# Město Kroměříž

Název projektu: Kroměříž - zlepšení kybernetické bezpečnosti infrastruktury

Registrační číslo projektu: CZ.31.2.0/0.0/0.0/23\_093/0008490

## Současný stav

### Provozované servery

Hlavní parametry všech tří serverů Dell R740 (dohromady):

* CPU: celkem 6 CPU / 48 jader / 96 vláken
* RAM: 3x 384GB DDR4
* disky pouze pro systém
* datum pořízení: červenec 2019
* podpora: 2 servery do červenec 2026, 1 server bez podpory

### Provozované diskové pole

Hlavní parametry stávajícího pole Dell EMC SCv3020:

* disková kapacita 43TB
* datum pořízení: červenec 2019
* podpora do červenec 2026

### Replika server

Hlavní parametry serveru Lenovo SR650 V3 pro replikaci dat:

* 2x Intel Xeon Gold 5415+ 8C 150W 2.9GHz Processor
* RAM: 512GB DDR5
* Disková kapacita: 8x 3,84TB pro repliky
* 2x 240GB pro systém
* NIC: 4x 10/25Gb

### Hlavní aktivní prvky (core switche)

Hlavní parametry switchů HP5140 (pro jeden prvek):

* 16 x SFP 100/1000 Mbps ports
* 8 x SFP dual-personality ports—10/100/1000BASE-T RJ-45 or 100/1000BASE-X Combo Ports
* 4 x SFP+ fixed 1000/10000 SFP+ ports
* 1 x RJ-45 serial console port
* redundantní napájení

Software

SW pro serverovou virtualizaci

VMware vSphere 8 Standard pro 8 procesorů v kombinaci s vCenter managementem

počet provozovaných virtuálních serverů (VM) – asi 70

Pozn.:   
Veškerá technologie je umístěna v jednom technologickém centru.

SW operačních systémů

24 x Microsoft Windows Server 2019 Datacenter 2 CoreLic +250 User Cal

Pozn.:   
Pokrývá stávajících 48 jader CPU na serverech

**SW pro replikaci/zálohu dat**:

Veeam Availability Suite Enterprise Plus. Public Sector. 8 socket pack.

Pozn.:   
Pro replikaci provozních dat je využívána pokročilá technologie Veeam, konkrétně Continuous Data Protection (CDP).

**Koncové stanice**

Koncové stanice jsou vybaveny operačním systémem Windows 11, antivir Eset.

## Požadovaný stav

V rámci veřejné zakázky budou pořízeny 3 fyzické servery, 4 nové switche a pásková mechanika. Přičemž zapojení síťové infrastruktury a pořízeného HW proběhne na základě níže uvedeného schématu. Nad diskovým úložištěm jednotlivých serveru vznikne virtuální datové úložiště, které bude umožňovat online replikaci dat mezi jednotlivými servery.



# Obecné požadavky

Část 1:

* Zabezpečení komunikační sítě a segmentace sítě
* Zálohování a archivace
* Servery a disková úložiště, která budou přímo využita v rámci zajištění kybernetické bezpečnosti (virtualizace, ukládání logů aj.).
* Nakup potřebného SW, operační systém, virtualizace datového úložiště

Část 2:

* Pořízení a implementace Endpoint protection řešení dvoufaktorové ověření uživatelů (2FA) a management mobilních zařízení (MDM

Část 3:

* Řízení přístupů a identit.

Část 4:

* Pořízení a implementace nástroje pro analýzu a monitoring síťového provozu.

Část 5:

* Pořízení a implementace nástroje pro log management.

**Důležité upozornění:**

Dodavatel, který se stane vybraným dodavatelem této veřejné zakázky v libovolné části 1 – 5, je vyloučen z možnosti ucházet se o plnění audit kybernetické bezpečnosti.

|  |
| --- |
| **Požadavek** |
| Pokud je k provozu níže uvedených informačních systémů nutné další zařízení, licence nebo prvek podle povahy zvoleného technického řešení s výjimkou nově nakupovaných nebo stávajících, uchazeč ho výslovně uvede a zahrne do ceny svého plnění včetně nutných upgrade a update po dobu udržitelnosti. |
| Dodavatel vždy dodrží uvedené požadavky na instalaci a konfiguraci. |
| Dodavatel zajistí instalaci a konfiguraci dodaných HW a SW komponent v návaznosti na stávající infrastrukturu organizace, a to včetně instalace a implementace do stávající IT infrastruktury v sídle zadavatele |
| V případě dodání více kusů zboží u téhož zboží budou dodány identické kusy. Např. server 3x znamená, že zadavatel požaduje 3x identický server. |
| Dodávané zboží bude, tam kde to je možné, od jednoho výrobce z důvodu zajištění maximální kompatibility a jednotného servisního místa a managementu. |
| **Požadavky na certifikaci dodavatele HW a původ zboží** |
| U zařízení, u kterých je výslovně uveden požadavek na certifikaci, musí být Dodavatelem doložena certifikace nebo čestné prohlášení a garance výrobce nabízeného HW, že nabízené zboží je určené pro český trh, je nové, nepoužité a pochází z oficiálního distribučního kanálu v ČR. Dodavatel dodrží uvedené požadavky na certifikaci dodavatele (subdodavatele) HW a původ zboží. |

# Část 1 Zabezpečení komunikační sítě a segmentace sítě

***Město Kroměříž využívá switch HPE Aruba 6300M 24-port SFP+ and 4-port SFP56 Switch JL658A. Nově pořizované switche musí být stohovatelné s již provozovaným switchem, budou tvořit páteřní síť města.***

## Implementace

Součástí dodávky jsou následující body:

1. Implementace síťových prvků

* Instalace a fyzické rozmístění switchů v definovaných lokalitách
* Konfigurace sítě a jednotlivých segmentů
* Fyzické propojení síťových prvků včetně přepojení celé sítě a serverového HW do nové sítě

1. Implementace serverového HW:

* Fyzická instalace serverového HW, aktualizace firmware, zahoření, provedení HW testů
* Konfigurace konzole pro vzdálenou správu a management
* Nasazení a konfigurace virtualizace
* Nasazení a konfigurace SW pro replikaci datového úložiště
* Instalace prostředí a virtuálních systémů
* Migrace stávajícího prostředí virtuálních serverů na nový HW

1. Implementace SW na diskovou/datovou virtualizaci:

* Předimplementační analýzy, popis způsob nasazení a zhodnotí jednotlivé varianty řešení
* Implementace SW na diskovou virtualizaci – synchronní replikace dat
* Konfigurace a zaškolení
* Otestovaní a předvedení krizových scenářů při výpadku síťové infrastruktury

1. Implementace zálohování a archivace:

* Instalace a konfigurace páskové knihovny
* Konfigurace zálohovacích politik pro zálohování serverové infrastruktury
* Ověření zálohovacích pravidel
* Migrace produkčního prostředí
* Virtualizace VMware cca 7O VM
* Návrh migračních scénářů s minimalizací doby výpadku
* Migrace bude probíhat přes víkend, maximálně patek až neděle.

1. Implementace služeb dohledu:

* Instalace a konfigurace sondy a agentů pro dohled nad celý prostředím
* Instalace a konfigurace systému pro sběr dat a vyhodnocení
* Konfigurace monitorovacích politik na základě doporučení dané technologie a schválené projektové dokumentace
* Ověření monitorovacích pravidel, testovací provoz
* Integrace celého prostředí, napojení na dohledovou službu a případné externí tiketovací systémy

1. Předání instalační a provozní dokumentace:

* technická dokumentace (produktové listy atd.)
* návody k použití (manuály), v tištěné nebo elektronické podobě
* Implementační dokumentace, obsahem dokumentace bude minimálně:
  1. textový popis řešení jako celku,
  2. schéma zapojení HW
  3. výrobce a typ zařízení,
  4. kompletní přehled dodaných a použitých licencí,
  5. Přístupové údaje nastavené při implementaci – přehledová tabulka musí obsahovat veškeré přístupové údaje k jednotlivým komponentám a jejich managementu tak, aby zadavatel měl po převzetí řešení neomezený přístup ke všem jeho částem.
  6. kontaktní informaci na technickou poimplementační podporu
  7. kontaktní informace na servisní pracoviště zajišťující podporu jednotlivých HW komponent.
  8. všechny funkcionality, které jsou využity, musí být podrobně zdokumentovány, tak aby uživatel neznalý těchto funkcionalit byl s nimi podle dokumentace schopný pracovat

1. Zaškolení administrátorů

* Zejména diskovou virtualizaci, administrace switchů, páskové knihovny a její administrace ve Veeam.
* Všechny funkcionality, které jsou využity, musí být zdokumentovány, tak aby zaškolený administrátor byl s nimi podle dokumentace schopný pracovat.

Provedení závěrečných akceptačních testů, zpracování dokumentace a zaškolení

* Provedení testu výpadku jednoho fyzického nodu
* Provedení testu výpadku napájení
* Provedení testu výpadku libovolného síťového prvku
* Provedení testu obnovy libovolného serveru či dat ze zálohy
* Zpracování komplexní dokumentace popisující konfiguraci celého prostředí
* Zpracování komplexní bezpečnostní dokumentace dle požadavků bezpečnostních norem
* Zpracování komplexní dokumentace pro správu a údržbu celé infrastruktury včetně plánu pro obnovu dat z páskové knihovny
* Zaškolení interní obsluhy správy sítě, zaškolení obsluhy dohledového centra podpory pro vyhodnocení bezpečnostních událostí.
* Poskytnutí nezbytné součinnosti realizátorům ostatních částí.

### HW1.1 Páteřní switch 4 ks

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Minimální požadavek** | **Dodavatel uvede, jestli splňuje požadavky (ano/ne) a navíc popíše jakým způsobem** |
| Výrobce |  |  |
| Model |  |  |
| Provedení | * montáž do racku, včetně příslušenství pro montáž, výška 1U, stohovatelný * redundantní interní hot-swap napájecí zdroje |  |
| Porty: | * Minimálně 24 Ports SFP/SFP+ 1G/10G * Minimálně 4 Ports SFP/SFP+/SFP28/SFP56 1G/10G/25G/50G |  |
| Management: | * 1 OOBM ethernet port * USB nebo USB-C konzolový port * Management prostřednictvím minimálně WEBGUI a SSH |  |
| Vlastnosti a funkce: | * Minimálně 880 Gbps Switching Fabric * Propustnost minimálně 654 Mpps * Packet buffer minimálně 8Mb * Latence maximálně 1Gbps: 2 μs, 10Gbps: 1.5 μs, 25Gbps: 2.9 μs 50Gbps: 2.9 μs * Podpora:   + SNMP v2c, v3,   + Link Aggregation,   + Stacking   + Syslog,   + L3,   + Spanning tree,   + multicast filtering,   + ACL |  |
| Kabeláž a optické moduly | * 2x 1 m 50Gb SFP56 DAC kabel * 16 x 10/25 Gb SFP+ (připojení serverů) * 6x SFP56 transeiver, SM, LC duplex, 10km (3 páry) * kabely a moduly budou dodány originální od výrobce switchů (použití OEM se nepovoluje) |  |
| Záruka | * standartní záruka výrobce na kompletní HW * jediné kontaktní místo pro nahlášení poruch pro všechny komponenty dodávaného systému * servis je poskytován přímo výrobcem zařízení nebo certifikovaným servisním partnerem * servisní zásahy budou prováděny vždy v místě instalace zařízení. Nabízené zařízení musí být pokryto oficiální podporou výrobce tak, aby v případě závady, kterou není Uchazeč schopen odstranit, mohl Zadavatel tuto závadu eskalovat přímo k technické podpoře výrobce zařízení * zadavatel musí mít možnost si sám legálně stahovat bezpečnostní záplaty i nové verze Software/Firmware pro nabízené zařízení přímo ze stránek výrobce zařízení |  |
| Certifikace dodavatele, původ zboží | * Jsou splněny „Požadavky na certifikaci dodavatele HW a původ zboží“ |  |
| Další požadavky | * Prodávající prohlašuje, že switche a příslušenství jsou určeny k prodeji na českém trhu, jsou nové, nepoužité. * Parametry switchů a záruka bude ověřena na veřejně dostupných webových stránkách výrobce v den dodání zboží. |  |

## Zálohování a archivace

### HW1.2Pásková knihovna

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Minimální požadavek** | **Dodavatel uvede, jestli splňuje požadavky (ano/ne) a navíc popíše jakým způsobem** |
| Výrobce |  |  |
| Model |  |  |
| Provedení, příslušenství | * rackmount, včetně montážního kitu do standardního 19" racku * základní jednotka max. 3U * redundantní napájecí zdroje * čelní panel s informací o stavu * kabely a moduly potřebné na propojení se serverem |  |
| LTO mechaniky | * 1x LTO-9 drive * podpora až 21 LTO mechanik * Propojení se serverem napřímo s propustností min. 8Gb/s (musí korespondovat se serverem) |  |
| LTO sloty | * min. 40 slotů v základní jednotce * možnost rozšíření knihovny až na 280 slotů, max. 21U |  |
| LTO média | * 25x LTO-9 páskové médium * 30x label * 2x LTO čisticí médium |  |
| Další vlastnosti | * kryptování dat, vč. potřebného SW a HW |  |
| Záruka, servis | * min. 5 let na kompletní HW, max. odezva NBD on-site po nahlášení problému * jediné kontaktní místo pro nahlášení poruch pro všechny komponenty dodávaného systému * servis je poskytován přímo výrobcem zařízení nebo certifikovaným servisním partnerem * servisní zásahy budou prováděny vždy v místě instalace zařízení. Nabízené zařízení musí být pokryto oficiální podporou výrobce tak, aby v případě závady, kterou není Uchazeč schopen odstranit, mohl Zadavatel tuto závadu eskalovat přímo k technické podpoře výrobce zařízení * zadavatel musí mít možnost si sám legálně stahovat bezpečnostní záplaty i nové verze Software/Firmware pro nabízené zařízení přímo ze stránek výrobce zařízení |  |
| Certifikace dodavatele, původ zboží | * Jsou splněny „Požadavky na certifikaci dodavatele HW a původ zboží“ |  |
| Kompatibilita | * Pásková knihovna bude plně kompatibilní s Veeam Backup & Replication 12 |  |
| Další požadavky | * Prodávající prohlašuje, že pásková knihovna a příslušenství jsou určeny k prodeji na českém trhu, jsou nové, nepoužité. * Parametry páskové knihovny a záruka bude ověřena na veřejně dostupných webových stránkách výrobce v den dodání zboží. |  |

## Servery a disková úložiště, která budou přímo využita v rámci zajištění kybernetické bezpečnosti (virtualizace, ukládání logů aj.).

### HW1.3 Server 3 ks

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Minimální požadavek** | **Dodavatel uvede, jestli splňuje požadavky (ano/ne) a navíc popíše jakým způsobem** |
| Výrobce |  |  |
| Model |  |  |
| Provedení, příslušenství | Provedení rack 2U do standardního 19" rozvaděče |  |
| CPU | * Minimálně 2 procesory o celkovém výkonu minimálně 24000 bodů dle <http://cpubenchmark.net/>, fyzických jader 8 * Servery budou zapojeny v VMware cluster s replika serverem, který je osazen CPU 2x Intel Xeon Gold 5415+ 8C 150W 2.9GHz. řešení musí umožnit migraci virtuálních serveru bez nutnosti vypnutí. |  |
| Vlastnosti | * Minimálně 24 paměťových slotů, podpora minimálně 4TB RAM * Osazená paměť RAM minimálně 768 GB * Rozhraní minimálně VGA connector, 2x USB 3.0, Minimálně 1x interní USB minimálně generace 3.0 s možností bootu OS * Minimálně 2x 10/25GbE SFP28 4-Port Ethernet Adapter * Vzdálené správa s dedikovaným vlastním portem RJ-45 a možností převzít plně vzdálené ovládání serveru * Řadič na minimálně 16 disků, 8GB cache, s podporou pro navrhované disky a diskovou kapacitu. * Server musí mít min. 24 pozic pro disky, přičemž po osazení dodaných disků musí zůstat minimálně 8 volných slotů * Server bude osazen dvěma SSD disky v RAID1 o min. kapacitě 240 GB, disky optimalizované pro boot systému, disky nesmí ponížit počet 24 využitelných pozic v serveru. * Server bude osazen min. 2x 960GB SSD zapojených do RAID řadiče * Server bude mít datové uložiště o **hrubé diskové kapacitě min. 60TB NVMe** * Plně redundantní za chodu měnitelné napájecí zdroje, Minimální certifikace použitého zdroje: Platinum * TPM 2.0 chip a podpora SED disků, Podpora Advanced Encryption Standard (AES) * Časově neomezená licence na hromadnou správu serverů, inverntarizace a alerting * Možnost hromadného sledováni a upgrade úrovní FW jednotlivých komponent serverů * Rackové výsuvné ližiny a rameno pro kabeláž na zadní straně serveru, bezel LCD * Call Home funkce * **Jeden ze tří serverů bude osazen kartou pro připojení páskové mechaniky s propustností min. 8Gbps** |  |
| Management | * Možnost nahrávání záznamu bootu serveru a pádu serveru, * Možnost vzdáleného mountu ISO a IMG image souborů (minimálně pomocí protokolů: HTTPS, SFTP, CIFS, a NFS), * Možnost sdílet jednu virtuální konzoli až šesti uživateli, * Podpora standardních Webových prohlížečů a HTML5, * Možnost blokovat konkrétní IP adresy |  |
| Záruka, servis | * podpora na 7 let, servisní zásah bude provádět technik výrobce následující pracovní den * oprava v místě instalace serveru, * servis je poskytován výrobcem serveru * jediné kontaktní místo pro nahlášení poruch pro všechny komponenty dodávaného systému * možnost stažení ovladačů a management software na webových stránkách * zdarma aktualizace firmware min. po dobu platné podpory * možnost automatického generování servisního incidentu přímo u výrobce hardware |  |
| Certifikace dodavatele, původ zboží | * Jsou splněny „Požadavky na certifikaci dodavatele HW a původ zboží“ |  |
| Kompatibilita | * Všechny servery budou od jednoho výrobce stejného typu z důvodu zajištění maximální kompatibility a jednotného servisního místa a managementu. |  |
| Další požadavky | * Prodávající prohlašuje, že severy a příslušenství jsou určeny k prodeji na českém trhu, jsou nové, nepoužité. * Parametry serveru a záruka bude ověřena na veřejně dostupných webových stránkách výrobce v den dodání zboží. |  |

### SW1.1 Serverový operační systém 4 ks a 270 ks uživatelských přístupových licencí

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Minimální požadavek** | **Dodavatel uvede, jestli splňuje požadavky (ano/ne) a navíc popíše jakým způsobem** |
| Výrobce, název, verze a licenční program serverového OS |  |  |
| Verze | * Serverový operační systém v nejnovější verzi s podporou virtualizace |  |
| Počet serverových licencí | * neomezený počet serverů v serverovém virtuálním prostředí * licence pro min. 2x osazené CPU v každém serveru * licence dle počtu procesorových jader |  |
| Vlastnosti OS | * adresářové služby kompatibilní s X. 509 * adresářová služba umožňuje obsahovat objekty typu uživatel, skupina, počítač a další * autentizace protokoly Kerberos V5, NTLMv2, NTLM * centrálně řízené politiky uživatelů a počítačů * možnost funkcí DNS, DHCP, WINS * možnost sdílení souborů a nastavování práv na objekty adresářové služby * sdílení souborů pomocí protokolu CIFS * distribuovaný souborový systém a delta replikace * možnost sdílení tiskáren a nastavování práv na objekty adresářové služby * možnost grafického uživatelského rozhraní v češtině * možnost downgrade na nižší verzi * 100% kompatibilita se stávajícími operačními systémy Microsoft Windows Server 2019 |  |
| Technické a licenční požadavky na uživatelské licence | * kompatibilita s nabízeným serverovým OS * kompatibilita s používanou správou uživatelů (Active directory) * kompatibilita s OS na koncových stanicích uživatelů |  |
| Počet uživatelských licencí | * dodání licencí minimálně pro přístup 270 uživatelů k nabízenému serverovému OS, jsou-li dle licenčních podmínek výrobce nabízeného serverového OS nutné * Nabízené licence pokryjí všechny servery města Kroměříže a veškeré uživatele k nim přistupující. |  |
| Správa systému | * pro správu operačního systému požadujeme grafické nástroje s jednoduchou obsluhou |  |
| Dokumentace | * požadujeme podrobnou technickou dokumentaci v elektronické podobě |  |

### SW1.2 SW pro datovou replikaci dat ve VMware

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Minimální požadavek** | **Dodavatel uvede, jestli splňuje požadavky (ano/ne) a navíc popíše jakým způsobem** |
| Výrobce, název, verze a licenční program serverového OS |  |  |
| Verze |  |  |
| Technické požadavky | * Auto-tiering - umožňuje ukládat a následně číst data na úložném médiu s nejlepším přizpůsobením na základě předdefinovaných pravidel nebo zásad * Podpora minimálně 8 TBs cache na NOD * Nepřetržitá ochrana dat. V případě poškození dat v důsledku logických chyb, uživatelských chyb nebo malwaru se lze vrátit zpět do konkrétního bodu v čase před nepožadovanou aktualizací. * Podpora deduplikace dat * Podpora komprese dat * Podpora šifrování dat * Podpora Storage Load Balancing * Podpora QoS pro I/O performance * Zrychlení úloh náhodného zápisu prostřednictvím sekvenční optimalizace * Podpora asynchronní replikace * Podpora snapshotů * Podpora storage a Disk Pooling - sjednocení a optimalizace heterogenních úložných zařízení * Podpora sychronního zrcadlení - zero downtime, zero touch failover * Podpora Thin Provisioning |  |
| Podpora | * platnost licence min. 60 měsíců, včetně nároku na opravné a nové verze software, vč. technické podpory výrobce. |  |
| Instalace a konfigurace | * součástí dodávky je vytvoření předimplementační analýzy, která popíš způsob nasazení, v případě že bude více variant, bude provedeno zhodnotí a návrh nejvhodnější. |  |
| Replikace dat | Předpokládaný objem replikovaných dat je 15TB |  |

## Požadavky na záruky

Zadavatel požaduje záruku na veškeré dodané technologie v délce trvání minimálně **36 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 = 3 roky bude součástí pořizovací ceny zařízení.

Cena záruky pro 4-7 rok požadovaných Zadavatelem (tj. rozdíl mezi Standardními zárukami 3ROKY a podporami a požadavky Zadavatele) dodavatel uvede v položce "**Nadstandardní záruky a podpory výrobců"**

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

## Požadavky na technickou podporu

Dodavatel nacení i potřebnou technickou podporu - (pouze pro SW1.2) je proces pravidelného udržování, vylepšování a opravování softwarových aplikací po jejich prvotním vývoji a nasazení. Zadavatel v rámci stanovení nabídkové ceny nacení veškerou potřebnou technickou podporu k řádnému provozovaní dodaného řešení. Potřebnou technickou podporu dodavatel nacení po dobu udržitelnosti projektu 5let. Technická podpora bude dle povahy dodaného řešení pokrývat minimálně níže uvedené scénáře:

* **Technická podpora:** 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.
* **Nové verze a aktualizace:** Úpravy a změny softwaru, aby zůstal kompatibilní s měnícím se prostředím. To může zahrnovat aktualizace pro nové operační systémy, hardware nebo jiné softwarové závislosti.
* **Optimalizace provozu:** 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.

**Garantovaná doba reakce Poskytovatele od nahlášení požadavku na poskytnutí technické podpory**

1. Služba je poskytována Pracovníky Poskytovatele v okamžiku, kdy dojde k zadání Požadavku.
2. Obsahem této služby je reakce Poskytovatele na Požadavky dle jejich priority a zahájení řešení v rámci **Servisního kalendáře, tj. pracovní dny od 7:00 do 17:00**.
   1. Je-li požadavek nahlášen mimo pracovní dobu, je počátkem uvedené doby 7:00 hodin nejbližšího pracovního dne.
   2. Dodavatel je povinen zahájit řešení požadavku bezodkladně, nejpozději však do níže uvedených časů, viz tabulka Klasifikace požadavku a stavů.
3. Požadavek na provedení této služby zadávají Kontaktní osoby Objednatele nebo Poskytovatele zadáním Požadavku na Helpdesk Poskytovatele.
4. Zahájení řešení je primárně poskytováno Vzdáleným připojením pracovníka Poskytovatele. Pokud to technická povaha řešení Požadavku vyžaduje, bude realizován fyzický zásah pracovníka Poskytovatele v místě technologických center města Kroměříže, přesné místo bude vždy specifikováno v zadaném požadavku.

**Klasifikace požadavku a stavů**

|  |  |  |  |
| --- | --- | --- | --- |
| **Klasifikace** | **Definice** | **SLA zahájení řešení** | **Předpokládané vyřešení požadavku** |
| 1. Nahlášení požadavku | Potvrzení přijetí nahlášeného požadavku jedním z výše uvedených způsobů hlášení požadavku. | Nejpozději do 15 minut | Není specifikováno |
| 1. Kritický požadavek (A) | Události, které znemožňují přístup ke službám a datům poskytovaných Prvky IT, nebo jejich využívání, vážně ovlivňují plnění termínů nebo ziskovost, případně mají vliv na většinu uživatelů a služeb. | Nejpozději do 2 hodiny od nahlášení požadavku v rámci Servisního kalendáře | Do 8 hodin od zahájení řešení, dle servisního kalendáře |
| 1. Závažný požadavek (B) | Události, které významným způsobem degradují, nebo silně omezují funkcionalitu nebo službu Prvku IT, ale existuje náhradní řešení (činnost pokračuje v omezeném provozu). | Nejpozději do 5 hodin od nahlášení požadavku v rámci Servisního kalendáře | Do 16 hodin od zahájení řešení, dle servisního kalendáře |
| 1. Ostatní požadavky (C) | Všechny ostatní požadavky, neomezující řádné používání Informačního systému, které tvoří Prvky IT. | Nejpozději do druhého pracovního dne od nahlášení požadavku | Do 32 hodin od zahájení řešení, dle servisního kalendáře |
| 1. Změnové požadavky | Součinnost při implementaci změn a činnostech při nasazovaní nových prvků IT či jejich částí. | Nejpozději do 7 pracovních dní | Stanoveno dohodou |
| 1. Konzultace a návrh řešení, programátorské práce | Konzultace při řešení problémů nebo při úpravách prvků IT. | Nejpozději do 5 pracovních dní | Stanoveno dohodou |

Pro případ, že bude zadavatel požadovat služby rozšířené technické podpory podle písmena e) a f), budou tyto služby vyúčtovány po skončení kalendářního měsíce, ve kterém byly čerpány, v hodinové sazbě uvedené v Kalkulaci ceny, dle skutečně realizovaných hodin rozšířené servisní podpory. Předpokládaný rozsah služeb rozšířené technické podpory pro účely přípravy nabídky je 100 hodin / na 5 let.

**Ceny za služby technické podpory**

|  |  |  |
| --- | --- | --- |
| **Typ požadavku** | **Cena bez DPH** | **Měrná jednotka** |
| Servisní požadavek "A" |  | Člověkohodina |
| Servisní požadavek "B" |  | Člověkohodina |
| Servisní požadavek "C" |  | Člověkohodina |
| Změnový požadavek |  | Člověkohodina |
| Konzultace a návrh řešení, programátorské práce |  | Člověkohodina |
| Dopravné mimo město |  | Km |

# Část 2 Pořízení a implementace Endpoint protection řešení, dvoufaktorové ověření uživatelů (2FA) a management mobilních zařízení (MDM), dále jen „Nástroj“

***Zadavatel v současné době používá ESET PROTECT Complete, na obsluhu tohoto programu je zaškolen. Nástroj je nasazen na všech koncových stanicích a serverech.***

Implementace

Součástí dodávky je:

1. Poskytnutí veškerých potřebných licencí – zahrnuje všechny potřebné softwarové a provozní licence pro správný chod nástroje, včetně licencí pro všechny moduly a funkce, které budou součástí implementace.
2. Předimplementační analýza a návrh řešení.
3. Instalace nástroje a zprovoznění přístupu na cloud – zahrnuje kompletní instalaci Nástroje, konfiguraci cloudového prostředí, nastavení přístupu pro administrátory.
4. Zprovoznění, nastavení a optimalizace provozu Nástroje – provedení všech potřebných nastavení pro plně funkční provoz Nástroje, včetně optimalizace výkonu, konfigurace parametrů a zajištění správného chodu všech procesů, aby bylo dosaženo maximální efektivity serverů a klientských stanic.
5. Migrace konfigurace současného řešení včetně politik či instalačních balíčků programů pro PC.
6. Předání instalační a provozní dokumentace – dodání podrobné dokumentace v českém jazyce, která obsahuje kompletní výčet všech potřebných úkonů pro správnou instalaci, konfiguraci a údržbu Nástroje. Dokumentace také zahrnuje návody pro administrátory.
7. Proškolení obsluhy – realizace školení pro administrátory Nástroje, které zahrnuje jak základní, tak pokročilé funkce Nástroje. Školení bude zaměřeno na efektivní využívání Nástroje a jeho správu.

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Minimální požadavek** | **Dodavatel uvede, jestli splňuje požadavky (ano/ne) a navíc popíše jakým způsobem** |
| Výrobce, název, verze a licenční program |  |  |
| Licence | Nevýhradní licence v délce trvání minimálně 5 let |  |
| Ochrana před škodlivým SW | * Nástroj bude obsahovat podporované klientské platformy - OS: Windows, Linux, MacOS, Android, vše v českém jazyce. * Nástroj bude obsahovat antimalware, antiransomware, antispyware a anti-phishing pro aktivní ochranu před všemi typy hrozeb. * Nástroj bude obsahovat personální firewall pro zabránění neautorizovanému přístupu k zařízení se schopností automatického přebrání pravidel z brány Windows Firewall. * Nástroj bude obsahovat modul pro ochranu operačního systému a eliminaci aktivit ohrožujících bezpečnost zařízení s možností definovat pravidla pro systémové registry, procesy, aplikace a soubory. * Nástroj bude obsahovat ochranu před neautorizovanou změnou nastavení a vyřazením z provozu / odinstalací antimalware řešení a kritických nastavení a souborů operačního systému. * Nástroj bude obsahovat aktivní i pasivní heuristickou analýzu pro detekci dosud neznámých hrozeb. * Nástroj bude obsahovat blokaci exploitů zneužívajících zero-day zranitelnosti, jenž pokrývá nejpoužívanější vektory útoku: o síťové protokoly, o Flash Player, o Javu, o Microsoft Office, o webové prohlížeče, o e-mailové klienty, o PDF čtečky. * Nástroj bude obsahovat detekci malwaru již na síťové úrovni poskytující ochranu i před zneužitím zranitelností na síťové vrstvě. * Nástroj bude obsahovat kontrolu šifrovaných spojení (SSL, TLS, HTTPS, IMAPS…). * Nástroj bude obsahovat anti-phishing se schopností detekce homoglyph útoků. * Nástroj bude obsahovat kontrolu RAM paměti pro lepší detekci malwaru využívajícího silnou obfuskaci a šifrování. * Nástroj bude obsahovat cloud kontrolu souborů pro urychlení skenování fungující na základě reputace souborů. * Nástroj bude obsahovat kontrolu souborů v průběhu stahování pro snížení celkového času kontroly. * Nástroj bude obsahovat kontrolu souborů při zapisování na disku a extrahování archivačních souborů. * Nástroj bude obsahovat detekci s využitím strojového učení. * Nástroj bude obsahovat funkci ochrany proti zapojení do botnetu pracující s detekcí síťových signatur. * Nástroj bude obsahovat ochranu před síťovými útoky skenující síťovou komunikaci a blokující pokusy o zneužití zranitelností na síťové úrovni. * Nástroj bude obsahovat kontrolu s podporou cloudu pro odesílání a online vyhodnocování neznámých a potenciálně škodlivých aplikací. * Nástroj bude obsahovat lokální sandbox. * Nástroj bude umožňovat rollback souborů zasažených ransomwarem s možností reportovat do konzole obnovené soubory zasažené ransomwarem, nevyužívá se shadow copy a pro svou správnou funkci nevyžaduje dodatečnou konfiguraci. * Nástroj bude obsahovat modul behaviorální analýzy pro detekci chování nových typů ransomwaru. * Nástroj bude obsahovat systém reputace pro získání informací o závadnosti souborů a URL adres. * Nástroj bude obsahovat cloudový systém pro detekci nového malwaru ještě nezaneseného v aktualizacích signatur. * Nástroj bude obsahovat technologii pro detekci rootkitů obvykle se maskujících za součásti operačního systému. * Nástroj bude obsahovat skener firmwaru BIOSu a UEFI. * Nástroj bude obsahovat skenování souborů v cloudu OneDrive. * Nástroj bude obsahovat funkcionalitu pro klienty MS Windows – Antimalware, Antispyware, Personal Firewall, Personal IPS, Application Control, Device Control, Security Memory (zabraňuje útokům na běžící aplikace), kontrolu integrity systémových komponent. * Nástroj bude obsahovat funkcionalitu pro klienty MacOS – Antimalware, Personal Firewall, Device Control, autoupgrade. * Nástroj bude obsahovat funkcionalitu pro klienty Linux – Antimalware, ICAPs scan, Botnet Protection. * Nástroj bude umožňovat aplikování bezpečnostních politik i v offline režimu na základě podmínek. * Nástroj bude obsahovat ochranu proti pokročilým hrozbám (APT) a 0-day zranitelnostem. * Nástroj bude podporovat automatické vytváření dump souborů na stanici na základě nálezů. * Nástroj bude umožňovat okamžité blokování/mazání napadených souborů na stanici (s možností stažení administrátorem k další analýze). * Nástroj bude obsahovat duální aktualizační profil pro možnost stahování aktualizací z mirroru v lokální síti a zároveň vzdálených serverů při nedostupnosti lokálního mirroru (pro cestující uživatele s notebooky). * Nástroj bude umožňovat definovat webové stránky, které se spustí v chráněném režimu prohlížeče, pro bezpečnou práci s kritickými systémy nebo internetovým bankovnictvím. * Nástroj bude obsahovat ochranu před útokem hrubou silou na protokol SMB a RDP. * Nástroj bude umožňovat zablokování konkrétní IP adresy po sérii neúspěšných pokusů o přihlášení pro protokoly SMB a RDP s možností výjimek ve vnitřních sítích. |  |
| SW pro sandboxing | * Nástroj bude obsahovat funkci cloudového sandboxu integrovanou do produktu pro koncové a serverové zařízení * Nástroj bude umožňovat spuštění vzorků malwaru pro: Windows, Linux, MacOS. * Nástroj bude umožňovat využití na koncových bodech a serverech pro aktivní detekci škodlivých souborů. * Nástroj bude obsahovat analýzu neznámých vzorků v řádu jednotek minut. * Nástroj bude obsahovat optimalizaci pro znemožnění obejití anti-sandbox mechanismy. * Nástroj bude umožňovat analýzu rootkitů a ransomwaru. * Nástroj bude obsahovat schopnost detekce a zastavení zneužití nebo pokusu o zneužití zero day zranitelnosti. * Nástroj bude řešit behaviorální analýzu. * Nástroj bude umožňovat reportování o analyzovaném souboru včetně exportu do PDF s informacemi o nalezeném škodlivém chování daného souboru formou webového reportu. * Nástroj bude umožňovat manuální odeslání vzorku do sandboxu. * Nástroj bude obsahovat blokování hrozby dokud není znám výsledek analýzy ze sandboxu. * Nástroj bude umožňovat neomezené množství odesílaných souborů. * Nástroj bude obsahovat veškerou komunikaci probíhající šifrovaným kanálem. * Nástroj bude obsahovat okamžité odstranění souboru po dokončení analýzy v cloudovém sandboxu. * Nástroj bude umožňovat volbu, jaké kategorie souborů do cloudového sandboxu budou odcházet (spustitelné soubory, archivy, skripty, pravděpodobný spam, dokumenty atp.). |  |
| SW pro odhalení škodlivé, či podezřelé aktivity včetně analýzy | * Nástroj bude umožňovat výběr mezi provozem EDR serveru v on-premise prostředí nebo cloud prostředí výrobce. * Nástroj bude umožňovat provoz on-premise s databázemi: MS SQL, MySQL. * Nástroj bude podporovat offline prostředí, technologie EDR vyhodnocuje a reaguje na události lokálně, nevyžaduje pro svou činnost připojení k internetu. * Nástroj bude obsahovat EDR řešení zajišťující stejnou ochranu i bez připojení k internetu. Pracuje autonomně a připojení k internetu neovlivní kvalitu detekční technologie na koncovém bodu. * Nástroj bude umožňovat logování činností administrátora. * Nástroj bude obsahovat EDR agenta pro prostředí Windows, Windows server, MacOS a linuxové distribuce. * Nástroj bude obsahovat autentizaci do management konzole EDR pomocí 2FA. * Nástroj bude umožňovat nutnost aktivace 2FA pro používání pokročilých nástrojů typu terminal. * Nástroj bude umožňovat řízení managementu EDR prostřednictvím API, a to jak pro: přijímání informací z EDR serveru, zasílání příkazů na EDR serveru. * Nástroj bude podporovat vzdálené pouštění příkazů přímo z EDR konzole na platformě Windows s nejvyšším oprávněním SYSTEM. * Nástroj bude umožňovat logování vzdáleného spouštění příkazů z konzole v EDR systému. * Nástroj bude umožňovat izolaci zařízení od sítě prostřednictvím EDR agenta přímo z konzole. * Nástroj bude umožňovat tvorbu vlastních indikátorů zneužití. * Nástroj bude umožňovat škálování množství historických dat vyhodnocených v EDR minimálně 2 měsíce pro low-level-data, minimálně 1,5 roku pro detekované incidenty při provozu v on-premise prostředí. * Nástroj bude obsahovat možnost aktivace „učícího režimu“ pro automatizované vytváření výjimek k detekčním pravidlům. * Nástroj bude obsahovat indikátory útoku pracující s behaviorální detekcí. * Nástroj bude obsahovat indikátory útoku pracující s reputací. * Nástroj bude umožňovat analýzu vektorů útoku. * Nástroj bude obsahovat schopnost detekce: škodlivých spustitelných souborů, skriptů, exploitů, rootkitů, síťových útoků, zneužití WMI nástrojů, bezsouborového malwaru. * Nástroj bude obsahovat schopnost detekce pokusů o dumpování přihlašovacích údajů uživatele. * Nástroj bude obsahovat schopnost detekovat laterální pohyb útočníka. * Nástroj bude obsahovat schopnost ukončit infikovaný proces. * Nástroj bude umožňovat ruční analýzu procesů veškerých spustitelných souborů a DLL knihoven. * Nástroj bude umožňovat náhled na spuštěné skripty použité v daném incidentu. * Nástroj bude umožňovat zabezpečené vzdálené spojení přes servery výrobce do on-premise konzole EDR. * Nástroj bude umožňovat vytváření automatizovaného response úkonu v podobě izolace stanice, blokace konkrétního hashe, odhlášení uživatele, restartování počítače pro jednotlivé scénáře nebo detekce. * Nástroj bude umožňovat automatické vyřešení incidentu definovaného administrátorem. * Nástroj bude obsahovat schopnost prioritizace vzniklých incidentů. * Nástroj bude umožňovat stažení podezřelého souboru ze stanice přes konzoli EDR. * Nástroj bude obsahovat schopnost zobrazení detekcí provedených antimalware produktem. * Nástroj bude umožňovat generování tzv. forest / full execution tree modelu. * Nástroj bude umožňovat vyhledávání pomocí nově vytvořených indikátorů zneužitelnosti nad historickými daty. * Nástroj bude obsahovat provázání s technikami popsanými v knowledge base MITRE ATT&CK. * Nástroj bude podporovat offline režim minimálně s možností detekce pravidel a setů detekčních pravidel. * Nástroj bude obsahovat průběžně aktualizovaná detekční pravidla EDR systému bez nutnosti aktualizace centrální správy/klienta. * Nástroj bude umožnovat EDR založit definice vlastních incidentů i s časovým pořadím detekce událostí * Nástroj bude obsahovat pokročilé detekční mechanismy pro detekci útoku i při nedostupnosti cloudového/centrálního serveru výrobce * Nástroj bude umožňovat export raw dat (veškerých dat) na externí úložiště, např. lokální disk, Azure Blob * Nástroj bude podporovat SHA256 algoritmus * Nástroj bude umožňovat filtrování určitého typu dat zpracovávaného z klientem * platnost licence min. 60 měsíců, včetně nároku na opravné a nové verze software, vč. technické podpory výrobce. |  |
| Správa a funkce konzole pro administraci | * Nástroj bude obsahovat konzoli dostupnou v internetovém prohlížeči. * Nástroj bude umožňovat instalaci v on-premise prostředí na Windows nebo Linux. * Nástroj bude umožňovat provoz konzole v cloudu výrobce. * Nástroj bude umožňovat instalaci formou virtual appliance pro virtuální prostředí VMware, Microsoft Hyper-V a Microsoft Azure, Oracle Virtual Box připravenou výrobcem. * Nástroj bude obsahovat server/proxy architekturu pro síťovou pružnost – snížení zátěže při stahování aktualizací detekčních modulů výrobce. * Nástroj bude umožňovat probuzení klientů pomocí Wake On Lan. * Nástroj bude obsahovat offline agent vzdálené správy pro zajištění komunikace a ovládání operačního systému klienta. * Nástroj bude umožňovat aktivaci politik a spouštění úloh při výskytu definované události i bez přístupu k internetu (například: odpojení od sítě při nalezení škodlivého kódu). * Nástroj bude obsahovat administraci v nejpoužívanějších jazycích včetně češtiny. * Nástroj bude umožňovat široké možnosti konfigurace oprávnění administrátorů (například možnost správy pouze části infrastruktury, které konkrétnímu administrátorovi podléhá). * Nástroj bude obsahovat zabezpečení přístupu administrátorů do vzdálené správy pomocí 2FA. * Nástroj bude obsahovat informace o aktuálně přihlášených uživatelích na daném zařízení. * Nástroj bude podporovat štítky/tagování pro snazší správu a vyhledávání. * Nástroj bude obsahovat správu karantény s možností vzdáleného vymazání / obnovení / obnovení a vyloučení objektu z detekce. * Nástroj bude umožňovat vzdálené získání zachyceného škodlivého souboru z klienta. * Nástroj bude obsahovat detekci nespravovaných (rizikových) počítačů komunikujících na síti. * Nástroj bude umožňovat instalaci a odinstalaci aplikací 3. stran. * Nástroj bude umožňovat vyčítání informací o verzích softwaru 3. stran. * Nástroj bude umožňovat vyčítání informací o hardwaru na spravovaných zařízeních (CPU, RAM, diskové jednotky, grafické karty…). * Nástroj bude umožňovat odeslání zprávy na počítač / mobilní zařízení, které se následně zobrazí uživateli na obrazovce. * Nástroj bude umožňovat vzdálené spuštění jakéhokoli příkazu na cílové stanici pomocí Příkazového řádku. * Nástroj bude obsahovat dynamické skupiny pro možnost definování podmínek, za kterých dojde k automatickému zařazení klienta do požadované skupiny a automatickému uplatnění klientské úlohy. * Nástroj bude podporovat klientské úlohy pro dynamické skupiny. * Nástroj bude umožňovat automatické zasílání upozornění při dosažení definovaného počtu nebo procent ovlivněných klientů (například: 5 % všech počítačů / 50 klientů hlásí problémy). * Nástroj bude podporovat SNMP Trap, Syslog, Rest API. * Nástroj bude podporovat instalaci agenta skriptem - \*.bat, \*.sh, \*.ini (GPO, SSCM…). * Nástroj bude umožňovat rychlé připojení na klienta pomocí RDP z konzole pro vzdálenou správu. * Nástroj bude obsahovat reportování stavu klientů chráněných jinými bezpečnostními programy. * Nástroj bude umožňovat zasílání reportů a upozornění na e-mail. * Nástroj bude umožňovat odesílání notifikací o vybraných událostech prostřednictvím tzv. Webhooků. * Nástroj bude umožňovat integraci s řešeními třetích stran podporujícími MDM (např. MS Intune, Workspace One). * Nástroj bude umožňovat řízení managementu konzole a jeho komponent prostřednictvím API, a to jak pro: Centrální správu samotnou, Komponenty antimalware řešení, jeho správy, politik a nastavení, EDR řešení, Export informací o detekcích, incidentech, Úpravu detekčních pravidel EDR. * Nástroj bude umožňovat správu zařízení a jeho nastavení, instalačních balíčků, včetně možnosti automatizace jednotlivých úkonů. * Nástroj bude umožňovat přidání zařízení do vzdálené správy pomocí: Synchronizace s Active Directory (jedné nebo více Active Directory), včetně možnosti synchronizace počítačů a uživatelů, Ručního přidání pomocí IP adresy nebo názvu zařízení, Síťového skenu nechráněných zařízení v síti. |  |
| Chráněné služby | * Nástroj bude umožňovat přihlášení do webových aplikací společnosti Microsoft (OWA, SharePoint…). * Nástroj bude umožňovat přihlášení přes RDP. * Nástroj bude umožňovat přístup k Exchange Control Panel & Exchange Administrator Center. * Nástroj bude umožňovat integraci s VMware Horizon View. * Nástroj bude umožňovat integraci s Citrix XenApp. * Nástroj bude umožňovat autentizaci pro VPN služby využívající protokol RADIUS (Cisco, Citrix, Fortinet, Juniper, Microsoft, OpenVPN…). * Nástroj bude umožňovat připojení ke cloudovým službám Office 365, G Suite a identity providerům (podpora SAML protokolu, podpora AD FS). * Nástroj bude umožňovat lokální přihlášení do Windows, Linux, macOS účtů. * Nástroj bude umožňovat vyžádání 2FA v nouzovém režimu Windows. * Nástroj bude umožňovat vyžádání 2FA při vyvolání UAC dialogu ve Windows. * Nástroj bude umožňovat vyžádání 2FA při uzamčeném účtu. |  |
| Požadavky na správu | * Nástroj bude obsahovat webové konzole provozované v cloudu výrobce s možností nasazení v on-premise prostředí. * Nástroj bude umožňovat přístup do konzole chráněný 2FA ověřením. * Nástroj bude umožňovat multitenantní provoz (možnost spravovat vícero uživatelských struktur v jedné konzoli). * Nástroj bude umožňovat synchronizaci uživatelských účtů z Active Directory. * Nástroj bude umožňovat tvorbu výjimek pro vnitřní sítě, kde není 2FA vyžadováno. * Nástroj bude umožňovat uživatelům přihlášení bez použití 2FA pro vybrané služby. * Nástroj bude umožňovat dočasné pozastavení požadavku na 2FA pro uživatele. * Nástroj bude umožňovat nastavení limitu pro počet neúspěšných zadání OTP. * Nástroj bude umožňovat centrální správu a přidělování hardwarových tokenů jednotlivým uživatelům. * Nástroj bude umožňovat reportování o úspěšných/neúspěšných přihlášeních uživatelů a způsobu použité autentizace (SMS, Push, OTP). |  |
| Ochrana poštovních serverů | * Nástroj bude obsahovat víceúrovňovou ochranu celého serveru – databáze schránek, transport zpráv i souborový systém serveru. * Nástroj bude podporovat MS Exchange 2019 a novější. * Nástroj bude obsahovat antivirus, antispyware a antispoofing technologie. * Nástroj bude obsahovat antispam s funkcí graylisting. * Nástroj bude umožňovat blokování nevyžádané pošty a phishingu bez potřeby manuální úpravy hodnot SCL (Spam Confidence Level). * Nástroj bude umožňovat vytváření pokročilých antispamových pravidel s možností vyhodnocení více podmínek v jednom pravidlu. * Nástroj bude umožňovat kontrolu jednotlivých MBX databází nebo konkrétních uživatelských schránek. * Nástroj bude umožňovat uživatelům poštovních schránek pracovat v samostatném prohlížeči se spamovými a potenciálně infikovanými zprávami, které nebyly doručeny do jejich e-mailové schránky. * Nástroj bude umožňovat tvorbu vlastních pravidel s vlastním hodnocením obsahu. * Nástroj bude podporovat více-serverové prostředí a zajišťovat P2P komunikaci. * Nástroj bude umožňovat detekci škodlivých souborů v reálném čase. * Nástroj bude podporovat správu přes příkazovou řádku (podpora edice Windows Server Core). * Nástroj bude obsahovat komplexní protokoly blokovaného spamu a zobrazovat greylistingované odesílatele. * Nástroj bude umožňovat sledování výkonu serveru v reálném čase. * Nástroj bude umožňovat nastavení pravidel inspekce souborů, například mazání spustitelných souborů a skriptů. * Nástroj bude obsahovat cloudovou reputační službu pro kontrolu příloh e-mailových zpráv. * Nástroj bude umožňovat správu ochrany na Exchange Serveru samostatně nebo prostřednictvím management konzole v cloudu. * Nástroj bude umožňovat export protokolů událostí produktu do protokolu operačního systému. * Nástroj bude podporovat tvorbu pravidel "Z hlavičky" pro přesnější detekci podvržených e-mailů na základě vyhodnocení pole From:. * Nástroj bude obsahovat backscatter ochranu. * Nástroj bude umožňovat synchronizaci lokální karantény zpráv napříč uzly clusteru. * Nástroj bude podporovat hybridní prostředí s možností kontroly poštovních schránek v Office 365. * Nástroj bude umožňovat zasílání přehledů o zachycených e-mailových hrozbách koncovým uživatelům. * Nástroj bude umožňovat zabezpečení poštovního serveru a jeho komponent heslem proti neautorizovaným úpravám. * Nástroj bude umožňovat dočasnou deaktivaci heslového zabezpečení pro vybrané uživatele na základě ověření administrátora vůči doméně. * Nástroj bude podporovat správu karantény prostřednictvím webového portálu pro vybrané uživatele i administrátory. * Nástroj bude umožňovat ochranu nastavení dodatečným heslem před neoprávněnou změnou konfigurace produktu. * Nástroj bude umožňovat editaci zpráv o stavu karantény a zachycených souborů (úprava těla e-mailu, předmětu a odkazu na blokovaný e-mail). * Nástroj bude obsahovat integrovanou funkci cloudového sandboxu pro e-mailovou ochranu MS Exchange, která nevyžaduje instalaci dalších komponent. * Nástroj bude řešit zpracování dat odesílaných v rámci cloudového sandboxu v rámci EU. * Nástroj bude umožňovat sandboxovou analýzu vzorků malwaru pro Windows, macOS a Linux. * Nástroj bude umožňovat využití sandboxu na koncových bodech a Exchange serveru pro aktivní detekci škodlivých souborů v e-mailech. * Nástroj bude podporovat analýzu neznámých vzorků v řádu jednotek minut. * Nástroj bude optimalizován pro znemožnění obejití anti-sandbox mechanismů. * Nástroj bude umožňovat analýzu rootkitů a ransomwaru. * Nástroj bude podporovat detekci a zastavení zneužití nebo pokusů o zneužití zero-day zranitelností. * Nástroj bude využívat behaviorální analýzu. * Nástroj bude poskytovat kompletní výsledky analýzy souboru v centrálním managementu včetně informací o nalezeném i nenalezeném škodlivém chování. * Nástroj bude umožňovat manuální odesílání vzorků do sandboxu. * Nástroj bude podporovat proaktivní ochranu, kdy je potenciální hrozba blokována do doby dokončení analýzy v sandboxu. * Nástroj bude umožňovat neomezené množství odesílaných souborů. * Nástroj bude zabezpečovat veškerou komunikaci šifrovaným kanálem. * Nástroj bude umožňovat okamžité odstranění souborů po dokončení analýzy z cloudového sandboxu. * Nástroj bude umožňovat výběr kategorií souborů odesílaných do cloudového sandboxu (spustitelné soubory, archivy, skripty, pravděpodobný spam, dokumenty atd.). * Nástroj bude podporovat odesílání souborů do cloudového sandboxu o velikosti až 64 MB. |  |
| Ochrana cloud Microsoft 365 | * Nástroj bude poskytovat komplexní ochranu pro prostředí Microsoft 365, včetně Exchange Online, OneDrive, SharePoint Online a Microsoft Teams. * Nástroj bude umožňovat nezávislou cloudovou správu pro vyhodnocení zachycených hrozeb. * Nástroj bude obsahovat neinvazivní technologii, která při nedostupnosti neovlivní fungování Microsoft 365. * Nástroj bude zahrnovat funkce Antimalware, Antispam a Antiphishing. * Nástroj bude umožňovat detekci útoků využívajících homoglyf techniku. * Nástroj bude umožňovat zasílání pravidelných reportů. * Nástroj bude podporovat vícenásobnou kontrolu podezřelých e-mailů. * Nástroj bude umožňovat export událostí, detekcí a audit logů přes Syslog. * Nástroj bude umožňovat ochranu celého tenantu nebo jednotlivých uživatelů. * Nástroj bude umožňovat automatickou aplikaci ochrany pro nově vzniklé uživatele v Microsoft 365 nebo Google Workspace. * Nástroj bude obsahovat integrovanou funkci analýzy neznámých vzorků v prostředí cloudového sandboxu. |  |
| Detekci a správu zranitelností (VAPM) | * Nástroj bude obsahovat integrovanou součást agenta poskytovatele bezpečnostní platformy bez nutnosti instalace dalších komponent. * Nástroj bude podporovat operační systémy Windows, Linux a macOS. * Nástroj bude umožňovat správu všech detekovaných zranitelností a jejich dostupných záplat přes centrální správu výrobce bezpečnostního řešení. * Nástroj bude obsahovat informace o zranitelnostech ve standardizovaném formátu CVE, včetně data zařazení, popisu povahy zranitelnosti a odkazu na zdroj s podrobnostmi. * Nástroj bude přidělovat každé zranitelnosti "bezpečnostní skóre" dle databáze CVSS 3.0 či novější. * Nástroj bude integrovaný v centrálním managementu bezpečnostního nástroje výrobce. * Nástroj bude umožňovat skenování zranitelností na vyžádání. * Nástroj bude umožňovat ruční spuštění záplaty podporované aplikace. * Nástroj bude umožňovat automatické spuštění záplaty podporované aplikace podle časových kritérií s možností výběru aplikací pomocí blacklist/whitelist logiky. * Nástroj bude umožňovat automatizované spuštění záplaty vybrané aplikace podle definovaných podmínek, například dle skóringu zranitelnosti, konkrétních CVE nebo verzí aplikací. * Nástroj bude umožňovat automatické záplatování Windows OS s možností definice typů aktualizací, včetně kritických a důležitých updatů. * Nástroj bude umožňovat definovat minimální prostor na disku potřebný pro stažení a aplikaci záplat. * Nástroj bude umožňovat vynucení instalace záplaty po uplynutí stanovené lhůty. * Nástroj bude řešit notifikaci uživatele v případě potřeby restartu aplikace, přičemž aplikace nebude bez vyzvání restartována. * Nástroj bude řešit možnost odložení restartu zařízení v případě potřeby jeho restartování po instalaci záplaty. |  |
| Správa mobilních zařízení | * Nástroj bude obsahovat podporu operačních systémů Android, iOS a iPadOS. * Nástroj bude umožňovat centrální správu zařízení pomocí management konzole výrobce bezpečnostního řešení. * Nástroj bude umožňovat registraci zařízení v režimu vlastníka nebo prostřednictvím Apple Business Manager (ABM). * Nástroj bude umožňovat integraci s managementem zařízení Microsoft Intune. * Nástroj bude řešit správu účtů (email, LDAP, Exchange…). * Nástroj bude umožňovat konfiguraci restrikcí na spravovaných zařízeních. * Nástroj bude umožňovat vynucení složitosti zámku obrazovky zařízení. * Nástroj bude umožňovat definici informací na zamčené obrazovce (např. kontaktní údaje společnosti). * Nástroj bude obsahovat ochranu před výměnou SIM karty s možností definice důvěryhodné SIM. * Nástroj bude obsahovat detekci roamingu. * Nástroj bude umožňovat lokalizaci zařízení. * Nástroj bude obsahovat podporu anti-theft akcí (siréna, zámek telefonu, vzdálené smazání dat). * Nástroj bude umožňovat filtrování hovorů a SMS s definicí časových slotů pro uplatnění pravidel. * Nástroj bude umožňovat WebControl s možností filtrování obsahu webu. * Nástroj bude umožňovat Application Control s možností vynucení požadovaných aplikací. * Nástroj bude umožňovat správu aktualizací systému. * Požadavky na antivirové zabezpečení:   + Nástroj bude obsahovat podporu antivirového zabezpečení pro operační systém Android.   + Nástroj bude obsahovat rezidentní ochranu běžící a chránící zařízení v reálném čase.   + Nástroj bude umožňovat definici naplánovaných kontrol.   + Nástroj bude umožňovat kontrolu výměnných zařízení.   + Nástroj bude obsahovat detekci potenciálně nechtěných aplikací.   + Nástroj bude umožňovat definici aktualizačního serveru.   + Nástroj bude obsahovat ochranu proti phishingu.   + Nástroj bude obsahovat detekci phishingových URL v SMS zprávách.   + Nástroj bude umožňovat instalaci a odinstalaci aplikací třetích stran.   + Nástroj bude umožňovat vyčítání informací o verzích softwaru třetích stran.   + Nástroj bude umožňovat vyčítání informací o hardwaru na spravovaných zařízeních. |  |
| Dvoufaktorová autentizace | * Nástroj bude umožňovat doručení OTP aplikací v mobilním zařízení. * Nástroj bude umožňovat doručení OTP e-mailem. * Nástroj bude umožňovat doručení OTP bezpečnostním tokenem. * Nástroj bude umožňovat doručení OTP SMS zprávou. * Nástroj bude umožňovat konfiguraci vlastní SMS brány pro doručení OTP kódu. * Nástroj bude umožňovat doručení OTP vlastní aplikací. * Nástroj bude podporovat ověřování metodou FIDO. * Nástroj bude umožňovat ověřování pomocí Push Authentication. * Aplikace výrobce s podporou Push-Notifications pro platformy: * Nástroj bude podporovat push notifikace pro iOS. * Nástroj bude podporovat push notifikace pro Android. * Nástroj bude podporovat push notifikace pro watchOS a Wear OS. * Požadavky na aplikaci výrobce systému:   + Nástroj bude obsahovat mobilní aplikaci v hlavních jazykových lokalizacích včetně češtiny.   + Nástroj bude umožňovat přístup do mobilní aplikace chráněný PINem nebo biometrikou.   + Nástroj bude umožňovat generování OTP v off-line prostředí (bez internetového připojení, bez GSM spojení). * Další požadavky:   + Nástroj bude podporovat hardwarové tokeny HOTP splňující standard OATH.   + Nástroj bude podporovat hardwarové tokeny certifikované výrobcem.   + Nástroj bude umožňovat kompletně softwarové řešení bez nutnosti nákupu dalšího hardwaru.   + Nástroj bude podporovat time-based hardwarové tokeny (PSKC).   + Nástroj bude umožňovat self-enrollment uživatelů. |  |
| Další požadavky | * Nástroj bude v souladu s:   + ISO27001 Standard,   + PCI/DSS - The Payment Card Industry Data Security Standard,   + ISAE 3402 – International Standards for Assurance Engagements no. 3402,   + HIPAA - Health Insurance Portability and Accountability Act,   + FFIEC - Federal Financial Institutions Examination Council compliances,   + Technická podpora v češtině. |  |

## Požadavky na záruky

Zadavatel požaduje záruku na veškeré dodané technologie v délce trvání minimálně **24 měsíců** od okamžiku předání díla, není-li u konkrétního zařízení či komponenty požadováno jinak v specifikaci ZD

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.

## Požadavky na technickou podporu

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

* **Technická podpora:** 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.
* **Nové verze a aktualizace:** Úpravy a změny softwaru, aby zůstal kompatibilní s měnícím se prostředím. To může zahrnovat aktualizace pro nové operační systémy, hardware nebo jiné softwarové závislosti. Soulad SW s platnou legislativou.
* **Optimalizace provozu:** 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.

**Garantovaná doba reakce Poskytovatele od nahlášení požadavku na poskytnutí technické podpory**

1. Služba je poskytována Pracovníky Poskytovatele v okamžiku, kdy dojde k zadání Požadavku.
2. Obsahem této služby je reakce Poskytovatele na Požadavky dle jejich priority a zahájení řešení v rámci **Servisního kalendáře, tj. pracovní dny od 7:00 do 17:00**.
   1. Je-li požadavek nahlášen mimo pracovní dobu, je počátkem uvedené doby 7:00 hodin nejbližšího pracovního dne.
   2. Dodavatel je povinen zahájit řešení požadavku bezodkladně, nejpozději však do níže uvedených časů, viz tabulka Klasifikace požadavku a stavů.
3. Požadavek na provedení této služby zadávají Kontaktní osoby Objednatele nebo Poskytovatele zadáním Požadavku na Helpdesk Poskytovatele.
4. Zahájení řešení je primárně poskytováno Vzdáleným připojením pracovníka Poskytovatele. Pokud to technická povaha řešení Požadavku vyžaduje, bude realizován fyzický zásah pracovníka Poskytovatele v místě technologických center města Kroměříže, přesné místo bude vždy specifikováno v zadaném požadavku.

**Klasifikace požadavku a stavů**

|  |  |  |  |
| --- | --- | --- | --- |
| **Klasifikace** | **Definice** | **SLA zahájení řešení** | **Předpokládané vyřešení požadavku** |
| 1. Nahlášení požadavku | Potvrzení přijetí nahlášeného požadavku jedním z výše uvedených způsobů hlášení požadavku. | Nejpozději do 15 minut | Není specifikováno |
| 1. Kritický požadavek (A) | Události, které znemožňují přístup ke službám a datům poskytovaných Prvky IT, nebo jejich využívání, vážně ovlivňují plnění termínů nebo ziskovost, případně mají vliv na většinu uživatelů a služeb. | Nejpozději do 2 hodiny od nahlášení požadavku v rámci Servisního kalendáře | Do 8 hodin od zahájení řešení, dle servisního kalendáře |
| 1. Závažný požadavek (B) | Události, které významným způsobem degradují, nebo silně omezují funkcionalitu nebo službu Prvku IT, ale existuje náhradní řešení (činnost pokračuje v omezeném provozu). | Nejpozději do 5 hodin od nahlášení požadavku v rámci Servisního kalendáře | Do 16 hodin od zahájení řešení, dle servisního kalendáře |
| 1. Ostatní požadavky (C) | Všechny ostatní požadavky, neomezující řádné používání Informačního systému, které tvoří Prvky IT. | Nejpozději do druhého pracovního dne od nahlášení požadavku | Do 32 hodin od zahájení řešení, dle servisního kalendáře |
| 1. Změnové požadavky | Součinnost při implementaci změn a činnostech při nasazovaní nových prvků IT či jejich částí. | Nejpozději do 7 pracovních dní | Stanoveno dohodou |
| 1. Konzultace a návrh řešení, programátorské práce | Konzultace při řešení problémů nebo při úpravách prvků IT. | Nejpozději do 5 pracovních dní | Stanoveno dohodou |

Pro případ, že bude zadavatel požadovat služby rozšířené technické podpory podle písmena e) a f), budou tyto služby vyúčtovány po skončení kalendářního měsíce, ve kterém byly čerpány, v hodinové sazbě uvedené v Kalkulaci ceny, dle skutečně realizovaných hodin rozšířené servisní podpory. Předpokládaný rozsah služeb rozšířené technické podpory pro účely přípravy nabídky je 100 hodin / na 5 let.

**Ceny za služby technické podpory**

|  |  |  |
| --- | --- | --- |
| **Typ požadavku** | **Cena bez DPH** | **Měrná jednotka** |
| Servisní požadavek "A" |  | Člověkohodina |
| Servisní požadavek "B" |  | Člověkohodina |
| Servisní požadavek "C" |  | Člověkohodina |
| Změnový požadavek |  | Člověkohodina |
| Konzultace a návrh řešení, programátorské práce |  | Člověkohodina |
| Dopravné mimo město |  | Km |

# Část 3 Řízení přístupů a identit.

Stávající infrastruktura města Kroměříže obsahuje 4 produkčních serverů, na kterých je provozována virtualizace VMware vSphere 8. Virtualizační platforma je centrálně spravována přes vCenter 8.

Pro správu identit využívá MS Active Directory, verze OS Windows Server 2019 a identity management EOS4.

Objednavatel provozuje, či spravuje zařízení (HW + VMs Windows/Linux/appliance) a webových aplikací k zajištění správného chodu organizace. O správný běh těchto zařízení a aplikací se stará 15 interních uživatelských účtů, 35 externích uživatelských účtů, z toho může být cca 20 konkurenčních účtů.

|  |  |  |
| --- | --- | --- |
| Zdroje | Výrobce | Kusy |
| HW + VMs Linux servery |  | 10 |
| HW + VMs Windows servery |  | 60 |
| Virtualizační nody | 3x Dell, 1x Lenovo | 4 |
| Switche | HPE | 35 |
| WiFi AP | Ubiquiti UniFi | 40 |
| SAN + NAS | Dell, Synology | 4 |

Implementace

Součástí dodávky je:

1. Poskytnutí veškerých potřebných licencí – zahrnuje všechny potřebné softwarové a provozní licence pro správný chod nástroje, včetně licencí pro všechny moduly a funkce, které budou součástí implementace.
2. Předimplementační analýza a návrh řešení.
3. Analýza privilegovaných účtů, způsob užití a návrh implementace nástroje.
4. Instalace nástroje a veškerých potřebných SW komponent, popřípadě zprovoznění přístupu na cloud (pokud bude součástí řešení) – zahrnuje kompletní instalaci Nástroje, konfiguraci cloudového prostředí, nastavení přístupu pro administrátory.
5. Zprovoznění, nastavení a optimalizace provozu Nástroje – provedení všech potřebných nastavení pro plně funkční provoz Nástroje, včetně optimalizace výkonu, konfigurace parametrů a zajištění správného chodu všech procesů, aby bylo dosaženo maximální efektivity.
6. Předání instalační a provozní dokumentace – dodání podrobné dokumentace v českém jazyce, která obsahuje kompletní výčet všech potřebných úkonů pro správnou instalaci, konfiguraci a údržbu Nástroje. Dokumentace také zahrnuje návody pro administrátory.
7. Proškolení obsluhy – realizace školení pro administrátory Nástroje, které zahrnuje jak základní, tak pokročilé funkce Nástroje. Školení bude zaměřeno na efektivní využívání Nástroje a jeho správu.

## Řízení přístupů a identit

|  |  |  |
| --- | --- | --- |
| **Požadavek** | **Minimální plnění** | **Dodavatel uvede, jestli splňuje požadavky (ano/ne) a navíc popíše jakým způsobem** |
| Výrobce a licenční program |  |  |
| Licence | * nevýhradní licence minimálně na 5 let |  |
| Základní vlastnosti | * Licence pro technologii určenou pro správu přístupů ke kritické infrastruktuře * Nástroj je dodáván jako fully packaged software (obsahuje i OS) s podporou pro virtuální prostředí jako Hyper-V/VMWARE či možností instalace do cloudové infrastruktury (Amazon Web Services, Microsoft Azure). Možnost instalace do cloudové infrastruktury (Amazon Web Services, Microsoft Azure) * Podpora instalace v režimu vysoké dostupnosti. * Systém dokáže fungovat jako jednotný přístupový bod pro několik instancí v necentralizované infrastruktuře. * Nástroj funguje jako přístupová proxy. * Nástroj podporuje protokoly SSH a RDP protokoly pro primární spojení, tedy mezi privilegovaným účtem a proxy. * Nástroj podporuje protokoly SSH, RDP, VNC, RLOGIN a TELNET pro sekundární spojení, tedy mezi proxy a monitorovaným systémem. * Nástroj u nepodporovaných protokolů umožňuje spuštění klientské aplikace na Jump serveru tak, aby uživateli byla přístupná pouze daná klientská aplikace. * Nástroj podporuje integraci s externími uživatelskými databázemi v minimálním rozsahu LDAP/LDAPS/Microsoft Active Directory/RADIUS/KERBEROS/TACACS+ * Nástroj nevyžaduje žádné instalace software agentů na monitorovaný systém. * Nástroj umožňuje uživatelskou autentizaci pomocí jména / hesla, X.509 certifikátu či SSH klíče. * Integrace nástroje s LDAP či Active Directory nezávisí na periodických synchronizacích. Systém mapuje schémata uživatelských skupin z LDAP/AD do lokálních PAM skupin. * Nástroj umožňuje tvorbu účtů s rozdílnými rolemi – minimálně správce, uživatel a auditor. * Nástroj umožňuje definici uživatelů, spravovaných zařízení a jejich skupin, u kterých bude jednotlivým auditorským účtům uděleno oprávnění prohlížet záznamy. * Nástroj umožňuje konfigurace uživatelských profilů se zahrnutím možnosti filtrovat příchozí připojení na základě zdrojové IP adresy, síťové adresy a masky sítě či FQDN. * Nástroj umožňuje definování cílových systémů zadáním IP adresy, DNS nebo zadáním IP adresy a masky. * Nástroj umožňuje definování přístupových politik přiřazováním uživatelských účtů či skupin k cílovým systémům či jejich skupinám. * Nástroj podporuje integraci se SIEM/SYSLOG. * Nástroj umožňuje zaznamenávání všech zprostředkovaných relací formou videozáznamu s doplňujícími metadaty. * Nástroj umožňuje aktivaci / deaktivaci zaznamenání relací dle jednotlivých uživatelských skupin. * Nástroj umožňuje shlédnutí záznamů relací prostřednictvím webového rozhraní. * Nástroj umožňuje následný export videozáznamu do běžně podporovaného typu souboru (.mp4 či .flv) * Nastroj umožňuje ukládání zaznamenaných relací lokálně či na externí úložiště CIFS/NFS. * Nástroj zaznamenává a uchovává všechny uživatelem zadané příkazy v průběhu SSH relací. * Nástroj zaznamenává a uchovává názvy všech oken a procesů otevřených v průběhu RDP relace. * Nástroj umožňuje sběr metadata v průběhu RDP relace. * Nástroj u relací SSH umožňuje definovat vzory regulárních výrazů pro prováděné příkazy, a pokud je takový vzor detekován, umožní nastavit jednu z akcí: ukončení relace nebo odeslání oznámení o detekci vzoru. * Nástroj umožňuje přiřazení definovaných vzorů k monitoringu / ukončování relací k vybraným skupinám uživatelů či systémů. * Nástroj poskytuje ochranu hesel zadávaných v průběhu RDP relace prostřednictvím detekce vstupu kurzoru do pole pro vyplnění hesla či UAC (User Account Control) okna. * Nástroj umožňuje schvalování přístupu privilegovaného uživatele k určitým monitorovaným systémům. Schvalování přístupu musí fungovat minimálně v následujícím rozsahu:   + Privilegovaný uživatel požádá o přístup   + Definovaní uživatelé obdrží žádost o schválení přístupu.   + Minimální definovaný počet uživatelů schválí žádost.   + Privilegovaný uživatel po schvalovacím procesu automaticky získá přístup k monitorovanému systému. * Nástroj umožňuje vyžadování výše uvedených schvalování v určitých časových rámcích- např. Pondělí-pátek, 9:00-16:00 bez potřeby schválení, v jiných časech pouze po schválení. * Správce nástroje/auditor má možnost pozorovat probíhající relace v reálném čase, včetně možnosti pozorovanou relaci ukončit. * Při auditu či kontrole proběhlé relace má nástroj možnost zobrazit metadata a videozáznam relace na jedné stránce s časovou osou propojující metadata s vizuální reprezentací. * Nástroj dokáže pracovat se sdílenými účty s možností určení, kdo v daný moment tento účet využíval. * Nástroj poskytuje různé metody autentizace privilegovaných uživatelů na monitorovaných systémech, minimálně:   + Autentizace privilegovaného uživatele na monitorovaném systému pomocí stejných přihlašovacích údajů, které byly využity pro autentizaci na proxy.   + Autentizace privilegovaného uživatele na monitorovaném systému pomocí statických a bezpečně uložených přihlašovacích údajů. (např. root, admin, privilegovaný lokální účet).   + Vyzváním uživatele k opětovnému zadání přihlašovacích údajů k monitorovanému systému, bez jejich zaznamenání. * Nástroj umožňuje vyhledávání systémů a privilegovaných účtů formou scanování RDP + SSH portů a importů z AD. * Nástroj disponuje mechanismem pro plnou či částečnou automatizaci onboardingu nově nalezených zařízení / účtů. * Nástroj lze rozšířit o modul umožňující centralizaci přístupu k několika odděleným instancím prostřednictvím jednotného webového HTML5 rozhraní s integrovaným RDP a SSH klientem pro primární spojení. * Modul pro centralizaci přístupů podporuje prohlížeče Internet Explorer, Microsoft Edge, Google Chrome a Mozilla Firefox bez potřeby instalace pluginů (java, flash) * Modul pro centralizaci přístupů je dodán jako aplikace běžící na jednom z těchto OS: Microsoft Windows Server 2012 R2, Microsoft Windows Server 2016 (x64), Red Hat Enterprise Linux, CentOS 6.6, Red Hat Entreprise Linux, CentOS 7.1, Debian 8 (amd64). * Modul pro centralizaci přístupů umožňuje auditorským účtům globální vyhledávání napříč metadaty ze všech realizovaných relací všech instancí nástroje. * Technologie umožňuje automatické rotace hesel a SSH klíčů. * Technologie umožňuje vytvářet různé plány automatické změny hesel a SSH klíčů na cílových systémech. * Technologie podporuje přístup pomocí jednorázových hesel s omezenou platností pro RDP a SSH relace * Technologie podporuje vlastní zásady/požadavky na změnu hesla:   + Požadovaný minimální počet znaků,   + Vyloučení znaků určených správcem,   + Povinná velká a malá písmena,   + Požadované speciální znaky |  |

## Požadavky na záruky

Zadavatel požaduje záruku na veškeré dodané technologie v délce trvání minimálně **24 měsíců** od okamžiku předání díla, není-li u konkrétního zařízení či komponenty požadováno jinak v specifikaci ZD

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.

## Požadavky na technickou podporu

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

* **Technická podpora:** 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.
* **Nové verze a aktualizace:** Úpravy a změny softwaru, aby zůstal kompatibilní s měnícím se prostředím. To může zahrnovat aktualizace pro nové operační systémy, hardware nebo jiné softwarové závislosti. Soulad SW s platnou legislativou.
* **Optimalizace provozu:** 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.

**Garantovaná doba reakce Poskytovatele od nahlášení požadavku na poskytnutí technické podpory**

1. Služba je poskytována Pracovníky Poskytovatele v okamžiku, kdy dojde k zadání Požadavku.
2. Obsahem této služby je reakce Poskytovatele na Požadavky dle jejich priority a zahájení řešení v rámci **Servisního kalendáře, tj. pracovní dny od 7:00 do 17:00**.
   1. Je-li požadavek nahlášen mimo pracovní dobu, je počátkem uvedené doby 7:00 hodin nejbližšího pracovního dne.
   2. Dodavatel je povinen zahájit řešení požadavku bezodkladně, nejpozději však do níže uvedených časů, viz tabulka Klasifikace požadavku a stavů.
3. Požadavek na provedení této služby zadávají Kontaktní osoby Objednatele nebo Poskytovatele zadáním Požadavku na Helpdesk Poskytovatele.
4. Zahájení řešení je primárně poskytováno Vzdáleným připojením pracovníka Poskytovatele. Pokud to technická povaha řešení Požadavku vyžaduje, bude realizován fyzický zásah pracovníka Poskytovatele v místě technologických center města Kroměříže, přesné místo bude vždy specifikováno v zadaném požadavku.

**Klasifikace požadavku a stavů**

|  |  |  |  |
| --- | --- | --- | --- |
| **Klasifikace** | **Definice** | **SLA zahájení řešení** | **Předpokládané vyřešení požadavku** |
| 1. Nahlášení požadavku | Potvrzení přijetí nahlášeného požadavku jedním z výše uvedených způsobů hlášení požadavku. | Nejpozději do 15 minut | Není specifikováno |
| 1. Kritický požadavek (A) | Události, které znemožňují přístup ke službám a datům poskytovaných Prvky IT, nebo jejich využívání, vážně ovlivňují plnění termínů nebo ziskovost, případně mají vliv na většinu uživatelů a služeb. | Nejpozději do 2 hodiny od nahlášení požadavku v rámci Servisního kalendáře | Do 8 hodin od zahájení řešení, dle servisního kalendáře |
| 1. Závažný požadavek (B) | Události, které významným způsobem degradují, nebo silně omezují funkcionalitu nebo službu Prvku IT, ale existuje náhradní řešení (činnost pokračuje v omezeném provozu). | Nejpozději do 5 hodin od nahlášení požadavku v rámci Servisního kalendáře | Do 16 hodin od zahájení řešení, dle servisního kalendáře |
| 1. Ostatní požadavky (C) | Všechny ostatní požadavky, neomezující řádné používání Informačního systému, které tvoří Prvky IT. | Nejpozději do druhého pracovního dne od nahlášení požadavku | Do 32 hodin od zahájení řešení, dle servisního kalendáře |
| 1. Změnové požadavky | Součinnost při implementaci změn a činnostech při nasazovaní nových prvků IT či jejich částí. | Nejpozději do 7 pracovních dní | Stanoveno dohodou |
| 1. Konzultace a návrh řešení, programátorské práce | Konzultace při řešení problémů nebo při úpravách prvků IT. | Nejpozději do 5 pracovních dní | Stanoveno dohodou |

Pro případ, že bude zadavatel požadovat služby rozšířené technické podpory podle písmena e) a f), budou tyto služby vyúčtovány po skončení kalendářního měsíce, ve kterém byly čerpány, v hodinové sazbě uvedené v Kalkulaci ceny, dle skutečně realizovaných hodin rozšířené servisní podpory. Předpokládaný rozsah služeb rozšířené technické podpory pro účely přípravy nabídky je 100 hodin / na 5 let.

**Ceny za služby technické podpory**

|  |  |  |
| --- | --- | --- |
| **Typ požadavku** | **Cena bez DPH** | **Měrná jednotka** |
| Servisní požadavek "A" |  | Člověkohodina |
| Servisní požadavek "B" |  | Člověkohodina |
| Servisní požadavek "C" |  | Člověkohodina |
| Změnový požadavek |  | Člověkohodina |
| Konzultace a návrh řešení, programátorské práce |  | Člověkohodina |
| Dopravné mimo město |  | Km |

# Část 4 Pořízení a implementace nástroje pro analýzu a monitoring síťového provozu

1. Poskytnutí veškerých potřebných licencí – zahrnuje všechny potřebné softwarové a provozní licence pro správný chod nástroje, včetně licencí pro všechny moduly a funkce, které budou součástí implementace.
2. Předimplementační analýza a návrh variant řešení.
3. Instalace nástroje a veškerých potřebných SW komponent, popřípadě zprovoznění přístupu na cloud (pokud bude součástí řešení) – zahrnuje kompletní instalaci Nástroje, konfiguraci cloudového prostředí, nastavení přístupu pro administrátory.
4. Zprovoznění, nastavení a optimalizace provozu Nástroje – provedení všech potřebných nastavení pro plně funkční provoz Nástroje, včetně optimalizace výkonu, konfigurace parametrů a zajištění správného chodu všech procesů, aby bylo dosaženo maximální efektivity.
5. Předání instalační a provozní dokumentace – dodání podrobné dokumentace v českém jazyce, která obsahuje kompletní výčet všech potřebných úkonů pro správnou instalaci, konfiguraci a údržbu Nástroje. Dokumentace také zahrnuje návody pro administrátory.
6. Proškolení obsluhy – realizace školení pro administrátory Nástroje, které zahrnuje jak základní, tak pokročilé funkce Nástroje. Školení bude zaměřeno na efektivní využívání Nástroje a jeho správu.

## Pořízení a implementace nástroje pro analýzu a monitoring síťového provozu

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Minimální požadavek** |  |
| Výrobce, název, verze a licenční program | (doplnit) |  |
| Licence | * Nevýhradní licence v délce trvání minimálně 5 let |  |
| Data | * Minimální doba uložení dat pro analýzu bude 6 měsíců. Požadavek musí odpovídat platné legislativě. |  |
| Funkce | * HW appliance * Počet monitorovacích portů minimálně 2 x 1000 MbE * Pasivní zapojení bez vlivu na monitorovanou síť (zapojení pomocí TAPů, případně v kombinaci se SPAN/mirror porty). * Cache minimálně 0,5 M * Podpora flow dat minimálně - NetFlow v5/v9, IPFIX, NetStream, jFlow, cflowd * Podpora IPv4, IPv6, VLAN, MPLS, Ethernet 10Mb/s až 100Gb/s * Sběr síťových statistik ze vzdálených lokalit s centrálním přístupem k reportům, incidentům a síťovým statistikám a centrální správou systému. * Bezztrátový sběr dat na kolektorech z různých datových zdrojů, podpora standardizovaných protokolů pro výměnu dat o IP tocích (NetFlow v5, NetFlow v9 – RFC3954, IPFIX, jFlow, cflowd, NetStream). * Dlouhodobé ukládání statistik IP toků a jejich centrální sledování a vyhodnocování bezpečnostních hrozeb v síti, prokazování bezpečnostních incidentů. * Reporty a alerty minimálně - e-mail, PDF/CSV, syslog, SNMP, packet capture trigger, script trigger * Otevřené rozhraní a dokumentované API s možností integrace nástrojů i třetích stran. * Podpora pro nativní nasazení v prostředí Microsoft Azure. Podpora pro zpracování dat zrcadleného provozu v Microsoft Azure. * Zabezpečená vzdálená správa, dohled a konfigurace – SSH, HTTPS. * Správa uživatelů a přístupových práv na zařízení prostřednictvím uživatelských rolí. * Vestavěný kolektor pro dočasné ukládání flow statistik (zajištění redundance), který zahrnuje plnohodnotnou funkcionalitu flow kolektoru. * Podpora autentizace vůči LDAP (Active Directory). * Použití DNS cache na zařízení pro rychlejší překlad IP adres na doménová jména. * Zpracování datového provozu IPv4 a IPv6, VLAN, MPLS a jejich reportování na kolektor. * Monitorování provozu v tunelu (dekapsulace) GRE, VxLAN, ESP a OTV. * Uživatelsky definovatelné šablony pro protokoly NetFlow v9 a IPFIX. * Monitorování a reportování MAC adres ve flow statistikách. Možnost použít MAC adresu jako položku klíče flow záznamu. * Reportování RTT, SRT, delay, jitter, retransmise, out-of-order pakety jako součást flow statistik. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX). * Monitorování a analýza HTTP provozu - včetně položek typu URL, hostname, stavový kód HTTP, dotazovací metoda. Pro HTTPS reportování hostname jako SNI. Použití standardní technologie reportování těchto rozšiřujících statistik (IPFIX). * Identifikace operačního systému vč. jeho verze. Identifikace internetového prohlížeče vč. jeho verze. Použití standardní technologie reportování těchto rozšiřujících statistik (IPFIX). * Monitorování VoIP statistik, protokol SIP – položky typu SIP URI, jitter, latence, ztrátovost paketů. Použití standardní technologie reportování těchto rozšiřujících statistik IPFIX). * Monitorování a analýza DNS provozu - položky jako typ dotazu, dotazovaná doména, návratová hodnota, odpověď. Použití standardní technologie reportování těchto rozšiřujících statistik (IPFIX). * Monitorování a analýza SMB/CISF provozu – položky typu síťová cesta, název souboru, typ operace. Použití standardní technologie reportování těchto rozšiřujících statistik (IPFIX). * Monitorování DHCP provozu – položky jako typ DHCP požadavku, originální MAC adresa. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX). * Monitorování e-mailového provozu – protokolů SMTP, POP3, IMAP a položek jako uživatelské jméno, jméno odesílatele, selhání autentizace a další. Použití standardní technologie reportování těchto rozšiřujících statistik (IPFIX). * Monitorování Microsoft SQL provozu (TDS protokolu) – položky jako typ dotazu, verze klienta a serveru, uživatelské jméno a další. Použití standardní technologie reportování těchto rozšiřujících statistik (IPFIX). * Schopnost monitorování a reportování různých charakteristik provozu šifrovaného pomocí SSL/TLS. To zahrnuje verzi protokolu, šifrovací algoritmus, cipher suite, detaily certifikátu a další. * Monitorování rozšířených L3/L4 informací - TTL (Time to live), TCP Window size, TCP SYN packet size umožňujících detekci NATů. * Podpora vzorkování na úrovni paketů. Podpora vzorkování na úrovni toků. * Podpora filtrování dat na sondě na základě IP prefixů, VLAN, AS (pro různé cíle exportu různé statistiky). * Podpora vyplňování AS na základě vestavěného či dodaného seznamu. * Podpora pro nastavení hodnoty interface index pro exportované flow statistiky per monitorovací port. * Sonda umožňuje rozšíření o funkcionalitu záznamu provozu v plném rozsahu na základě pravidla záchytu definovaného uživatelem. * Rozšíření je řešeno formou licence/instalace SW bez nutnosti změny HW konfigurace. * Architektura systému umožňuje streamové zpracovávání flow dat pro rychlou detekci bezpečnostních nebo provozních anomálií. * Systém umožňuje deduplikovat flow statistiky před jejich vlastní analýzou. * Systém umožňuje korelovat toky před a za proxy serverem před jejich vlastní analýzou s cílem identifikovat provoz procházející proxy serverem a tento provoz přiřadit koncovému uživateli. * Systém podporuje vzorkování na úrovní toků před jejich vlastním zpracováním. * Systém umožňuje spravovat zdroje síťových toků, umožňuje dočasně pozastavit příjem toků a indikovat poruchu zdroje síťových toků. * Systém zobrazuje informace o identitě uživatelů obsaženou ve flow datech jako součást události. * Systém podporuje persistenci doménových jmen, tedy uložení doménové jména původce události v okamžiku zaznamenání výskytu této události. * Systém obsahuje předdefinovanou sadu detekčních metod a algoritmů pro analýzu flow statistik, detekci bezpečnostních incidentů, provozních problémů a síťových anomálií. * Detekce skenování portů, slovníkové útoky, útoky odepření služeb (DoS), útoky na síťové protokoly SSH, RDP, Telnet a další obdobné služby. * Detekce anomálií v DNS, DHCP, SMTP, multicast provozu a nestandardní komunikace. * Detekce P2P sítí, a VPN komunikace * Systém umožňuje identifikovat bezpečnostní události (např. komunikaci s botnet command & control centry, přístup na phishing servery, apod.) * využíváním zdrojů IP a host reputačních databází poskytovaných * výrobcem a aktualizovaných nejméně každých 24 hodin. Systém umožňuje zapojit další zdroje IP a host reputačních dat pro automatickou detekci. * Detekce nadměrné zátěže sítě, výpadků služeb, nových a cizích zařízení připojených k síti. * Detekce síťových anomálií na základě predikce budoucího chování sítě s využíváním znalosti historie komunikace. * Systém je schopen k jednotlivým detekcím vytvářet a evidovat události a umožňuje jejich analýzu v uživatelském prostředí * Systém obsahuje konfiguračního průvodce pro nastavení systému při prvním spuštění podle parametrů sítě, do kterého je systém nasazen. * Jednotlivé detekční schopnosti je možné konfigurovat a parametrizovat tak, aby bylo dosaženo maximální efektivity a minimálního počtu falešných poplachů. Detekční mechanismy je možné konfigurovat různým způsobem (např. s různou citlivostí) pro statistiky z různých segmentů sítě (např. LAN nebo DMZ). * Systém umožňuje spravovat detekční metody z uživatelského prostředí, vytvářet kopie detekčních metod a nastavit jejich individuální parametry. * Systém umožňuje definovat vlastní detekční metody pomocí poskytnutých příkazů, které vyhledávají ve flow statistikách (včetně informací z aplikační vrstvy) specifické vzory chování. Události detekované vlastními metodami jsou zpracovávány standardně jako události z dostupných detekčních metod (notifikace, reportování, atd.). * Detekce NATů v síti s využitím rozšířených informací z L3/L4. * Systém umožňuje definovat filtry vč. komplexních filtrů složených z dílčích filtrů. Pro zjednodušení definice filtrů je možné používat operace jako inverze nebo rozdíl filtrů. Filtry je možné exportovat do formátu XML nebo z tohoto formátu importovat. K jednotlivým záznamům a filtrům lze připojit uživatelský popis účelu. * Případné události, které představují falešné poplachy (false positives) je možné odstranit prostřednictvím jednoduché konfigurace pravidel pro vyloučení falešných poplachů dostupné v uživatelském rozhraní. * Systém umožňuje zastavit a opět spustit pravidla falešného poplachu, aby bylo možné ověřit jejich požadovanou funkčnost při běžném provozu * Systém umožňuje při vytváření pravidel pro falešné poplachy smazat již detekované falešné události. * Předdefinované priority událostí s možností uživatelského nastavení závažnosti událostí na základě IP adresních rozsahů, typů událostí, míst výskytu nebo detailů události. Jedna událost může mít v závislosti na konfiguraci přiřazeno více priorit. * Systém umožňuje předdefinovat uživatelské pohledy na události a prioritu dle uživatelských rolí. * Správa uživatelů a přístupových práv k událostem prostřednictvím uživatelských rolí. Separace událostí s omezením přístupu pro jednotlivé role/uživatele. * Události je možné reportovat do dohledových systémů prostřednictvím funkcionality SNMP trap. * Notifikace o detekovaných událostech prostřednictvím e-mailu s podporou různých formátů (HTML, incident handling systém, úsporný textový formát). Možnost připojit vzorek flow dat, na základě kterých byla událost detekována k e-mailovému reportu. * Systém integruje informace ze služeb DNS, WHOIS, geolokační služby. * Uživatelsky definované externí služby fungující na protokolu HTTP. * Systém je schopen za pomoci zabezpečeného komunikačního rozhraní získat další informace k IP adrese z adresářových služeb AD/LDAP. * Systém zaznamenává na základě definovaného pravidla záchytu síťový provoz v plném rozsahu (vrstvy L2-L7) a záznamy zachyceného síťového provozu ukládá v souboru s formátem PCAP, který je možno stáhnout z webového uživatelského prostředí pro následnou analýzu v programu třetí strany (např. Wireshark). * Systémem je možné provozovat celý na monitorovací sondě včetně webového rozhraním pro manuální zadávání požadavků na záchyt síťového provozu. Webové rozhraní sondy umožňuje definovat, na jakých monitorovacích rozhraních sondy bude prováděn záchyt. * Systém umožňuje pro jednotlivé záznamy definovat filtry a zachytávat tak část síťového provozu. Kritéria filtrace jsou parametry z vrstev L2-L4 a L7. * Systém umožňuje filtrovat síťový provoz podle VLAN tagu, MPLS značky. * Systém umožňuje filtrovat síťový provoz podle IPv4, IPv6 adresy, čísla sítě a masky. * Systém umožňuje filtrovat síťový provoz podle portů TCP, UDP a SCTP * Systém umožňuje filtrovat síťový provoz VoIP hovorů používající SIP a H.323 protokoly * Záchyt síťového provozu je možné spustit automaticky na základě detekce události systémem pro automatické vyhodnocování NetFlow dat. * Systém umožňuje analyzovat síťový provoz a výsledky analýzy prezentuje ve srozumitelné podobě v rámci událostí, které popisují, jak jednotlivé komunikace v záznamu provozu probíhaly. Události jsou rozlišovány podle závažnosti do několik úrovní a indikují problémy vzniklé v síťovém provozu na podporovaných protokolech. * Systém umožňuje analyzovat vlastní záznamy provozu nebo externí záznamy nahrané do systému ve formě souboru PCAP. * Systém podporuje nejčastěji používané protokoly v podnikových sítích včetně protokolů pro konfiguraci sítě (DHCP, DNS), e-mailovou komunikaci (IMAP, POP, SMTP), síťové úložiště a posílání dat (SMB, FTP), protokoly HTTP s SSL/TLS. Systém umožňuje analýzu i na nižších vrstvách a diagnostikuje chyby v protokolech TCP, IP. * Sondu je možné integrovat do dohledového systému pro kontrolu dostupnosti a vytížení zdrojů technologií SNMP. * SIEM podpora minimálně - Using CEF (over syslog), SNMP * Stream data processing minimálně 1000 (flows/s) * Behavior patterns processing minimálně 1000 (flows/s) * Data feeds minimáně 3 * Kompletní záznam síťového provozu L2-L7 na vyžádání a při konkrétní události (packet sniffing). * Vestvaěné expertní znalosti - Rozkliknutím výsledků analýzy lze procházet jednotlivé kroky a zobrazit vysvětlení možných příčin problémů a to včetně doporučení, jak daný problém řešit. * Provádění automatické analýzy rozhodovacího stromu síťových protokolů, jejich závislosti, RFC specifikací, chyb a okamžité informování o nalezených problémech a jejich závažnosti. * Systém umožňuje postupné rozšiřování řešení pro automatické vyhodnocení přidáním dalších instancí systému při zachování jednoho uživatelského rozhraní pro dané řešení bez ohledu na počet zapojených instancí. * Systém detekce anomálií poskytuje dokumentované API pro získávání a zpracování událostí. Prostřednictvím API je možné systém detekce anomálií rovněž konfigurovat (např. vytvářet filtry, měnit nastavení detekčních metod, apod.). * Události je možné exportovat do formátu CSV pro další zpracování. * Předdefinovaná sada reportů s možností plné konfigurace uživatelem. Reporty dostupné prostřednictvím webového uživatelského rozhraní, ve formátu PDF. Automatická distribuce reportů e-mailem. * Systém umožňuje interaktivní vizualizaci detekovaných událostí formou grafické reprezentace flow statistik, na základě kterých byla událost rozpoznána. * Systém nabízí flexibilní uživatelské rozhraní pro vyhledávání událostí dle různých parametrů (typ události, IP adrese původce události, filtr, přiřazení události do kategorie, ID události apod.). Události je možné prezentovat různým způsobem (prostý seznam, agregace dle zdrojů, dle cílů apod.). * Webové uživatelské rozhraní v českém jazyce. Uživatelsky definovatelný dashboard (konfigurace per uživatel). Vizualizace průběhu provozu s vyznačením detekovaných událostí v závislosti na nastavené závažnosti událostí. * Plná zákaznická podpora v českém jazyce. |  |
| Implementace | * Instalace sondy a propojení se sběrnými porty - flowdata * Sběr dat, vyhodnocení a analýza provozu * Konfigurace bezpečnostních pravidel a alertů * Propojení na dohledové centrum |  |
| Podpora | * Propojení na dohledové centrum zajišťující komplexní monitoring infrastruktury v pracovní dny od 6h do 18h. * Fyzický operátor zajišťující okamžitou komunikaci směrem k servisní podpoře na straně objednavatele, bezpečnostní specialista, garantující správné vyhodnocení bezpečnostní události a garanci následného řešení. * Konzole pro dohled k dispozici 24x7 pro správce na straně objednatele služby * Automatizované vyhodnocování událostí a korelace událostí * Měsíční zasílání reportů a statistik monitorovaných dat * Pravidelná správa a dohled nad provozem monitorovacího zařízení včetně všech provozních i bezpečnostních aktualizací na denní bázi |  |

## Požadavky na záruky

Zadavatel požaduje záruku na veškeré dodané technologie (HW a SW) v délce trvání minimálně **24 měsíců** od okamžiku předání díla, není-li u konkrétního zařízení či komponenty požadováno jinak v specifikaci ZD.

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

## Požadavky na technickou podporu

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

* **Technická podpora:** 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.
* **Nové verze a aktualizace:** Úpravy a změny softwaru, aby zůstal kompatibilní s měnícím se prostředím. To může zahrnovat aktualizace pro nové operační systémy, hardware nebo jiné softwarové závislosti.
* **Optimalizace provozu:** 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.

**Garantovaná doba reakce Poskytovatele od nahlášení požadavku na poskytnutí technické podpory**

1. Služba je poskytována Pracovníky Poskytovatele v okamžiku, kdy dojde k zadání Požadavku.
2. Obsahem této služby je reakce Poskytovatele na Požadavky dle jejich priority a zahájení řešení v rámci **Servisního kalendáře, tj. pracovní dny od 7:00 do 17:00**.
   1. Je-li požadavek nahlášen mimo pracovní dobu, je počátkem uvedené doby 7:00 hodin nejbližšího pracovního dne.
   2. Dodavatel je povinen zahájit řešení požadavku bezodkladně, nejpozději však do níže uvedených časů, viz tabulka Klasifikace požadavku a stavů.
3. Požadavek na provedení této služby zadávají Kontaktní osoby Objednatele nebo Poskytovatele zadáním Požadavku na Helpdesk Poskytovatele.
4. Zahájení řešení je primárně poskytováno Vzdáleným připojením pracovníka Poskytovatele. Pokud to technická povaha řešení Požadavku vyžaduje, bude realizován fyzický zásah pracovníka Poskytovatele v místě technologických center města Kroměříže, přesné místo bude vždy specifikováno v zadaném požadavku.

**Klasifikace požadavku a stavů**

|  |  |  |  |
| --- | --- | --- | --- |
| **Klasifikace** | **Definice** | **SLA zahájení řešení** | **Předpokládané vyřešení požadavku** |
| 1. Nahlášení požadavku | Potvrzení přijetí nahlášeného požadavku jedním z výše uvedených způsobů hlášení požadavku. | Nejpozději do 15 minut | Není specifikováno |
| 1. Kritický požadavek (A) | Události, které znemožňují přístup ke službám a datům poskytovaných Prvky IT, nebo jejich využívání, vážně ovlivňují plnění termínů nebo ziskovost, případně mají vliv na většinu uživatelů a služeb. | Nejpozději do 6 hodiny od nahlášení požadavku v rámci Servisního kalendáře | Do 12 hodin od zahájení řešení, dle servisního kalendáře |
| 1. Závažný požadavek (B) | Události, které významným způsobem degradují, nebo silně omezují funkcionalitu nebo službu Prvku IT, ale existuje náhradní řešení (činnost pokračuje v omezeném provozu). | Nejpozději do 10 hodin od nahlášení požadavku v rámci Servisního kalendáře | Do 24 hodin od zahájení řešení, dle servisního kalendáře |
| 1. Ostatní požadavky (C) | Všechny ostatní požadavky, neomezující řádné používání Informačního systému, které tvoří Prvky IT. | Nejpozději do 14 hodin od nahlášení požadavku v rámci Servisního kalendáře | Do 32 hodin od zahájení řešení, dle servisního kalendáře |
| 1. Změnové požadavky | Součinnost při implementaci změn a činnostech při nasazovaní nových prvků IT či jejich částí. | Nejpozději do 7 pracovních dní | Stanoveno dohodou |
| 1. Konzultace a návrh řešení, programátorské práce | Konzultace při řešení problémů nebo při úpravách prvků IT. | Nejpozději do 5 pracovních dní | Stanoveno dohodou |

Pro případ, že bude zadavatel požadovat služby rozšířené technické podpory podle písmena e) a f), budou tyto služby vyúčtovány po skončení kalendářního měsíce, ve kterém byly čerpány, v hodinové sazbě uvedené v Kalkulaci ceny, dle skutečně realizovaných hodin rozšířené servisní podpory. Předpokládaný rozsah služeb rozšířené technické podpory pro účely přípravy nabídky je 100 hodin / na 5 let.

**Ceny za služby technické podpory**

|  |  |  |
| --- | --- | --- |
| **Typ požadavku** | **Cena bez DPH** | **Měrná jednotka** |
| Servisní požadavek "A" |  | Člověkohodina |
| Servisní požadavek "B" |  | Člověkohodina |
| Servisní požadavek "C" |  | Člověkohodina |
| Změnový požadavek |  | Člověkohodina |
| Konzultace a návrh řešení, programátorské práce |  | Člověkohodina |
| Dopravné mimo město |  | Km |

# Část 5 Pořízení a implementace nástroje pro log management

1. Poskytnutí veškerých potřebných licencí – zahrnuje všechny potřebné softwarové a provozní licence pro správný chod nástroje, včetně licencí pro všechny moduly a funkce, které budou součástí implementace.
2. Předimplementační analýza a návrh řešení.
3. Instalace nástroje a veškerých potřebných SW komponent, popřípadě zprovoznění přístupu na cloud (pokud bude součástí řešení) – zahrnuje kompletní instalaci Nástroje, konfiguraci cloudového prostředí, nastavení přístupu pro administrátory.
4. Zprovoznění, nastavení a optimalizace provozu Nástroje – provedení všech potřebných nastavení pro plně funkční provoz Nástroje, včetně optimalizace výkonu, konfigurace parametrů a zajištění správného chodu všech procesů, aby bylo dosaženo maximální efektivity.
5. Předání instalační a provozní dokumentace – dodání podrobné dokumentace v českém jazyce, která obsahuje kompletní výčet všech potřebných úkonů pro správnou instalaci, konfiguraci a údržbu Nástroje. Dokumentace také zahrnuje návody pro administrátory.
6. Proškolení obsluhy – realizace školení pro administrátory Nástroje, které zahrnuje jak základní, tak pokročilé funkce Nástroje. Školení bude zaměřeno na efektivní využívání Nástroje a jeho správu.

## Pořízení a implementace nástroje pro log management

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Minimální požadavek** |  |
| Výrobce, název, verze a licenční program | (doplnit) |  |
| Katalogový list produktu | (doplnit odkaz na web nebo do přílohy nabídky)  Požadujeme předložit link na online dokumentaci nebo připojit pdf aktuální kompletní dokumentace k ověření jednotlivých vlastností navrhovaného systému. |  |
| Licence | * Nevýhradní licence v délce trvání minimálně 5 let |  |
| Data | * Minimální doba uložení dat pro analýzu bude 6 měsíců. Požadavek musí odpovídat platné legislativě. |  |
| Funkce | * Systém pracuje 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. * Systém provádí zpracování událostí z předdefinovaných zdrojů logů napříč výrobci aplikací, operačních systémů a síťového hardware. * Veškerá konfigurace systému se musí provádět v grafickém rozhraní jednotné uživatelské webové konzole. Systém poskytuje podporu pro vizuální programování pro všechny kroky zpracování strojových dat. Ve webové konzoli se nepřipouští konfigurace za využití skriptů, maker nebo textových konfiguračních polí, do kterých se složité textové skripty/makra vkládají. * Systém umožňuje dopsání parserů pro výše neuvedená zařízení uživatelem bez nutnosti spolupráce s výrobcem nebo dodavatelem (vč. subdodavatelů) nabízeného systému - Uživatelsky definované parsery. * 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. * 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 výrobce popisující funkčnost třídění vstupních dat. * Systém přijímá a zpracovává logy, události a další strojově generovaná data prostřednictvím minimálně následujících protokolů: SYSLOG (dle RFC3164, RFC5424, RFC5425) a RELP. Systém musí umožňovat příjem logů i na rozsahu alespoň 50 UDP a TCP portů pro zjednodušené třídění vstupních zpráv. Dále požadujeme podporu sběru strojových dat z databází s nastavením v grafickém menu systému minimálně pro databáze MSSQL, MySQL, Oracle a PostgreSQL a to bez nutnosti instalovat na databázový server doplňkový software nebo agenta. * 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. * Hodnoty jednotlivých parsovaných polí je možné v definici parseru přetypovat a standardizovat alespoň na tyto základní druhy: číslo, IP adresa, MAC adresa, URL. Nad uloženými čísly je pak možné při prohledávání dat provádět matematické operace (součty všech hodnot, průměry, nejmenší/největší hodnota apod.). * Systém zachovává původní informaci ze zdroje logu o časové značce události, ale nedůvěřuje jí a vytváří vlastní důvěryhodné časové razítko ke každému logu, které vzniká v okamžiku přijetí logu systémem a kterým se systém defaultně řídí. * Všechna pole a položky přijaté systémem jsou automaticky indexovány. Nad všemi položkami je možné ihned provádět vyhledávání bez nutnosti dodatečného ručního indexování administrátorem. * Možnost sběru událostí minimálně ve formátech RAW, Syslog RFC5424, CEF, LEEF, JSON RFC8259. * Systém nesmí v žádném případě umožnit mazání nebo modifikování již uložených logů v rámci požadované retence. A to ani libovolnou konfigurační změnou - administrátorovi s nejvyššími oprávněními k navrhovanému systému. Každý zpracovaný log musí mít dohledatelný unikátní identifikátor, který umožní jeho jednoznačnou identifikaci. * Systém musí umožňovat konfiguraci filtrace nerelevantních událostí v grafickém rozhraní vizuálního programovacího jazyka. Pro psaní filtrace nesmí být použito textové psaní programového kódu ale tzv. vizuální programování, které automaticky opravuje uživatele a upozorňuje ho na chyby. Předložte odkaz na dokumentaci popisující způsob filtrování nerelevantních událostí. * Systém provádí konsolidaci logů na interním storage logovacího systému. * Systém umožňuje snadné vyhledávání událostí a okamžité vytváření grafických reportů (ad hoc) bez nutnosti dodatečného programování nebo aplikování dotazů v SQL jazyce. Reportovací nástroj musí být integrální součástí navrhovaného systému a musí se obsluhovat v jednotném rozhraní nabízeného produktu. Předložte link nebo pdf popisující způsob vytváření reportů. * Systém provádí ucelenou vizualizaci logů, událostí a strojových dat (grafy událostí). Vizualizace musí být dynamická, tj. volbou v jednom grafu se ostatní příslušné grafy v pohledu na data upraví dle požadované volby automaticky. * Systém umožňuje snadno vytvářet grafické znázornění událostí v dashboardech nad všemi uloženými daty za libovolné časové období bez nutnosti nejprve modifikovat konfiguraci systému nebo parametrů uložených dat. Historická data v požadované délce retence uložená v systému je možné prohledávat okamžitě bez časových prodlev opětovného importu nebo dekomprimace starších dat, prohledávání dat nesmí vyžadovat manuální konfiguraci a zásahy uživatele. * Systém umožňuje snadno vytvářet grafické znázornění událostí v dashboardech nad všemi uloženými daty za libovolné časové období bez nutnosti nejprve modifikovat konfiguraci systému nebo parametrů uložených dat. Historická data v požadované délce retence uložená v systému je možné prohledávat okamžitě bez časových prodlev opětovného importu nebo dekomprimace starších dat, prohledávání dat nesmí vyžadovat manuální konfiguraci a zásahy uživatele. * Systém podporuje nativní získávání logů z Office365/Microsoft365 prostředí bez ohledu na použitou licenci 365 prostředí a bez nutnosti instalovat dodatečné externí komponenty. * V případě krátkodobého (do 10 minut) až dvounásobného přetížení systému proti jeho tabulkovým hodnotám nesmí dojít ke ztrátě logů nebo nesprávnému stanovení časového razítka. Všechny přijaté nezpracované logy/události musí být ukládány do vyrovnávací paměti. * Systém musí umožňovat unifikované vyhledávání napříč všemi typy dat a zařízeními dle normalizovaných polí (uživatelské jméno, zdrojová IP, značka/tag apod.). * Dodavatel musí předložit potvrzení vystavené autorizovanou osobou o shodě, že nabízený systém splňuje požadavky normy ČSN/ISO 27001:2013 na pořizování auditních záznamů. Toto potvrzení není možné nahradit certifikátem na společnost dodavatele (subdodavatele) nebo výrobce nabízeného systému. Nelze nahradit ani čestným prohlášením. * Systém musí mít možnost uložení uživatelem vytvořených pohledů na data (dashboardů) pro budoucí zpracování. Továrně dodané pohledy na data nesmí jít administrátorem ani uživatelem systému nevratně modifikovat nebo smazat. * Systém obsahuje reportovací nástroj s přednastavenými nejběžnějšími reporty a možností vlastních úprav a vytvoření nových pohledů. Pro vytváření nových pohledů na data není přípustné používat povinně SQL jazyk. * Systém obsahuje předpřipravené pohledy na uložená data dle jednotlivých kategorií zdrojových zařízení i dle logického členění. * Na základě pohledu na uložená data lze provést export dat ve strukturovaném formátu tak, jak jsou v továrně nastaveném nebo uživatelsky nastaveném pohledu data skutečně zobrazena. * Konfigurační a Systémové rozhraní a dokumentace k těmto rozhraním musí být identické v anglickém i v českém jazyce. Nepřipouští se omezená dokumentace v českém jazyce nebo zjednodušená dokumentace odkazující na další dokumentaci v anglickém jazyce, případně na dokumentaci třetích stran. * Systém nabízí kapacitní i výkonovou škálovatelnost. * Monitoring stavu systému - alertování při překročení prahových hodnot nebo chybě systému, přeposlání upozornění pomocí SMTP nebo Syslog. * Požadujeme, aby systém obsahoval REST-API pro integraci s externím monitorovacím systémem (Zabbix, Nagios, MRTG a další) a umožňoval autorizovaný přístup ke strukturované databázi logů. Součástí požadavku je vzorový návod na integraci s externím monitorovacím systémem. * Dodavatel doloží prohlášení výrobce o shodě s požadavky Vyhlášky 82 / 2018 Sb. „o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)“ k Zákonu 181 / 2014 Sb. „o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)“. * Jednotná centrální webová konzole s jednotným grafickým rozhraním pro přístup k logům, alertům, reportům a pro správu systému. Z této konzole se provádí veškerá konfigurace, správa i analýza logů. Není přípustné, aby navrhovaný systém měl více rozdílných konzolí od různých výrobců s rozdílným ovládáním nebo aby se konfigurace musela provádět mimo jednotné webové rozhraní včetně dokumentace, ze které je zřejmé, jakým způsobem je realizována konfigurace v rámci jednotné konzole. * Požadujeme, aby systém umožňoval jednotné vytváření uživatelských rolí definujících přístupová práva k uloženým událostem na základě typu zdrojů a značek a k jednotlivým ovládacím komponentům systému. * Dodaný systém musí obsahovat ucelené all-in-one řešení pro parsování a normalizaci přijatých událostí bez nutnosti dodatečné instalace externích aplikací nebo systémů. Jedinou přípustnou výjimkou je monitorování systémů Windows pomocí agentů. * Systém musí podporovat ověřování uživatele systému na externím LDAP serveru. V případě výpadku externího LDAP systému musí podporovat ověření lokálního účtu. Systém automaticky zaznamenává uživatelská jména u akcí provedených konkrétním uživatelem. |  |
| Výkonnostní a SW parametry systému | * Všechny části systémů je možné nastavit v centrální webové konzoli a není nutné editovat žádné konfigurační soubory, scripty nebo makra v příkazové řádce). * Aktualizace systému jsou distribuovány v jednotném balíku a jejich instalace je prováděna uživatelsky přes centrální webovou správcovskou konzoli. Všechny aktualizace musí být prováděny z webového prostředí bez potřeby asistence dodavatele/výrobce dodávaného systému. * Systém musí podporovat downgrade v jednom kroku, pro případ problémů s novou verzí systému po upgrade. Není přípustný downgrade pouze za součinnosti výrobce. Popis způsobu realizace downgrade bude součástí dokumentace. * Průměrný trvalý příjem min. 2000 událostí/s. Výkon musí být dosažen na požadované množství událostí s průměrnou délkou zpráv minimálně 700Byte trvale. Systém musí prokazatelně kompletně zpracovat přijaté události včetně vytváření očekávaných metadat (DNS-PTR, čísla a jména ASN, geolokace), zajišťovat normalizaci, zamezovat ztrátě přijatých událostí nebo posunutí důvěryhodného časového razítka oproti času skutečného příjmu každé události. * Špičkový příjem minimálně 4000 událostí/s po dobu nejméně 10 minut a průměrnou délkou minimálně 700byte. Systém musí prokazatelně kompletně zpracovat přijaté události, zamezovat ztrátě ukládaných dat nebo posunutí důvěryhodného časového razítka oproti času skutečného příjmu zpráv. Při zpracování dat během špičkového příjmu akceptujeme zpoždění zobrazení zpracovávaných dat. Systém ani ve špičkovém výkonu nesmí dovolit ztrátu dat, skluz důvěryhodného časového razítka nebo jiné prokazatelné vady na zpracovávaných datech oproti zpracování při průměrném trvalému příjmu událostí. * Licenčně neomezený počet zařízení pro příjem zasílaných událostí. Licenčně neomezený počet událostí v GB za den nebo licence na minimálně 200GB uložených událostí za den. * 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. * Konfigurace uživatelských parserů musí umožňovat automatické doplňování DNS reverzních záznamů, čísel a jmen autonomních sítí, geolokační informace a identifikace výrobce zařízení podle MAC adresy. * Systém musí podporovat doplňování zpráv o informace z textových prohledávacích tabulek. (Například k uživatelskému jménu doplnit z textové prohledávací tabulky informaci o jeho emailu, členství v AD skupinách a podobně). Pro automatickou aktualizaci takto uložených doplňujících informací musejí být tyto textové prohledávací tabulky naplnitelné pomocí REST API nabízeného systému a modifikovatelné přes jednotné webové rozhraní. Doložte odkazem na dokumentaci, jakým způsobem lze plnit textové tabulky prostřednictvím REST-API nabízeného systému. * Možnost on-line ladění uživatelsky definovaných parserů - při jejich vytváření je možné vložit skupinu testovacích zpráv, při změně je okamžitě zobrazena výsledná podoba rozparsovaných dat a případná chybová hlášení s upozorněním na chybná místa vytvářeného parseru. Pro snadnější vytváření parserů požadujeme mít možnost vložení minimálně 20 testovacích zpráv současně. Doložte odkazem na dokumentaci, ze které je zřejmé, jakým způsobem se vkládají testovací zprávy během psaní nového uživatelského parseru a jakým způsobem je prezentován výstup testu. * V centrální správcovské konzoli je možné přidávat k jednotlivým zdrojům dat, aplikacím, zařízením nebo IP subnetům tzv. značky, označující například umístění zařízení, typ zařízení, kritičnost zařízení apod. Systém obsahuje předdefinované značky, které automaticky přidává k přijímaným zprávám. Příklady značek: konfigurační změna, úspešné ověření uživatele, neúspěšné ověření uživatele, zpráva přišla z windows, zpráva byla vygenerována firewallem atd. * Všechny přidávané značky jsou ukládány s každou přijatou událostí, na základě značky je možné filtrovat data nebo omezovat oprávnění uživatelů systému k jednotlivým událostem. * Pro budoucí nasazení ve vysoké dostupnosti a výkonnostní rozšíření je vyžadována podpora sestavení ve vysoké dostupnosti – požadujeme podporu minimálně 4 nodů v clusteru. Nastavení clusteru se musí kompletně realizovat v grafickém rozhraní správcovské konzole v jednom kroku, není přípustné konfigurovat sestavení scripty, makry nebo úpravou textové konfigurace systému a pomocí ručních restartů služeb. Systém ve vysoké dostupnosti musí přehledně informovat o stavu clusteru a procesu synchronizace databází. Dokumentace k realizaci vysoké dostupnosti musí být kompletní a popisovat všechny kroky sestavování a obnovení v případě výpadku komponenty clusteru. Doložte odkazem na dokumentaci, jakým způsobem se cluster vytváří a jakým způsobem se provádí obnovení po možném výpadku jednotlivých zúčastněných komponent. * Vícenodový cluster se chová i ovládá jako jednotný systém, nutnost nezávislé konfigurace na každé jednotce v clusteru je vyloučena. Vícenodový cluster umožnuje geolokační oddělení a pro komunikaci v rámci clusteru musí využívat definovaný TCP/UDP port pro snadné nastavení prostupy firewallu. Veškerá komunikace v rámci clusteru musí být šifrovaná s vysokým kryptografickým standardem pro bezpečné vytvoření privátní virtuální sítě na síťové vrstvě. Popište použitou technologii zabezpečení komunikace v rámci clusteru. * V případě využití více nodů v clusteru se automaticky zrychluje zpracování vstupních dat a vyhledávání v již uložených datech. * V případě rozšíření systému na cluster musí navrhovaný systém zajistit bezvýpadkovost sběru logů. * Systém musí umožňovat export dat ve formátu vhodném pro další strojové zpracování bez dodatečných omezení na časové období, množství nebo obsah exportovaných dat. Během exportu je možné označit pouze vybraná pole, která mají být do exportu zahrnuta. * Podpora zálohování nebo obnovení konfigurace v jednom kroku a jednom souboru pro celý systém. Doložte odkazem na dokumentaci, jakým způsobem se provádí zálohování a obnova konfigurace systému. * Podpora důvěryhodného zálohování dat na externí systém. Požadováno plánované i ad-hoc zálohování. Zálohy dat musejí být vhodně kompresovány a umožnit v budoucnosti obnovení bez ohledu na verzi systému, ve které byla záloha pořízena. Doložte odkazem na dokumentaci, jakým způsobem se realizuje zálohování a obnova záloh. |  |
| Alerty | * Systém je schopen na základě uživatelsky zadaných podmínek splněných v přijatých datech vygenerovat alert. * Text emailu vygenerovaného alertem musí být uživatelsky definovatelný s proměnnými, které jsou vyplněny z přijaté rozparsované události. * Systém musí obsahovat výrobcem předpřipravené sety/vzory alertů a korelací. * Systém musí provádět konfigurace alertů a korelací pomocí vizuálního programovacího jazyka. Vizuální programovací jazyk není prezentován čistě textově, ale textově-grafickou formou, která vizualizuje aplikační logiku vytvářeného alertu. Konfigurace alertů musí umožňovat okamžitou kontrolu funkčnosti výstupu alertu nebo korelace vložením příslušné testovací zprávy, včetně zobrazení upozornění na případné uživatelské chyby. Doložte odkazem na dokumentaci, jakým způsobem realizujete konfiguraci a testovaní alertů a korelací. * Jako výstupní pravidlo Alertu musí systém umět odeslat událost, která alert vyvolala, na externí systém minimálně prostřednictvím SMTP nebo Syslogu přes TCP protokol. U Syslog protokolu požadujeme možnost definice formátu odesílaných dat pro snazší integraci se systémy třetích stran. Doložte odkazem na dokumentaci, jakým způsobem se zpráva, která vyvolala spuštění alertu, odesílá na externí systém a jak se definuje formát odesílání dat. * V alertech je možné nejen využívat, ale i přiřazovat značky (příklad: pošli alert jen v případě, že se událost stala na kritickém serveru a je označen názvem lokality, nebo pokud událost obsahuje podmínku, přiřaď novou značku). Doložte odkazem na dokumentaci, jakým způsobem lze v jednotném grafickém rozhraní systému definovat a přiřazovat značky. * Systém podporuje základní funkce SIEM - funkce pro korelace událostí a upozornění s hraničními limity. Definice korelačních pravidel je prováděna pomocí vizuálního programovacího jazyka a musí obsahovat možnost vložení testovací zprávy a zobrazení výsledku testu o provedené akci. |  |
| Sběr událostí z Microsoft prostředí | * Události z Microsoft prostředí jsou vyčítány pomocí agenta instalovaného přímo v koncových systémech. Windows agent musí současně podporovat jak monitoring interních windows logů, tak monitoring textových souborových logů. Agent se nesmí instalovat individuálně, ale prostřednictvím MS AD Group Policy a nesmí vyžadovat žádnou konfiguraci na cílovém systému. Doložte odkaz na dokumentaci popisující požadované vlastnosti integrovaného Windows agenta. * Agent provádí instalaci a podporuje centralizovanou konfiguraci Microsoft Sysmon pro obohacení logů, včetně globálního a selektivního zapínaní/vypínaní služby Sysmon a výběr z několika přednastavených konfigurací Sysmon v grafickém rozhraní centrální správcovské konzole systému. Doložte odkazem na dokumentaci, jakým způsobem se provádí centralizované řízení a konfigurace Microsoft Sysmon služby. * Agent sběru z Microsoft podporuje globální i lokální nastavení filtrace odesílaných událostí pomocí centrální správcovské konzole. Například, zašli pouze logy z adresářů eventview Systém, Security, Sysmon a Terminal Services a zahoď logy s EventId 7036. * Filtrace odesílaných událostí agenty se konfiguruje pomocí vizuálního programovacího jazyka z centrální správcovské konzole systému. Logy nastavené k filtraci jsou filtrovány na straně windows agenta a nejsou nijak odesílány po síti. Vizuální programovací jazyk není prezentován textově, ale textově-grafickou formou, která vizualizuje aplikační logiku vytvářeného alertu. Doložte odkazem na dokumentaci, jakým způsobem se vytváří a přiřazují filtry pro Windows agenty pro sběr logů a jakým způsobem se testuje účinnost filtru. * Windows agent nevyžaduje administrátorské zásahy na koncovém systému – je centrálně spravovaný a jeho konfigurace musí být kompletně realizována v grafickém rozhraní systému bez využití skriptů nebo maker. Konfigurace musí být automaticky distribuována přímo z centrální konzole systému. Tj. vlastní správa a aktualizace Windows agenta se neprovádí z Group Policy. * Komunikace Windows agenta a centrálního systému musí být zabezpečena TLS 1.2 a výše a musí podporovat ověřování certifikátem. * Windows agent podporuje sběr nejen ze základních systémových logů (Aplikace, Zabezpečení, Instalace, Systém), ale je možné z centrální konzole v grafickém rozhraní nastavit i sběr všech ostatních logů ve složce Protokoly aplikací a služeb a logy rozšířené Sysmonem. Dále musí Windows agent podporovat centralizované nastavení z administrátorské konzole systému pro sběr textových logů včetně možnosti výběru jejich formátu. Doložte odkazem na dokumentaci, jakým způsobem se nastavují parametry sběru logů globálně a jakým způsobem u konkrétního agenta. * Windows agent automaticky doplňuje ke všem odesílaným událostem jejich textový popis tak, jak je zobrazen v Prohlížeči událostí (Event Viewer) na koncovém systému. K bezpečnostním událostem hodným pozornosti doplňuje značku a popis dle MITRE ATT&CK® matrice a k takto detekovaným procesům a souborům automaticky vytváří SHA256 hash. * Počet instalací Windows agenta není licenčně a časově omezen minimálně na dobu 5 let a pokrývá všechny klientské stanice úřadu, jejichž předpokládaný počet je 300. |  |
| Vysoká dostupnost, SW Podpora a záruka na hardware | * Požadujeme volitelnou podporu pro nasazení ve vysoké dostupnosti. * Systém musí podporovat vygenerování TSR (technického support reportu) pro možnost diagnostiky bez vzdáleného přístupu. |  |
| Dokumentace | * Dokumentace k vytváření parserů a testování jejich funkčnosti. 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. * Detailní komunikační matrice s popisem všech použitých protokolů a portů pro nabízený systém a dokumentaci k nastavení sběru z databází v grafickém rozhraní systému. * Odkaz na dokumentaci popisující nastavení systému v jednotném grafickém rozhraní tak, aby získával logy z Office365/Mircosoft365. * Popis vytváření uživatelských rolí v grafickém rozhraní systému. |  |
| Certifikace | * Pokud je dodavatel různý od výrobce, předloží certifikaci nebo jiné potvrzení o autorizovaném partnerství pro nabízený systém. |  |
| Implementace | * Nastavení systému a jeho konfigurace tak, aby mohl pracovat v prostředí zadavatele, včetně dodávky nezbytné kabeláže. * Konfigurace stávajících systémů a zařízení zadavatele tak, aby posílaly logy do dodávaného systému. * Instalace Windows agenta na systémy požadované zadavatelem a jeho konfigurace. * Konfigurace systému pro komunikaci s nainstalovanými Windows agenty. * Vytvoření a uložení vlastního dashboardu a reportu, nastavení pravidelného odesílání reportu mailem vybraným zaměstnancům zadavatele – jeden vzorový dashboard. * Vytvoření vzorového alertu specifikovaného zadavatelem. |  |
| Servisní podpora | * SW - Podpora výrobce na aktualizaci systému a parserů na 5 let. Podpora musí obsahovat aktualizaci SW minimálně 3x ročně, opravy chyb a telefonickou a emailovou podporu s diagnostikou vzdáleným přístupem. |  |

## Požadavky na záruky

Zadavatel požaduje záruku na veškeré dodané technologie v délce trvání minimálně **24 měsíců** od okamžiku předání díla, není-li u konkrétního zařízení či komponenty požadováno jinak v specifikaci ZD

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.

## Požadavky na technickou podporu

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

* **Technická podpora:** 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.
* **Nové verze a aktualizace:** Úpravy a změny softwaru, aby zůstal kompatibilní s měnícím se prostředím. To může zahrnovat aktualizace pro nové operační systémy, hardware nebo jiné softwarové závislosti. Soulad SW s platnou legislativou.
* **Optimalizace provozu:** 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.

**Garantovaná doba reakce Poskytovatele od nahlášení požadavku na poskytnutí technické podpory**

1. Služba je poskytována Pracovníky Poskytovatele v okamžiku, kdy dojde k zadání Požadavku.
2. Obsahem této služby je reakce Poskytovatele na Požadavky dle jejich priority a zahájení řešení v rámci **Servisního kalendáře, tj. pracovní dny od 7:00 do 17:00**.
   1. Je-li požadavek nahlášen mimo pracovní dobu, je počátkem uvedené doby 7:00 hodin nejbližšího pracovního dne.
   2. Dodavatel je povinen zahájit řešení požadavku bezodkladně, nejpozději však do níže uvedených časů, viz tabulka Klasifikace požadavku a stavů.
3. Požadavek na provedení této služby zadávají Kontaktní osoby Objednatele nebo Poskytovatele zadáním Požadavku na Helpdesk Poskytovatele.
4. Zahájení řešení je primárně poskytováno Vzdáleným připojením pracovníka Poskytovatele. Pokud to technická povaha řešení Požadavku vyžaduje, bude realizován fyzický zásah pracovníka Poskytovatele v místě technologických center města Kroměříže, přesné místo bude vždy specifikováno v zadaném požadavku.

**Klasifikace požadavku a stavů**

|  |  |  |  |
| --- | --- | --- | --- |
| **Klasifikace** | **Definice** | **SLA zahájení řešení** | **Předpokládané vyřešení požadavku** |
| 1. Nahlášení požadavku | Potvrzení přijetí nahlášeného požadavku jedním z výše uvedených způsobů hlášení požadavku. | Nejpozději do 15 minut | Není specifikováno |
| 1. Kritický požadavek (A) | Události, které znemožňují přístup ke službám a datům poskytovaných Prvky IT, nebo jejich využívání, vážně ovlivňují plnění termínů nebo ziskovost, případně mají vliv na většinu uživatelů a služeb. | Nejpozději do 6 hodiny od nahlášení požadavku v rámci Servisního kalendáře | Do 12 hodin od zahájení řešení, dle servisního kalendáře |
| 1. Závažný požadavek (B) | Události, které významným způsobem degradují, nebo silně omezují funkcionalitu nebo službu Prvku IT, ale existuje náhradní řešení (činnost pokračuje v omezeném provozu). | Nejpozději do 10 hodin od nahlášení požadavku v rámci Servisního kalendáře | Do 24 hodin od zahájení řešení, dle servisního kalendáře |
| 1. Ostatní požadavky (C) | Všechny ostatní požadavky, neomezující řádné používání Informačního systému, které tvoří Prvky IT. | Nejpozději do 14 hodin od nahlášení požadavku v rámci Servisního kalendáře | Do 32 hodin od zahájení řešení, dle servisního kalendáře |
| 1. Změnové požadavky | Součinnost při implementaci změn a činnostech při nasazovaní nových prvků IT či jejich částí. | Nejpozději do 7 pracovních dní | Stanoveno dohodou |
| 1. Konzultace a návrh řešení, programátorské práce | Konzultace při řešení problémů nebo při úpravách prvků IT. | Nejpozději do 5 pracovních dní | Stanoveno dohodou |

Pro případ, že bude zadavatel požadovat služby rozšířené technické podpory podle písmena e) a f), budou tyto služby vyúčtovány po skončení kalendářního měsíce, ve kterém byly čerpány, v hodinové sazbě uvedené v Kalkulaci ceny, dle skutečně realizovaných hodin rozšířené servisní podpory. Předpokládaný rozsah služeb rozšířené technické podpory pro účely přípravy nabídky je 100 hodin / na 5 let.

**Ceny za služby technické podpory**

|  |  |  |
| --- | --- | --- |
| **Typ požadavku** | **Cena bez DPH** | **Měrná jednotka** |
| Servisní požadavek "A" |  | Člověkohodina |
| Servisní požadavek "B" |  | Člověkohodina |
| Servisní požadavek "C" |  | Člověkohodina |
| Změnový požadavek |  | Člověkohodina |
| Konzultace a návrh řešení, programátorské práce |  | Člověkohodina |
| Dopravné mimo město |  | Km |

.

# Společné požadavky pro části 1 – 5

|  |
| --- |
| **Požadavek** |
| Dodavatel bere na vědomí, že součástí akceptace plnění jsou výsledky auditu, který bude prověřovat, zda jím implementovaná bezpečnostní opatření jsou funkční. Dodavatel pak poskytne součinnost nebo napraví nalezené chyby vysoké závažnosti v implementaci technických opatření. |
| Součástí je zajištění instalace a konfigurace veškerých komponent v návaznosti na stávající infrastrukturu úřadu (tj. včetně dopravy, montáže, instalace a implementace do stávající IT infrastruktury) v sídle zadavatele. |
| Součástí instalace musí být i zaškolení IT administrátorů minimálně v rozsahu nutném pro samostatnou administraci všech komponent zakázky. Administrací se rozumí zejména: konfigurace, monitoring činnosti, aktualizace, řešení problémů, zálohování konfigurace. |
| Zákaznická dokumentace bude zahrnovat:   * popis všech prvků/zařízení, * popis způsobu zálohy a obnovy konfigurace všech prvků/zařízení * veškeré požadavky na zachování záruky/podpory (např. environmentální, kompatibilita, …) * informaci o způsobu řešení servisních požadavků |
| Dodavatel do své nabídky zahrne veškerý instalační materiál a kabeláž nutnou k plnohodnotnému zprovoznění dodané technologie jako logického a funkčního celku. |
| Dodavatel zajistí instalaci a konfiguraci dodaných HW a SW komponent v návaznosti na stávající infrastrukturu organizace, a to včetně instalace a implementace do stávající IT infrastruktury v sídle zadavatele:   * instalace zařízení do standardní RACK skříně 19“ * implementace Best Practice scénářů pro dané konfigurace * kontroly kompatibility verzí ovladačů a firmware jednotlivých zařízení a jejich aktualizace * registrace záruk u výrobců * umístění do racku a zapojení kabeláže vč. jejího označení, * inicializace a konfigurace všech dodaných zařízení * nastavení IP adres * nastavení vysoké dostupnosti * konfiguraci datových prostor polí, integrace s hypervizorem, nastavení dohledu a instalace SW pro monitoring výkonu * zapojení do stávající SAN |
| Dodavatelé za všechny části si budou poskytovat vzájemnou součinnost při zprovoznění nebo implementaci všech částí zakázky v nezbytném rozsahu. Předpokládaná součinnost pro každého dodavatele v každé části je 1 člověkoden celkem pro všechny části. |

# Provozní podpora

|  |
| --- |
| **Požadavek** |
| Podpora a servis pro dodaný HW a SW budou poskytovány minimálně po celou dobu udržitelnosti projektu (tj. 60 měsíců od předání díla), pokud není specifikováno jinak. |
| Bude zajištěna udržitelnost HW a SW včetně třetích stran, dodaných v rámci veřejné zakázky. |
| Technická podpora a servis zařízení HW a SW budou realizovány dodavatelem, případně prostřednictvím odpovídajícího servisního kanálu výrobce. |
| Technická podpora a servis budou realizovány v místě zadavatele. Výjimku tvoří činnosti realizovatelné vzdáleným připojením. |
| Technická podpora bude zajišťována těmito způsoby:   * Telefonicky prostřednictvím přiděleného tel. kontaktu. * Prostřednictvím elektronické oznamovací služby (tzv. helpdesku). * Prostřednictvím vzdáleného připojení na PC uživatele / server. |
| Telefonická, e-mailová podpora a podpora prostřednictvím vzdáleného připojení bude k dispozici minimálně v pracovních dnech od 7 do 17 hod. |
| Služba HelpDesk umožní příjem požadavku na servisní zásah v českém jazyce prostřednictvím webového rozhraní v režimu 7x24 hod (s výjimkou předem nahlášených servisních zásahů při správě systému HelpDesk). |