# **Technická špecifikácia**

# **Opis predmetu zákazky**

Predmetom zákazky je **„****Dodanie, implementácia a služby podpory prevádzky a údržby komplexného nástroja pre Kybernetickú bezpečnosť**“ ktorého cieľom je naplnenie požiadaviek legislatívy na riešenie kybernetických bezpečnostných incidentov a opatrení pre oblasť monitorovania, testovania bezpečnosti a bezpečnostných auditov /ďalej ako komplexný nástroj/, a to najmä:

- zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov,

- vyhlášky NBÚ č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení.

Poskytovateľ poskytne:

1. **Dodanie a implementáciu komplexného nástroja pre Kybernetickú bezpečnosť s požadovanými funkciami**

**B**. **Služby podpory prevádzky a údržby dodaného komplexného nástroja pre Kybernetickú bezpečnosť** pre zaistenie spoľahlivej, kontinuálnej a bezpečnej prevádzky v súlade s dokumentáciou systému a aktuálnymi požiadavkami Objednávateľa, vrátane riešenia Problémov podľa stanovených SLA parametrov

1. **Kapacitné požiadavky na komplexný systém**

Definovanie vstupných zdrojov verejného obstarávateľa

|  |  |  |  |
| --- | --- | --- | --- |
| Počet lokalít | Počet kolektorov | Počet NTA zariadení | Počet orchestrátorov zariadení |
| 5 | 2 | 5 | 2 |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Lokalita | Počet AD užívateľov | Počet AD administrátorov | Počet AD servisných účtov | Počet serverov (virtualizačné + virtuálne) a počet fyzických serverov | Počet sieťových zariadení | Počet pracovných staníc | Počet iných zariadení pripojených do siete (tlačiarne, skenery, dochádzkový terminál a pod.) |
| OL | 900 | 3 | 40 | 60 | 60 | 230 | 50 |
| TR |  |  |  | 4 | 75 | 160 | 60 |
| PE |  |  |  | 2 | 20 | 50 | 15 |
| HR |  |  |  | 2 | 15 | 30 | 15 |
| KR |  |  |  | 2 | 30 | 60 | 30 |

Dodávaný komplexný nástroj musí podporovať zber logov z nasledujúcich typov zariadení a systémov verejného obstarávateľa:

MS Windows Server 2012 R2 a neskoršie vrátane všetkých jeho rolí

MS Exchange Server 2016 a neskoršie

Linux server

Sieťové smerovače, prepínače a firewally (Cisco, Fortinet, Microtik, Palo Alto)

NetApp úložiská radu FAS a AFF

Synology úložiská

Eset Antivirus

Microsoft 365

1. **Špecifikácia požadovaných služieb** 
   1. **Dodanie a implementáciu komplexného nástroja pre Kybernetickú bezpečnosť s požadovanými funkciami, ktorými sú**

* SIEM (Security Information & Event management)
* UBA (User Behavior Analytics)
* ABA (Attacker Behavior Analytics)
* EDR (Endpoint Detection & Response) & FIM (File Integrity Monitoring)
* NTA (Network Traffic Analysis)
* DT (Deception Technology)
* SOAR (Security orchestration and Automation)

Pre realizáciu činností

• zaznamenávanie činnosti sietí a informačných systémov a ich používateľov

• podporu riešenia kybernetických bezpečnostných incidentov

• tvorbu, odhaľovanie a upozorňovanie na nastavené pasce na útočníka

• izoláciu koncových bodov v prípade bezpečnostného incidentu

• automatizáciu odozvy na kybernetické incidenty prostredníctvom workflow

• reporting kybernetických bezpečnostných udalostí a incidentov

spolu so softvérovými licenciami pre Komplexný nástroj alebo predplatenými službami na poskytovanie Komplexného nástroja na obdobie **12 mesiaco**

* + 1. Funkčné požiadavky na SIEM

|  |  |
| --- | --- |
| **Č.** | **Požiadavka** |
| SIEM-1 | SIEM musí umožňovať zber aplikačných, databázových aj systémových logov zo sieťových aj bezpečnostných zariadení (napr. firewally, sieťové alebo host. IPS/IDS), pracovných staníc, serverov ako aj cloud prostredí (Microsoft Azure, Microsoft 365,..)  Bližšia špecifikácia v opise |
| SIEM-2 | SIEM musí zbierať, detegovať a vyhodnocovať udalosti ako sú pokusy o neautorizované prístupy, zmeny integrity vybraných častí operačného systému, útoky škodlivého kódu, botov, neoprávnený prístup k aplikáciám, neautorizovanú zmenu konfigurácií, detegovať chybové stavy siete, porušení bezp. politík (Zákazníka) |
| SIEM-3 | SIEM musí umožňovať monitoring, vyhodnocovanie a korelovanie udalostí a následné generovanie alertov a to všetko v reálnom čase, pričom nesmie technicky limitovať počet spracovávaných a ukladaných udalostí (napríklad pri prekročení licencie alebo výkonu riešenia). |
| SIEM-4 | SIEM musí umožňovať uchovávanie pôvodnej informácie zo zdroja logu o časovej značke udalosti |
| SIEM-5 | SIEM nesmie umožniť odstránenie alebo modifikovanie uložených logov administrátorovi systému |
| SIEM-6 | SIEM musí pre každý log mať unikátny identifikátor, pre jednoznačnú identifikáciu |
| SIEM-7 | SIEM podporuje jednoduché vyhľadávanie udalostí a okamžité vytváranie reportov bez nutnosti dodatočného programovania |
| SIEM-8 | SIEM musí podporovať pokročilé korelácie (časové, z viacerých zdrojov, atď.) |
| SIEM-9 | SIEM musí podporovať integráciu s Vulnerability Assessment pre kontextualizáciu aká zraniteľnosť na konkrétnom koncovom bode existuje. |
| SIEM-10 | SIEM bude podporovať úpravy alertingu, parsingu bez nevyhnutnosti učiť sa akýkoľvek programovací/skriptovací jazyk (v súlade s požiadavkou na vykonanie týchto zmien vlastnými silami objednávateľa) |
| SIEM-11 | SIEM bude podporovať detekciu sieťových incidentov na základe korelácie informácií z poskytnutých logov a bude podporovať behaviorálnu analýzu spracovaných udalostí. |
| SIEM-12 | SIEM bude obsahovať Incident Management konzolu pre správu kybernetických bezpečnostných udalostí a incidentov. V rámci konzoly je k dispozícií časový sled udalostí daného incidentu, možnosť prideľovať riešiteľov, možnosť vyvolať akcie (pre zisťovanie ďalších informácií, dopĺňanie logov, vrátane podrobných informácií z koncového bodu resp. súvisiacich aktív a pod.) |
| SIEM-13 | Riešenie je možné prevádzkovať vo forme on premise alebo cloud |
| SIEM-14 | SIEM bude bez požiadaviek na externý databázový server |
| SIEM-15 | SIEM bude podporovať možnosť súčasnej práce minimálne 10 analytikov |
| SIEM-16 | SIEM bude podporovať možnosť tvorby vlastných Dashboardov a Vizuálnych Analýz |
| SIEM-17 | Všetky úkony užívateľa (aj interného) v SIEMe budú auditované |
| SIEM-18 | SIEM bude podporovať pokročilý reporting s možnosťou schedulingu a distribúcie reportu. |
| SIEM-19 | SIEM podporuje zber dát so šifrovaným prenosom (TLS, prípadne šifrovaný obsah správ) na celej trase zdroj /kolektor/ centrálna konzola |
| SIEM-20 | SIEM Riešenie podporuje outbound API. Príkladom môže byť pripojenie sa na externé zariadenia alebo systémy (napr. Azure, AWS, Microsoft 365, ticketing system) |
| SIEM-21 | SIEM Riešenie podporuje inbound API. Príkladom môže byť pripojenie sa na riešenie SIEM pre vykonanie reportovacích, konfiguračných alebo iných administratívnych úloh. |
| SIEM-22 | SIEM Riešenie podporuje minimálne nasledujúce úrovne užívateľských oprávnení (administrátor, read/write, read/only) |
| SIEM-23 | SIEM musí podporovať integráciu s Active Directory. |
| SIEM-24 | SIEM podporuje vlastnú alebo externú integráciu na Multifaktorovú autentifikáciu. |
| SIEM-25 | SIEM podporuje integráciu na Microsoft Azure a Microsoft 365 pre účely monitoringu aktivít užívateľov. |
| SIEM-26 | SIEM podporuje spracovanie štruktúrovaných aj neštruktúrovaných dát. |
| SIEM-27 | SIEM podporuje vkladanie a monitorovanie vlastných IoC (indikátorov kompromitácie) vrátane manipulácie cez inbound API. |
| SIEM-28 | SIEM umožňuje realizáciu tzv. kaskádových dotazov (kaskádové dotazy sú dotazy generované na základe údajoch vrátených z predchádzajúceho dotazu, príkladom by mohlo byť zobrazenie aktív, na ktoré sa vzťahuje alert, s následnou možnosťou rozbalenia na používateľov, ktorých sa táto stránka s výsledkami vyhľadávania týka), |
| SIEM-29 | Zber udalostí v prostredí Microsoft:  - Udalosti z Microsoft prostredí sú získavané pomocou agenta inštalovaného priamo na koncovom Windows systéme. Windows agent musí súčasne podporovať ako monitoring interných windows logov, tak i monitoring textových súborových logov.  - Agent zaisťuje zber nemodifikovaných udalostí a detailné spracovávanie auditných informácií.  - Agent zabezpečuje v prípade potreby funkcionalitu kontroly integrity súborov  - Agent zabezpečuje v prípade potreby funkcionalitu auditovania prístupov k súborom na zariadení.  - Agent podporuje nastavenie filtrácie odosielaných udalostí pomocou centrálnej správcovskej konzoly.  - Filtrácia odosielaných udalostí agentom. Nerelevantné logy sú filtrované na strane windows agenta a nie sú odosielané po sieti.  - Windows agent nevyžaduje administrátorské zásahy na koncovom systéme – je centrálne spravovaný a automaticky aktualizovaný priamo z centrálnej správcovskej konzoly systému.  - Windows agent má buffer pre prípad straty spojenia medzi koncovým systémom a centrálnym úložiskom logov. |
| SIEM-30 | Zber udalostí v prostredí Linux / MacOs:  - Udalosti z Linux / MacOs prostredí sú získavané pomocou agenta inštalovaného priamo na koncovom Linux / MacOs systéme. Linux / MacOs agent musí súčasne podporovať ako monitoring interných logov, tak i monitoring textových súborových logov.  - Agent zaisťuje zber nemodifikovaných udalostí a detailné spracovávanie auditných informácií.  - Agent podporuje nastavenie filtrácie odosielaných udalostí pomocou centrálnej správcovskej konzoly.  - Filtrácia odosielaných udalostí agentom. Nerelevantné logy sú filtrované na strane Linux / MacOs agenta a nie sú odosielané po sieti.  - Linux / MacOs nevyžaduje administrátorské zásahy na koncovom systéme – je centrálne spravovaný a automaticky aktualizovaný priamo z centrálnej správcovskej konzoly systému.  - Linux / MacOs agent má buffer pre prípad straty spojenia medzi koncovým systémom a centrálnym úložiskom logov. |
| SIEM-31 | SIEM umožňuje generovať alert na základe   * Zhoda s vyhľadávaním reťazcom * Definovanej nečinnosti * Definovanej zmeny |
| SIEM-32 | SIEM umožňuje nastavenie sieťových zón a sieťových politík podľa ktorých budú generované alerty |
| SIEM-33 | SIEM umožňuje nastavenie privilegovaných skupín užívateľov Active Directory podľa ktorých budú generované alerty |

**2.1.2 Funkčné požiadavky na systém UBA**

|  |  |
| --- | --- |
| **Č.** | **Požiadavka** |
| UBA-1 | UBA podporuje minimálne nasledujúce korelačné pravidlá pre analýzu správania sa užívateľa:  Vytvorenie/Zablokovanie/ Resetovanie / Povolenie / Únik účtu |
| UBA-2 | UBA podporuje minimálne nasledujúce korelačné pravidlá pre analýzu správania sa užívateľa:  Eskalácia privilégií  Prijatie podozrivého odkazu v emailovej správe  Prístup na podozrivý odkaz cez web  Brute Force útok na heslá – lokálny účet  Brute Force útok na heslá – doménový účet  Autentifikácia užívateľa z podozrivej databázy  Manipulácia s lokálnymi udalosťami (event logs)  Prvé prihlásenie na aktívum  Prvé prihlásenie z inej krajiny  Prihlásenie z viacerých krajín súčasne  Detegovaný hash z podozrivej databázy  Spustenie procesu z podozrivej databázy  Impersonizácia administrátora  Autentifikácia servisným účtom  Autentifikácia doménovým účtom  Komunikácia s podozrivou IP  Spustenie vzdialeného súboru  Protokol poisoning  Alert s Microsoft Defender ATP  Spearphishing URL detegovaná |
| UBA-3 | UBA podporuje úpravu špecifických korelačných pravidiel (vytvorenie investigatívy, vytvorenie informácie, ..) |
| UBA-4 | UBA vytvára rizikový profil užívateľa na základe jeho správania |
| UBA-5 | UBA vytvára rizikový profil privilegovaného užívateľa na základe jeho správania |
| UBA-6 | UBA podporuje podrobný monitoring definovaných užívateľov |
| UBA-7 | UBA podporuje podrobný monitoring aktivít privilegovaného užívateľov v lokálnom aj cloud prostredí |

**2.1.3 Funkčné požiadavky na systém ABA**

|  |  |
| --- | --- |
| **Č.** | **Požiadavka** |
| ABA-1 | ABA podporuje korelačné pravidlá pre analýzu správania sa útočníka:  Ako príklad (Zistenie externej IP pomocou príkazového riadku, Spustenie klúča z registra Windows , Spúšťanie procesov pomocou MMC konzole, Rundl32.exe spúšťa súbor s adresára Program Data, Premenovanie netcat, Windows debug v príkazovom riadku a dalšie |
| ABA-2 | ABA má integrovaných viac ako 1500 takýchto korelačných pravidiel správania sa útočníka |
| ABA-3 | ABA umožňuje mapovať správanie sa útočníka podľa taktík z metodiky MITRE ATT&CK  Reconnaissance  Resource Development  Initial Access  Execution  Persistence  Privilege Escalation  Defense Evasion  Credential Access  Discovery  Lateral Movement  Collection  Command And Control  Exfiltration  Impact |
| ABA-4 | ABA podporuje úpravu korelačných pravidiel prostredníctvom výnimiek |
| ABA-5 | Databáza korelačných pravidiel správania sa útočníka je kontinuálne aktualizovaná o nové techniky používane útočníkmi. |

**2.1.4 Funkčné požiadavky na systém EDR**

|  |  |
| --- | --- |
| **Č.** | **Požiadavka** |
| EDR-1 | EDR podporuje základnú funkcionalitu odozvy na incident (zrušenie bežiaceho procesu, karanténa aktíva) prostredníctvom Windows/Linux agenta priamo z centrálnej konzole |
| EDR-2 | EDR podporuje funkcionalitu vyšetrovania incidentu prostredníctvom zberu dôkazov minimálne v rozsahu:  Arp Cache  Current Process  Directory Entry  Dns Cache  Installed Service  Network Connection  Prefetch Entry  Registry Key  Scheduled Task  User Session |
| EDR-3 | EDR podporuje funkcionalitu vyšetrovania incidentu prostredníctvom zberu dôkazov preverovaného uživateľa o nasledujúce udalosti:  Account modified  Advanced malware alert  Asset authentication  Cloud service account modified  DNS query  Firewall  IDS  Ingress authentication  Virus infection  Web proxy |
| EDR-4 | EDR podporuje rozšírenú funkcionalitu odozvy na incident (spustenie automatizačného workflow,..) |
| EDR-5 | EDR podporuje funkcionalitu auditovania integrity súborov pre nasledujúce typy súborov Windows:  .bat  .cfg  .conf  .config  .dll  .exe  .ini  .sys |
| EDR-6 | EDR podporuje funkcionalitu auditovania integrity súborov pre nasledujúce typy súborov Linux:  /bin  /boot  /etc  /sbin  /usr/bin  /usr/local/bin  /usr/local/sbin  /usr/sbin  /usr/share/keyrings  /var/spool/cron |

**2.1.5 Funkčné požiadavky na systém NTA**

|  |  |
| --- | --- |
| **Č.** | **Požiadavka** |
| NTA-1 | NTA podporuje zber nasledujúcich sieťových udalostí:  IDS udalosti  DHCP udalosti  DNS udalosti  IPv4 Flows |
| NTA-2 | NTA môže byť nasadené do internej či externej časti siete bez licenčného obmedzenia množstva nasadených zariadení |
| NTA-3 | NTA poskytuje špecifické korelačné pravidlá pre SIEM súvisiace s analýzou sieťovej prevádzky. |
| NTA-4 | NTA poskytuje špecifické vyhľadávacie vzory (queries) pre SIEM súvisiace s analýzou sieťovej prevádzky. |
| NTA-5 | NTA poskytuje špecifické šablóny pre tvorbu dashboard v SIEM súvisiace s analýzou sieťovej prevádzky. |
| NTA-6 | Zariadenie pre NTA môžeme inštalovať do fyzického , virtualizačného alebo cloud prostredia. |

**2.1.6 Funkčné požiadavky na systém DT**

|  |  |
| --- | --- |
| **Č.** | **Požiadavka** |
| DT-1 | DT podporuje tvorbu nasledujúcich pascí pre identifikovanie aktivít útočníka  HoneyPots  HoneyFiles  HoneyUsers  HoneyCredentials |
| DT-2 | DT poskytuje špecifické korelačné pravidlá pre SIEM súvisiacich s pascami |
| DT-3 | DTumožňuje vyhladávať vzory (queries) pre SIEM súvisiacich s pascami |
| DT-4 | DT pasce môžu byť nasadené do internej časti siete bez licenčného obmedzenia množstva nasadených zariadení |

**2.1.7 Ostatné požiadavky na komplexný nástroj**

* + Požadovaná retencia logov udalostí pre okamžité spracovanie systémom pre požadovaná počty zariadení je minimálne 360 dní. Systém musí zároveň umožňovať archivovať staršie záznamy
  + Systém musí obsahovať centrálne spravované riešenie, ktoré zbiera udalosti na pobočkách alebo v záložnom datacentre a umožňuje ich odoslanie po saturovanej linke bez straty dát
  + Systém musí podporovať centralizovanú správu pre zber udalostí z viacerých lokalít priamo z centrálneho úložiska dát vrátane požiadaviek na virtualizáciu a komunikačnú maticu pre šifrovaný prenos dát
  + Riešenie pre zber udalostí z iných lokalít musí byť schopné automaticky nadviazať spojenie s centrálnym úložiskom dát a prenášané dáta šifrovať. V prípade výpadku spojenia medzi inou lokalitou a centrálou musí spojenie automaticky obnoviť

**2.1.8 Implementácia komplexného nástroja v  rozsahu**

* + - nastavenie a konfigurácia prostredí verejného obstarávateľa,
      * konfigurácia Windows systémov pre zasielanie logov do systému,
      * overenie funkčných a výkonových parametrov Windows agentov,
      * konfigurácia Linux systémov pre zasielanie logov do systému,
      * overenie funkčných a výkonových parametrov Linux agentov,
      * predvedenie vytvorenia a uloženia vlastného dashboardu a reportu,
      * predvedenie vytvorenia a uloženia užívateľsky definovaného parseru,
    - nastavenie pravidelného zasielania definovaných reportov vybraným zamestnancom verejného obstarávateľa,
    - zaškolenie obsluhy a správy systému pre minimálne 2 zamestnancov verejného obstarávateľa,
    - vytvorenie a odovzdanie prevádzkovej dokumentácie systému, administrátorskej dokumentácie,

1. **Služby podpory prevádzky a údržby dodaného komplexného nástroja pre Kybernetickú bezpečnosť**
   * post-implementačná podpora v rozsahu **minimálne 1 človekodeň / mesačne na obdobie 12 kalendárnych mesiacov**, ktorá obsahuje:

* Technická  podpora prostredia
  + Inštalácia a konfigurácia
  + Konfigurácia systémových nastavení
  + Konfigurácia kolektorov
  + Konfigurácia alertov
  + Konfigurácia queries
  + Konfigurácia dashboard
  + Konfigurácia custom parser a event sources (data management)
  + podpora pri riešení technických problémov s platformou
* Konzultačná podpora pri identifikovaných bezpečnostných incidentoch
* Podpora ďalšieho rozvoja riešenia
  + zdroje udalostí,
  + integrácie
  + využitie funkcionalít systému,
  + licenčný model
* Komunikácia s výrobcom
  + hlásenie technických problémov výrobcovi,  dotazy na obchodnú podporu

1. **Postup pri riešení Problémov/požiadaviek – Helpdesk:**

Na hlásenie problémov zo strany Objednávateľa bude Poskytovateľ prevádzkovať Helpdesk, ktorý bude poskytovať službu, ktorá pozostáva z nasledujúcich činností:

* Identifikácia Problému – poskytnutie pomoci Objednávateľovi s cieľom identifikovať príčinu daného Problému v rozsahu podporovaného IS Objednávateľa,
* Poskytovanie informácií o stave riešenia požiadaviek prostredníctvom on-line vzdialeného prístupu oprávnených osôb Objednávateľa do Helpdesku.

**Postup**

1. Oprávnená osoba Objednávateľa zadáva/hlási problém/požiadavku v systéme Helpdesk na adrese: XXXXXX, v prípade nedostupnosti e-mailom na xxx Oprávnená osoba Objednávateľa nahlasuje problém podľa predchádzajúcej vety Poskytovateľovi až potom, ako nebolo možné vyriešiť tento problém v prvom stupni Oprávnenou osobou Objednávateľa.

Uskutočniť takéto hlásenie môže výlučne Oprávnená osoba Objednávateľa. Každé hlásenie Problému prijaté akýmkoľvek spôsobom sa zaeviduje v Helpdesku. Helpdesk vygeneruje identifikačné číslo požiadavky/problému. Helpdesk eviduje minimálne: čas odoslania hlásenia a oprávnenú osobu, kritickosť , čas prijatia hlásenia oprávnenou osobou Poskytovateľa, čas pridelenia riešiteľovi, čas zahájenia riešenia a čas vyriešenia požiadavky alebo Problému. Akákoľvek budúca komunikácia medzi Poskytovateľom a Objednávateľom sa uskutočňuje použitím priradeného identifikačného čísla požiadavky/Problému. Všetky záznamy, prílohy a komunikácia Oprávnených osôb Poskytovateľa a Objednávateľa sú evidované najmä v Helpdesku dostupnom on-line.

1. Špecialista Poskytovateľa preverí požiadavku/Problém a začne ich prešetrenie. Podľa potreby kontaktuje Oprávnenú osobu Objednávateľa. Komunikácia pracovníka Poskytovateľa prebieha priamo s Oprávnenou osobou Objednávateľa. Špecialista Poskytovateľa oznámi výsledok prešetrenia a odporúčané riešenie Oprávnenej osobe Objednávateľa. Na základe výsledkov prešetrenia bude pokračovať riešenie Problému.
2. Problém bude riešený na základe priority určenej dohodou a definíciou kategórie požiadavky/Problému Oprávnenými osobami Objednávateľa a Poskytovateľa. Oprávnená osoba Objednávateľa má právo zmeniť poradie priorít riešenia otvorených Problémov/požiadaviek po dohode s oprávneným zástupcom zo strany Poskytovateľa dokumentovateľným spôsobom – záznamom v Helpdesku.
3. Oprávnená osoba Objednávateľa po vykonaní služieb pracovníkom Poskytovateľa v priestoroch Objednávateľa alebo na diaľku vzdialeným pripojením, potvrdí poskytnutie služby a funkčnosť riešenia v Helpdesku.
4. Všetky vyriešené požiadavky /Problémy Objednávateľa musia byť potvrdené a ich vyriešenie musí byť zaevidované v Helpdesku. Splnenie požiadavky/Problému bude potvrdené v rozsahu ich riešenia Oprávnenou osobou Objednávateľa. Objednávateľ je povinný potvrdiť vyriešenie každej požiadavky/Problému najneskôr do 5 pracovných dní odo dňa jej vyriešenia. Akceptovanie riešenia požiadavky/Problému bude zaevidované priamo v Helpdesku. V prípade, ak Objednávateľ riešenie požiadavky/Problému neakceptuje, v rovnakej lehote svoje pripomienky a výhrady uvedie v Helpdesku. Ak Objednávateľ bez závažného dôvodu neakceptuje vyriešenie požiadavky/Problému a ani nevznesie pripomienky k riešeniu požiadavky/Problému ani do 5 pracovných dní od ich vykonania, považuje sa riešenie požiadavky/Problému za akceptované a Helpdesk automaticky vykoná mailovú notifikáciu.

Reakčná doba Poskytovateľa na problém Objednávateľa sa určuje na základe príslušnej úrovne spracovania Problémov. Čas sa vždy meria od momentu, kedy je Problém zaznamenaný do Helpdesku alebo v prípade nedostupnosti Helpdesku od momentu nahlásenia Problému alternatívnym spôsobom, t. j. od momentu doručenia hlásenia Problému emailom.

* + 1. **Služby podpory prevádzky a údržby dodaného komplexného nástroja softvéru**

|  |  |  |
| --- | --- | --- |
| **Popis** | **Parameter** | **Poznámka** |
| Prevádzkové hodiny | 9 hodín | 08:00 – 17:00 hod, počas pracovných dní |

### 

* + - 1. **Mimoriadna pohotovosť**

V prípade potreby, na základe žiadosti Objednávateľa, Poskytovateľ zabezpečí mimoriadnu pohotovosť a mimoriadne výkony nespadajúce do bežnej pracovnej doby. Objednávateľ je povinný takéto mimoriadne akcie nahlásiť Poskytovateľovi v predstihu minimálne desať (10) pracovných dní vopred.

|  |  |
| --- | --- |
| **Popis** | **Poznámka** |
| Pohotovosť – nočná | Od 17:00 – 8:00 hod počas pracovných dní |
| Pohotovosť – 24 hod. | 00:00 – 24:00 hod počas pracovných dní |
| 00:00 – 24:00 hod počas pracovných dní počas sviatkov a dní pracovného pokoja |

* + 1. **Úroveň spracovania požiadaviek/Problémov**

Prevádzkové hodiny Poskytovateľa pre Služby podpory prevádzky a údržby ,Služby podpory aplikačného programového vybavenia a systémového softvéru sú počas pracovných dní od 08:00 do 17:00 hod.

Čas mimo prevádzkové hodiny Poskytovateľa podľa predchádzajúcej vety sa do Reakčnej doby nezapočítava.

Reakčná doba Poskytovateľa na Problém sa určuje na základe príslušnej úrovne Problému. Poskytovateľ poskytuje Služby podpory prevádzky a Služby podpory aplikačného programového vybavenia a systémového softvéru podľa tabuľky uvedenej nižšie. Čas sa vždy meria od momentu, kedy je Problém zaznamenaný do Helpdesku.

|  |  |
| --- | --- |
| **Typ požiadavky** | **Reakčná doba v prevádzkových hodinách** |
| Kategória A - Kritický problém  Kritické poruchy alebo vady spôsobujúce nefunkčnosť komplexného nástroja | do 8 hod. |
| Kategória B - Nekritický problém | do 24 hod. |
| Kategória C – Modifikácia komplexného nástoja, iné požiadavky | do 48 hod. |

* + 1. **Akceptačné konanie**

Poskytovateľ sa zaväzuje poskytovať Služby podpory prevádzky a údržby, Služby podpory aplikačného programového vybavenia a systémového softvéru sústavne počas trvania Servisnej zmluvy, pričom akceptácia tohto plnenia je vykonaná na mesačnej báze na konci daného mesiaca.

Fakturácia je vykonávaná mesačne, pričom prílohou faktúry je report (výkaz):

* vykonaných Službách podpory prevádzky a údržby obsahujúci štatistiku (prehľad) a parametre poskytnutých služieb,