opatření | D+4 | D+24 |
| Školení administrátorů | D+24 | D+26 |
| Akceptační testy | D+26 | D+28 |
| Zahájení ostrého provozu | D+28 | - |
| jednotka = 1týden |  |  |

Dodavatel může dle svého uvážení výše uvedené maximální lhůty zkrátit

Maximální lhůty trvání nesmí dodavatel při tvorbě detailního harmonogramu prodloužit.

### Požadavky na školení

Dodavatel zajistí školení pracovníků Zadavatele – administrátorů a uživatelů – na zařízení a systémy, dodávané v rámci této veřejné zakázky, a to minimálně v rozsahu předávané provozní dokumentace.

Školení zajistí seznámení pracovníků Zadavatele se všemi podstatnými částmi díla v rozsahu potřebném pro provoz, údržbu a identifikaci nestandardních stavů systému a jejich příčin a pracovníkům bude vystaveno osvědčení o školení s uvedením rozsahu školení. Budou provedena tato školení:

Školení administrátorů – minimální rozsah školení je 8 hodin, předpokládá se účast max. 2 účastníků, školení bude probíhat v sídle Zadavatele.

Školení uživatelů – minimální rozsah školení je 6 hodin, předpokládá se účast max. 5 účastníků, školení bude probíhat v sídle Zadavatele.

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

S ohledem na pandemii COVID-19 musí být formát školení připraven jak pro prezenční výuku, tak pro možnost provedení školení elektronicky (vzdálenou formou) např. pomocí MS Teams nebo jiných elektronických prostředí pro výuku. Formát školení bude zvolen zadavatelem nejpozději týden před realizací školení, a to podle aktuálního stavu pandemie a dle doporučení relevantních orgánů (Ministerstvo zdravotnictví ČR, Hygienická stanice atp.).

### Požadavky na provedení akceptačních testů a přechod do zkušebního (testovacího) provozu

Dodavatel navrhne způsob a provedení akceptačních testů. Akceptační testy musí pro všechny komodity vždy zahrnovat minimálně:

Prokázání kompletnosti dodávky a splnění povinných i hodnocených požadavků.

Prokázání vysoké dostupnosti u řešení, která jsou takto koncipována.

Prokázání aktivací software i hardware aktivačními klíči či jinými prostředky, je-li aktivace potřebná.

Prokázání registrace / aktivace podpory hardware a software výrobce, je-li podpora součástí dodávky a její aktivace potřebná

O provedení akceptace a jejím výsledku musí být vyhotoven písemný akceptační protokol. Šablony akceptačních protokolů budou předány zadavatelem při zahájení projektu, pro zapracování dodavatelem do prováděcí dokumentace.

Dodavatel zajistí pro každou komoditu zkušební (testovací) provoz v délce minimálně 14 dnů včetně technické podpory minimálně 1 specialisty na dodané řešení s dojezdem maximálně do 2 hodin od nahlášení požadavku v pracovní den v době od 7h do 17h. Dojezd do 2 hodin od nahlášení požadavku (v rámci pracovní doby) je zásadní pro udržení provozu kritických informačních systémů v potřebném rozsahu při plnění zákonných povinností zadavatele. V případě předávání díla po částech je uchazeč povinen zajistit zkušební (testovací) provoz pro předávané části díla až do doby zahájení plného provozu díla jako celku, při dodržení minimální požadované lhůty pro zkušební provoz.

### Požadavky na dokumentaci

Dodavatel zpracuje provozní dokumentaci, která bude detailně popisovat konfiguraci zhotoveného díla a jeho vazby na stávající systémy.

Provozní dokumentace bude vycházet z prováděcí dokumentace, která bude před předáním do provozu aktualizovaná dle skutečného stavu.

Součástí provozní dokumentace bude popis úkonů doporučené údržby a specifikace intervalů jejích provádění a další dokumentaci v rozsahu stanoveném v prováděcí dokumentaci.

Dodavatel uvede do nabídky kompletní podmínky pro zajištění provozu dodaných prvků, včetně požadavků na aktualizace software (maintenance).

Zhotovitel dále dodá uživatelskou dokumentaci, která bude obsahovat minimálně základní popis práce s dodaným řešením, dále bude popisovat funkcionality řešení, a to pro potřebu řádné orientace a práce uživatele. Dokumentace musí být zhotovena v českém jazyce. Dokumentace bude dodána v elektronické podobě umožňující její zobrazení a čtení prostřednictvím běžných nástrojů typu kancelářského balíku nebo ve formátu PDF.

Zhotovitel dále dodá administrátorskou dokumentaci pro objednatele, která bude obsahovat popis správy a údržby dodaného řešení. Dokumentace musí být zhotovena v českém jazyce.

Dokumentace bude dodána v elektronické podobě umožňující její zobrazení a čtení prostřednictvím běžných nástrojů typu kancelářského balíku nebo ve formátu PDF.

## Požadavky na záruky a MAINTENANCE

Zadavatel požaduje záruku na veškeré dodané technologie v délce trvání minimálně **60 měsíců** od okamžiku předání díla, není-li u konkrétního zařízení či komponenty požadováno jinak v specifikaci ZD

Dodavatel ve své nabídce uvede ceny záruky takto:

Standardní záruka a standardní podpora běžně poskytovaná výrobcem infrastrukturní technologie na území České republiky = bude součástí pořizovací ceny zařízení (vždy však alespoň 36 měsíců, není-li výrobcem či dodavatelem poskytnuta jako standardní součást nákupu produktu záruka o délce přesahující 36 měsíců, resp. dosahující minimálně 60 měsíců).

V případě, že výrobce nebo dodavatel neposkytuje jako standardní součást nákupu produktu záruku o délce minimálně 60 měsíců, pak se rozdíl mezi jím nabízenou standardní délkou záruky pro daný produkt a zadavatelem požadovanou délkou záruky minimálně 60 měsíců považuje za nadstandardní (prodlouženou) záruku, kterou je dodavatel povinen k dodávanému produktu (včetně aktualizací software/firmware apod.) pro zadavatele zajistit. Hodnotu takto zajištěné nadstandardní (prodloužené) záruky dodavatel vyjádří v příslušné části cenové kalkulace v položce "**Nadstandardní záruky a podpory výrobců"**.

Veškeré opravy po dobu záruky budou provedeny bez dalších nákladů pro zadavatele. Veškeré komponenty, náhradní díly a práce, poskytnuté v rámci záruky budou poskytnuty bezplatně.

Hlášení záručních závad, řízení a evidence průběhu jejich řešení bude probíhat stejným způsobem a s využitím stejného helpdeskového systému jako u podpory provozu.

Dodavatel nacení i potřebnou MAINTENANCE - (software maintenance) je proces pravidelného udržování, vylepšování a opravování softwarových aplikací po jejich prvotním vývoji a nasazení. Zadavatel v rámci stanovení nabídkové ceny nacení veškerou potřebnou maintenance k řádnému provozovaní dodaného řešení. Potřebnou maintenance dodavatel nacení po dobu udržitelnosti projektu 5let. Maintenance bude dle povahy dodaného řešení pokrývat minimálně níže uvedené scénáře:

**Korekční údržba:** Oprava chyb a problémů, které se objeví po nasazení softwaru. To může zahrnovat opravy bezpečnostních zranitelností, chyb v kódu nebo jiné problémy, které ovlivňují funkčnost softwaru.

**Adaptivní údržba:** Úpravy a změny softwaru, aby zůstal kompatibilní s měnícím se prostředím. To může zahrnovat aktualizace pro nové operační systémy, hardware nebo jiné softwarové závislosti.

**Perfekcionistická údržba:** Vylepšení softwaru za účelem zvýšení jeho výkonu nebo použitelnosti. To může zahrnovat optimalizaci kódu, zlepšení uživatelského rozhraní nebo zavádění nových funkcí.

Údržba softwaru je klíčová pro zajištění, že software zůstane funkční, bezpečný a relevantní i po dlouhou dobu po jeho původním nasazení.

## Požadavky na podporu provozu

### Obecná pravidla provozu

Pro hlášení servisních požadavků zajistí dodavatel Zadavateli přístup ke svému helpdeskovému systému s on-line přístupem pro kompletní správu požadavků včetně uchování historie požadavků a jejich řešení.

Provozní doba helpdeskového systému pro zadávaní požadavků musí být 7x24x365.

Neplánované zásahy do systému, které mohou ovlivnit uživatelské prostředí, jsou uživatelům oznámeny minimálně 1 hodinu před zahájením poskytování služby nebo činnosti.

Plánované zásahy do systému, které mohou ovlivnit uživatelské prostředí, jsou uživatelům oznámeny minimálně 24 hodin před zahájením poskytování služby nebo činnosti

### Požadavky na podporu provozu

Rozsah základní technická podpory (**ZTP**):

Provádění aktualizací firmware a software dodaných produktů (nezahrnuje upgrade na nové hlavní verze software) v rozsahu **8 hodin měsíčně**. Nespotřebované hodiny v měsíci jsou převoditelné do dalších měsíců v rámci příslušného (uhrazeného) roku poskytované technické podpory. Četnost aktualizací řídí Dodavatel s ohledem na zajištění spolehlivého provozu systémů a jejich bezpečnost a kritičnost aktualizací.

Helpdeskový systém s on-line přístupem (web, e-mail) pro kompletní správu požadavků včetně uchování historie požadavků a jejich řešení.

### Způsob poskytování servisní podpory

Servisní podpora je poskytována zejména následujícím způsobem:

Prostřednictvím pracovníka dodavatele Vzdálenou správou

Prostřednictvím pracovníka dodavatele přímo na pracovišti Zadavatele

Prostřednictvím pracovníka dodavatele formou vzdálené konzultace

Dodavatel provede záznam o provedení servisní podpory, v záznamu uvede relevantní informace včetně doby poskytování servisní podpory a záznam zašle elektronicky zadavateli. Servisní služby, které jsou poskytovány vzdálenou formou, mohou být evidovány v elektronickém seznamu provedených úkonů.

Zadavatel je povinen zabezpečit v rámci své součinnosti dodavateli podmínky pro řádné plnění, zejména

- zajistit a udržovat podmínky pro Vzdálený přístup dodavatele,

- zajistit dostupnost nebo odpovídající zástup Odpovědné osoby Zadavatele, vyhrazení odpovídajících časových kapacit Odpovědné osoby Zadavatele a zajištění efektivní součinnosti odborných pracovníků Zadavatele,

- zabezpečit přítomnost kvalifikované osoby, která poskytne pracovníku dodavatele veškeré informace či přístupy potřebné k podpoře předmětného systému, resp. informace o zařízeních a programovém vybavení souvisejícím s předmětným systémem,

- umožnit dodavateli v případě nutnosti a po předchozím oznámení odstavení technických prostředků z běžného provozu,

- zajistit součinnost třetí strany, jestliže je to pro provedení služby potřebné (na výzvu takovou potřebnost písemně odůvodní).

Dodavatel je v případě potřeby též z vlastní iniciativy oprávněn požádat Zadavatele o dodatečné údaje o Incidentu a o nezbytnou součinnost Zadavatele na řešení Incidentu, bez které nelze zahájit či pokračovat v řešení Incidentu.

Zadavatel je dále v rámci součinnosti povinen

- elektronicky potvrdit dodavateli provedení služby,

- zajistit zálohování dat i programů a výměnu zálohovacích médií dle zálohovacího plánu, jejich dostupnost v případě potřeba a jejich uložení na bezpečných místech tak, aby bylo nešlo k jejich ztrátě nebo poškození,

- poskytovat potřebné nebo vyžádané informace a podklady včetně dokumentace k předmětnému systému nebo zařízení a programovému vybavení, které s ním souvisí (pokud tyto nepochází od dodavatele).

### Postup při řešení incidentů

Zadavatel bude incident oznamovat dodavateli bez zbytečného odkladu jedním ze způsobů a na kontaktních místech uvedených v Doplňku SLA, kam budou mít zajištěny přístup pověřené osoby Zadavatele (HelpDesk).

Součástí nahlášení požadavku Zadavatelem musí být:

- popis Incidentu nebo Požadavku,

- jiné relevantní upřesňující informace, včetně případných textových či obrazových příloh nezbytných pro replikaci incidentu,

- kontaktní osoba.

Dodavatelem používaný systém pro HelpDesk musí pokrýt uvedené informace pro nahlášení požadavku.

**Dodavatel zahájí řešení kritického incidentu ohrožující provoz organizace do 2 pracovních hodin od nahlášení, za pracovní hodiny se považuje období mezi 7:00 a 17:00 v pracovní dny.**

**Dodavatel zahájí řešení nekritického incidentu NBD od nahlášení.**

Dodavatel neprodleně potvrdí obdržení požadavku v systému HelpDesk a poskytne Zadavateli informace o předpokládaném způsobu řešení požadavku, požadavcích na součinnost Zadavatele a předpokládaný termín vyřešení požadavku.

Dodavatel v průběhu řešení požadavku, pokud mu to charakter požadavku a způsob řešení umožňuje, průběžně informuje Zadavatele o aktuálním stavu a případných změnách v předpokládaném způsobu, požadované součinnosti a termínů vyřešení. V případě že dodavatel v průběhu řešení požadavku zjistí, že se jedná o Incident, jehož zdroj je prvek třetích stran, informuje Zadavatele o této skutečnosti, předpokládaném způsobu, požadované součinnosti a termínů vyřešení a pokračuje v řešení v režimu BE (Best Effort) tzn. dodavatel vyvine maximální možné úsilí na provedení požadavku a zejména na zajištění požadovaných parametrů předmětu plnění v nejkratší možné době.

Zjistí-li dodavatel v průběhu řešení Incidentu, že Incident je neodstranitelný, je v rámci Běžné pracovní doby povinen nepřetržitě pracovat na náhradním řešení a informovat o tomto stavu Zadavatele.

Zjistí-li dodavatel v průběhu řešení Incidentu, že Incident má přímou souvislost s neodborným či neoprávněným jednáním osob Zadavatele případně byl Incident vyvolán produkty či službami třetí osoby, je dodavatel povinen bezodkladně informovat o tomto stavu Zadavatele. Zadavatel se zavazuje bezodkladně uhradit v plné výši náklady nad rámec této smlouvy dodavatelem prokazatelně vynaložené k řešení Incidentu, přičemž samotná identifikace Incidentu je součástí plnění této smlouvy.

Zadavatel je oprávněn dořešení Incidentu kdykoliv zastavit či pozastavit, přičemž nárok dodavatele na úhradu již vynaložených prostředků zůstává nedotčen. Incident je v tomto případě považován za vyřešený.

V případě úspěšného vyřešení požadavku, je řešitel před ukončením požadavku povinen provést ověření funkčnosti služby (pokud je to možné). Iniciátora Incidentu informuje o:

- v případě Incidentu specifikuje příčinu (pokud je známa),

- vyzve iniciátora k ověření funkčnosti služby.

Po ověření funkčnosti ze strany Zadavatele se Požadavek považuje za vyřešený.

Po vyřešení požadavku dodavatel požadavek uzavře v systému HelpDesk a informuje Zadavatele.

Zadavatel má právo ve lhůtě 10 dnů od uzavření požadavku vznést výhrady nebo připomínky ke způsobu řešení nebo k výslednému stavu; v takovém případě se požadavek nepovažuje za uzavřený a Strany se zavazují zahájit společné jednání za účelem odstranění veškerých vzájemných rozporů a nalezení shody nad způsobem řešení nebo výsledném stavu, a to nejpozději do pěti (5) pracovních dnů od výzvy kterékoliv Strany.

### Záruky na servisní služby

Zadavatel požaduje záruku na veškeré servisní služby provedené v rámci podpory provozu v délce trvání minimálně 3 měsíců (není-li u konkrétní služby uvedeno jinak) od okamžiku realizace. Veškeré opravy po dobu záruky budou bez dalších nákladů pro provozovatele.