Dopravný podnik Bratislava, akciová spoločnosť
ako Objednávateľ

a

ako Poskytovateľ

ZMLUVA O POSKYTNUTÍ SLUŽBY

2024

TÁTO ZMLUVA O POSKYTNUTÍ SLUŽBY (ďalej len „**Zmluva**“) je uzatvorená nižšie uvedeného dňa medzi:

(1) **Dopravný podnik Bratislava, akciová spoločnosť**, spoločnosť založená a existujúca podľa práva Slovenskej republiky, so sídlom Olejkárska 1, 814 52 Bratislava, IČO: 00 492 736, zapísaná v Obchodnom registri Mestského súdu Bratislava III, oddiel: Sa, vložka číslo: 607/B, DIČ: 2020298786, IČ DPH: SK2020298786, bankové spojenie: VÚB, a. s., číslo účtu: 48009012/0200, IBAN: SK98 0200 0000 0000 4800 9012, BIC (SWIFT): SUBASKBX, štatutárny orgán: Ing. Milan Donoval, podpredseda predstavenstva - CTO a Mgr. Gabriela Dikošová, člen predstavenstva - CFO, kontaktná osoba pre technické veci: telefón: e-mail: , kontaktná osoba pre zmluvné veci: telefón: e-mail: (ďalej len „**Objednávateľ**“) na jednej strane; a

(2) **airo, s. r. o.**, spoločnosť založená a existujúca podľa práva Slovenskej republiky so sídlom Ivanská cesta 30/B, 821 04 Bratislava, IČO: 48286621, zapísaná v Obchodnom registri Mestského súdu Bratislava III, oddiel: Sro, vložka číslo: 106156/B , DIČ: 2120122488, IČ DPH: SK2120122488, bankové spojenie: Tatra banka, a.s., číslo účtu: 2941044557/1100, IBAN: SK8211000000002941044557, BIC (SWIFT): TATRSKBX, štatutárny orgán: Mgr. Jakub Čeles, konateľ, Ladislav Liščák, konateľ a Ing. Tomáš Nečas, konateľ, kontaktná osoba pre technické veci: telefón: e-mail: kontaktná osoba pre zmluvné veci: telefón: e-mail: k (ďalej len „**Poskytovateľ**“) na druhej strane.

Vzhľadom k tomu, že:

(A) Objednávateľ má záujem o **Dodanie, implementáciu a služby podpory prevádzky a údržby Kyberbezpečnostných systémov Endpoint Protection Platform (EPP) a Endpoint Detection and Response (EDR) vrátane dohľadových služieb 24/7 s kontrolou incidentov z prostredí objednávateľskej organizácie, poskytované výrobcom riešenia, s priamym riešením a uzatváraním týchto incidentov a s analýzou prvotnej príčiny incidentov** (ďalej ako EPPEDR), za účelom čoho realizoval zákazku podľa internej smernice ER 97/2017 o obstarávaní v podmienkach DPB, a. s. označenú interným číslom č. CP 22/2024 ***„Dodanie, implementáciu a služby podpory prevádzky a údržby Kyberbezpečnostných systémov Endpoint Protection Platform (EPP) a Endpoint Detection and Response (EDR) vrátane dohľadových služieb 24/7 s kontrolou incidentov z prostredí objednávateľskej organizácie, poskytované výrobcom riešenia, s priamym riešením a uzatváraním týchto incidentov a s analýzou prvotnej príčiny incidentov“***;

(B) Poskytovateľ sa stal úspešným uchádzačom zákazky označenej interným číslom CP 22/2024 ***„Dodanie, implementáciu a služby podpory prevádzky a údržby Kyberbezpečnostných systémov Endpoint Protection Platform (EPP) a Endpoint Detection and Response (EDR) vrátane dohľadových služieb 24/7 s kontrolou incidentov z prostredí objednávateľskej organizácie, poskytované výrobcom riešenia, s priamym riešením a uzatváraním týchto incidentov a s analýzou prvotnej príčiny incidentov“***; a

(C) Zmluvné strany majú záujem upraviť si vzájomné práva a povinnosti súvisiace s poskytnutím Služby;

DOHODLO SA nasledovné:

1 DEFINÍCIE A INTERPRETÁCIA ZMLUVNÝCH USTANOVENÍ

1.1 Pokiaľ nebude ďalej uvedené inak, potom budú mať výrazy použité v Zmluve s veľkými začiatočnými písmenami nasledovný význam:

(a) **Akceptačné testy** znamená testy novej alebo zmenenej funkčnosti, ktoré Objednávateľ realizuje podľa vopred vzájomne odsúhlasených testovacích scenárov a testovacích prípadov dodaných Poskytovateľom a ktorých úspešný priebeh je podmienkou akceptácie odovzdávanej funkčnosti;

(b) **Autorské dielo** znamená autorské dielo, vrátane počítačového programu alebo databázy, vytvorené výhradne na základe plnenia Zmluvy;

(c) **Bezpečnostná politika** znamená Bezpečnostná politika obstarávateľskej organizácie a predpismi informačnej bezpečnosti Objednávateľa sa v tomto prípade rozumie povinnosť uchádzača dodržiavať všeobecné bezpečnostné štandardy, ktoré sú v súlade so Zákonom č. 69/2018 Z. z. o Kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov a vyhláškou NBÚ č. 362/2018 Z. z.;

(d) **Cena** znamená odplatu za poskytnutie Služby ako celku v celkovej výške, bližšie špecifikovanej v Prílohe 2 Zmluvy;

(e) **Človekodeň** alebo **MD** znamená mernú jednotku pre vykazovanie prácnosti, za ktorú sa považuje 8 (osem) človekohodín;

(f) **Defekt** znamená nesúlad medzi skutočným stavom funkčnosti dodaného riešenia a medzi funkčnými špecifikáciami riešenia uvedenými v príslušnej objednávke a jej prílohách a/alebo funkčnými špecifikáciami komplexného nástroja pre EPPEDR zistený v rámci Akceptačných testov dodávky alebo v záručnej dobe v zmysle článku 5 Zmluvy;

(g) **GDPR** znamená nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov);

(h) **Helpdesk** znamená systém pre správu, evidenciu hlásení Problémov, servisných požiadaviek a požiadaviek na zmenu systému, evidenciu a sledovanie parametrov SLA (úrovne poskytovaných služieb);

(i) **Chyba Softvéru** znamená chybné fungovanie Softvéru komplexného nástroja pre EPPEDR, nesplnenie požiadaviek vyplývajúcich z platnej legislatívy dodávanej výrobcom softvéru alebo chybné fungovanie systémového softvéru;

(j) **IS Objednávateľa** alebo **IS** znamená Informačný systém ktorý predstavuje komplexný nástroj pre EPPEDR;

(k) **Kľúčový používateľ** znamená Oprávnenú osobu Objednávateľa oprávnenou nahlasovať, riešiť a/alebo potvrdzovať vyriešenie problémov spôsobmi uvedenými v Zmluve a/alebo zadávať požiadavky a/alebo potvrdzovať ich vybavenie podľa Zmluvy;

(l) **Komponent** znamená každý nový produkt, program, softvér, či funkčnosť, ktorý Poskytovateľ nainštaluje, nakonfiguruje, naprogramuje alebo nastaví v IS Objednávateľa a ktorý je doplnením alebo zmenou voči stavu zaznamenanému v dokumentácii k IS Objednávateľa, ktorú Objednávateľ odovzdá Poskytovateľovi v zmysle článku 12 bodu 12.2 Zmluvy;

(m) **Kritický problém** znamená problém, ktorý sa prejavuje takým výpadkom fungovania IS Objednávateľa, modulu alebo funkčnosti, ktorý znemožňuje jeho/jej použitie ako celku alebo jeho podstatnej časti. Za kritický sa považuje problém, ktorý sa prejavuje globálne voči nezastupiteľnej skupine používateľov. Ako kritický problém je charakterizovaný problém, ktorý je opakovane vyvolateľný alebo má trvalý charakter;

(n) **Legislatívne zmeny** znamená zmeny v právnych predpisoch zverejnené v Zbierke zákonov Slovenskej republiky, Úradnom vestníku Európskej únie a v interných predpisoch týkajúcich sa komplexného nástroja pre Kybernetickú bezpečnosť, ktoré nadobudli účinnosť od uzatvorenia Zmluvy;

(o) **Miesto plnenia** znamená: Dopravný podnik Bratislava, a. s.;

(p) **Nekritický problém** znamená každý problém, ktorý nie je Kritický problém, pričom sa prejavuje tým, že znemožňuje a/alebo obmedzuje používanie IS, modulu alebo funkčnosti z hľadiska koncového používateľa IS;

(q) **Občiansky zákonník** znamená zákona č. 40/1964 Zb. Občiansky zákonník v znení neskorších predpisov;

(r) **Obchodný zákonník** znamená zákon č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov;

(s) **Oprávnená osoba Objednávateľa** znamená zástupca Objednávateľa, ktorého identifikačné údaje, vrátane rozsahu oprávnení oznámi Objednávateľ Poskytovateľovi. Oprávnená osoba Objednávateľa je oprávnená nahlasovať, riešiť a/alebo potvrdzovať vyriešenie problémov spôsobmi uvedenými v Zmluve a/alebo zadávať požiadavky a/alebo potvrdzovať ich vybavenie podľa Zmluvy;

(t) **Oprávnená osoba Poskytovateľa** znamená zástupca Poskytovateľa, ktorého identifikačné údaje, vrátane rozsahu oprávnení oznámi Poskytovateľ Objednávateľovi;

(u) **Plán realizácie** znamená Poskytovateľom vyplnený formulár Plánu realizácie zmeny, ktorý tvorí Prílohu 3 Zmluvy;

(v) **Používateľ IS** znamená zamestnanci Objednávateľa;

(w) **Pracovný deň** znamená deň, ktorý nie je sobotou, nedeľou ani dňom pracovného pokoja ani dňom pracovného voľna v Slovenskej republike;

(x) **Problém** znamená Objednávateľom hlásený stav, ktorý znemožňuje a/alebo obmedzuje používanie IS Objednávateľa, je obmedzením jeho funkčnosti alebo rozporom fungovania oproti dodanej dokumentácii;

(y) **Reakčná doba** znamená pre Poskytovateľa stanovený čas, do ktorého zahájí prešetrenie nahláseného problému a ktorý začína plynúť nahlásením problému. Do reakčnej doby sa nezapočítava čas, kedy nie je možné z dôvodu na strane Objednávateľa sprístupnenie IS Objednávateľa za účelom neutralizácie problému;

(z) **Register partnerov verejného sektora** znamená informačný systém verejnej správy, ktorý obsahuje údaje o partneroch verejného sektora a ich konečných užívateľoch výhod, pričom jeho správcom a prevádzkovateľom je Ministerstvo spravodlivosti Slovenskej republiky a je prístupný on-line na webovom sídle Ministerstva spravodlivosti Slovenskej republiky na adrese https://rpvs.gov.sk/rpvs/;

(aa) **Zmluva** znamená táto zmluva o dodaní, implementácii a službách podpory prevádzky a údržby komplexného nástroja pre EPPEDR;

(bb) **Servisné okno** znamená časový interval určený pre nasadzovanie zmien na produktívne prostredie jednotlivých systémov IS;

(cc) **Služba** znamená dodanie, implementácia a podpora prevádzky a údržby komplexného nástroja pre kybernetickú bezpečnosť v rozsahu podľa článku 3 Zmluvy;

(dd) **Služby** – služby poskytované na základe Zmluvy, predstavujú: (i) Služby o dodaní, implementácii komplexného nástroja pre Kybernetickú bezpečnosť, (ii) Služby podpory prevádzky a údržby komplexného nástroja pre Kybernetickú bezpečnosť poskytované na základe Zmluvy, ktorých parametre a podmienky poskytovania sú uvedené v Prílohe 1 Zmluvy;

(ee) **Služby o dodaní, implementácii komplexného nástroja pre EPPEDR** znamená služby, ktorých predmetom je dodanie a implementácia komplexného nástroja pre EPPEDR do prostredia objednávateľa;

(ff) **Služby podpory prevádzky a údržby komplexného nástroja pre EPPEDR** znamená služby, ktorých predmetom je najmä podpora používateľov pri používaní funkcionality systému, riešenie porúch, aktualizácia systémových nastavení aplikačného programového vybavenia, riešenie požiadaviek na zmenu systému, analýza porúch a v prípade zistenia poruchy tretích strán zadanie požiadaviek na tretie strany pre ich riešenie na úrovni 3rd level supportu, konzultačná podpora, aktualizácia príslušnej dokumentácie a zmeny funkčnosti IS Objednávateľa, ktoré vyplývajú z novo vzniknutých potrieb Objednávateľa, zmeny konfigurácie a nastavení IS vynútené zmenami prevádzkového prostredia Objednávateľa a udržiavanie aktuálnosti príslušnej dokumentácie IS poskytované na základe Zmluvy, ktorých parametre a podmienky poskytovania sú uvedené v Prílohe 1 Zmluvy;

(gg) **SW komponent** znamená časť IS Objednávateľa, ktorú možno používať samostatne a nezávisle od ostatných častí IS Objednávateľa;

(hh) **SW produkt 3. strany** znamená krabicový SW (FPP – Full Packaged Product), prípadne SW riešenie, ktoré nie je osobitne vytvorené pre Objednávateľa, ale tvorí súčasť IS Objednávateľa, a ktorý sa spravuje osobitnými licenčnými podmienkami výrobcu;

(ii) **Úroveň spracovania požiadaviek** znamená reakčnú dobu definovanú medzi Zmluvnými stranami v Prílohe 1 Zmluvy v závislosti od kategórie problému;

(jj) **Vady a nedostatky** znamená Poskytovateľom alebo Objednávateľom zistené odchýlky oproti aktuálnej dokumentácii IS a majú za následok chyby funkcionality, nedostupnosť už dodanej a riadne prevzatej funkcionality alebo obvyklej funkcionality aplikačného programového vybavenia, nedostatky interoperability softvéru s inými počítačovými programami alebo databázami, zvýšené požiadavky na databázu alebo výkon systému, prekročenie požadovanej doby odozvy systému, zníženie používateľského komfortu, ukončenie podpory aktuálne prevádzkovanej verzie komponentov IS spôsobujúce problémy pri prevádzke, neimplementované bezpečnostné záplaty dodávané výrobcom aplikačného programového vybavenia a podobne, o ktorých je Poskytovateľ povinný informovať Objednávateľa a navrhovať opatrenia potrebné pre ich odstránenie;

(kk) **Zákon o ochrane osobných údajov** znamená zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov;

(ll) **Zmluvná strana** znamená Objednávateľ a/alebo Poskytovateľ.

1.2 Okrem definovaných pojmov uvedených v článku 1 bode 1.1 Zmluvy, ak je inde v Zmluve použitý definovaný pojem, v Zmluve bude mať takýto pojem význam, ktorý mu je priradený v príslušnej časti Zmluvy, kde je definovaný.

1.3 V Zmluve, ak z kontextu nevyplýva iný zámer,

(a) každý odkaz na Zmluvnú stranu zahŕňa aj jej právnych nástupcov ako aj postupníkov a nadobúdateľov práv alebo záväzkov, vyplývajúcich zo Zmluvy;

(b) každý odkaz na Zmluvu alebo iný dokument znamená Zmluvu alebo iný dokument v znení jeho dodatkov a iných zmien, vrátane novácií;

(c) prílohy Zmluvy predstavujú jej neoddeliteľné súčasti a správny výklad ustanovení Zmluvy je možný len s prihliadnutím na ich obsah. Nadpisy častí, článkov a príloh slúžia výlučne pre uľahčenie orientácie a pri výklade Zmluvy sa nepoužijú;

(d) každý odkaz na „článok" alebo „prílohu" znamená odkaz na príslušný článok alebo prílohu Zmluvy; a

(e) výrazy definované v jednotnom čísle alebo v základnom gramatickom tvare majú v Zmluve rovnaký význam, keď sú použité v množnom čísle a inom gramatickom tvare a naopak.

2 PREDMET ZMLUVY

2.1 Predmetom Zmluvy je záväzok:

(a) Poskytovateľa poskytnúť Objednávateľovi Službu; a

(b) Objednávateľa zaplatiť Poskytovateľovi Cenu;

a to za podmienok stanovených Zmluvou.

2.2 Poskytnutie Služby bude uskutočnené na základe písomnej objednávky. Takto vystavená objednávka bude podkladom pre fakturáciu podľa článku 4 Zmluvy. Objednávku môže Objednávateľ zaslať poštou alebo elektronickou poštou na emailovú adresu kontaktnej osoby pre technické veci Poskytovateľa uvedenej v záhlaví Zmluvy. Doručením objednávky Poskytovateľovi sa objednávka považuje za potvrdenú Poskytovateľom.

2.3 Cena za poskytnutie Služby je Zmluvnými stranami stanovená v celkovej výške 124 795,70 **EUR** (slovom: stodvadsaťštyritisíc sedemstodeväťdesiat päť eur a sedemdesiat centov) bez DPH.

3 PODMIENKY POSKYTOVANIA SLUŽIEB

3.1 Poskytovateľ sa zaväzuje poskytnúť Službu riadne, včas a v rozsahu podľa objednávky. Zmluvné strany sa dohodli, že Poskytovateľ je povinný poskytnúť Službu **do 30 dní** odo dňa doručenia objednávky podľa článku 2 bod 2.2 Zmluvy.

3.2 Poskytnutie Služby zahŕňa prevádzku, údržbu a aktualizáciu IS Objednávateľa v rozsahu a za podmienok stanovených Zmluvou, a to prostredníctvom Služby podpory prevádzky a údržby komplexného nástroja pre Kybernetickú bezpečnosť.

3.3 Poskytovateľ sa zaväzuje poskytnúť Objednávateľovi Službu vo vlastnom mene, na vlastnú zodpovednosť a na vlastné nebezpečenstvo, za podmienok dohodnutých v Zmluve, samostatne, na požadovanej odbornej úrovni a v súlade s príslušnými osobitnými predpismi a slovenskými technickými normami. Zmluvné strany sa dohodli, že porušenie odbornej starostlivosti Poskytovateľom sa považuje za podstatné porušenie Zmluvy.

3.4 Poskytovateľ sa zaväzuje udržiavať IS Objednávateľa v súlade s podmienkami stanovenými Zmluvou a dodanou dokumentáciou a v prípade schválených zmien IS Objednávateľa udržiavať aktuálnosť tejto dokumentácie v zmysle tohto článku bodu 3.6. Zmluvy, v prípade neexistencie dokumentácie, vytvoriť a udržiavať aktuálnosť dokumentácie ku všetkým vykonaním činnostiam pri poskytovaní Služieb.

3.5 Poskytovateľ sa zaväzuje bez zbytočného odkladu podávať Objednávateľovi správy o priebehu ním poskytovaných Služieb podľa Zmluvy, tak ako je uvedené v Prílohe 1 Zmluvy.

3.6 Poskytovateľ sa zaväzuje bez zbytočného odkladu informovať Objednávateľa o nových skutočnostiach, ktoré vyšli najavo v súvislosti s poskytovaním Služieb, najmä o prípadných zistených vadách a nedostatkoch IS Objednávateľa, pričom súčasne je povinný navrhovať opatrenia potrebné pre ich odstránenie v súlade s touto Zmluvou.

3.7 Poskytovateľ je povinný pri poskytovaní Služieb dodržiavať a aplikovať povinnosti vyplývajúce z príslušných osobitných predpisov vzťahujúcich sa na IS Objednávateľa, ako aj Služby Poskytovateľa, Zákona o ochrane osobných údajov a GDPR.

3.8 Poskytovateľ je ďalej povinný:

(a) udržiavať aktuálnosť používateľskej, prevádzkovej, servisnej a administrátorskej dokumentácie, prípadne jej doplnky vzniknuté počas účinnosti Zmluvy, a to v súlade s aktuálnym stavom IS Objednávateľa, v prípade neexistencie dokumentácie, vytvárať a udržiavať v aktuálnom stave dokumentáciu ku všetkým vykonávaným činnostiam pri poskytovaní Služby;

(b) poskytovať Služby v lehotách dohodnutých v Zmluve, resp. lehotách osobitne dohodnutých Zmluvnými stranami, v prípade, ak takúto dohodu Zmluva pripúšťa alebo prezumuje; v prípadoch, kde Zmluva ponecháva určenie lehoty (času plnenia) na voľbe Poskytovateľa, je tento povinný bez zbytočného odkladu informovať Objednávateľa o lehote poskytnutia príslušného plnenia (čase plnenia);

(c) na základe žiadosti Objednávateľa zabezpečiť prítomnosť kvalifikovaných špecialistov, ktorých prítomnosť je nevyhnutná pre poskytovanie Služieb v dohodnutom mieste plnenia;

(d) v prípade potreby bezodkladne špecifikovať a predložiť Objednávateľovi požiadavky na potrebný HW a kompatibilitu SW, požiadavky na služby poskytované tretími stranami bezprostredne súvisiace s prevádzkou IS Objednávateľa;

(e) telefonicky, resp. písomne (e-mailom) v stanovenej lehote reagovať na každú požiadavku Objednávateľa zadanú dohodnutým spôsobom nahlasovania prostredníctvom HelpDesku, týkajúcu sa predmetu Zmluvy;

(f) zabezpečiť, aby Poskytovateľ na základe požiadavky Objednávateľa na zapracovanie zmeny bez zbytočného odkladu predložil odhad časovej a finančnej náročnosti zapracovania uvedenej požiadavky resp. špecifikáciu dopadu na spôsob používania IS Objednávateľa, stanoveným procesom change manažmentu; a

(g) informovať Objednávateľa o všetkých skutočnostiach, ktoré by mohli negatívne vplývať na plnenie predmetu Zmluvy.

3.9 Objednávateľ sa zaväzuje, že pri realizácii plnenia predmetu Zmluvy zabezpečí v záujme plynulého priebehu plnenia požadovanú nevyhnutnú súčinnosť, spočívajúcu predovšetkým v poskytnutí potrebných informácií, materiálnych prostriedkov, odovzdaní potrebných údajov a podkladov, ako aj spresnení týchto údajov a podkladov. Potreba takýchto informácií sa dohodne vopred, prípadne sa preukáže v priebehu plnenia.

3.10 Objednávateľ na základe písomnej požiadavky Poskytovateľa poskytne v primeranej lehote v dĺžke najmenej 5 (piatich) Pracovných dní, s výnimkou súčinnosti podľa tohto článku bodu 3.9. Zmluvy, pri ktorej lehota nemôže byť kratšia ako 10 (desať) Pracovných dní, najmä nasledovnú súčinnosť:

(a) poskytne Poskytovateľovi v nevyhnutnom rozsahu prístup na systémový a aplikačný softvér a hardvér, ako aj prístup do priestorov potrebných pre plnenie podľa Zmluvy, pod ktorými sa rozumie poskytnutie prevádzkového priestoru na prevádzkovej infraštruktúre a v prevádzkových priestoroch po dobu nevyhnutnú pre zásah;

(b) zabezpečí kontrolovaný prístup v nevyhnutnom rozsahu k hardvéru a softvéru pomocou diaľkového prenosu dát, a to v rozsahu vymedzenom Poskytovateľom, pričom Poskytovateľ je povinný dodržiavať ochranu dát Objednávateľa a konať tak, aby svojou činnosťou nenarušil prevádzku ostatných systémov Objednávateľa;

(c) poskytne informácie nevyhnutne potrebné pre implementáciu a konfiguráciu jednotlivých Komponentov IS Objednávateľa, ktoré si Poskytovateľ písomne vyžiada;

(d) zabezpečí realizáciu Akceptačných testov podľa pripravených testovacích scenárov;

(e) zabezpečí prevádzkové prostredie (všetky servery), na ktorých je IS Objednávateľa prevádzkovaný tak, že akékoľvek balíky služieb (service packy) operačných systémov a softvérových produktov, ktoré majú dopad na prevádzku IS Objednávateľa, nebudú aplikované bez predchádzajúcej konzultácie s Poskytovateľom;

(f) zabezpečí poskytovanie štandardnej podpory SW produktov 3. strán, tzn. podpora v rámci podmienok údržby Softvérového produktu 3. strany (na základe licencie výrobcu softvéru – tzv. softvérový maintenance);

(g) zabezpečí podľa pokynov Poskytovateľa vykonanie opatrení ktoré môžu spresniť diagnostikovanie problému a urýchliť jeho odstránenie; a

(h) zabezpečí dodržiavanie postupov v zmysle prevádzkovej príručky a Backup & Recovery plánu odsúhlasenej Zmluvnými stranami.

3.11 Objednávateľ je povinný poskytnúť Poskytovateľovi všetky nevyhnutné informácie a materiály opodstatnene potrebné pre realizáciu Zmluvy, ktoré Poskytovateľ odôvodnene požaduje, aby sa tak Poskytovateľovi umožnilo poskytnúť plnenie. Objednávateľ sa zaväzuje, že vyvinie všetko úsilie, ktoré je od neho možné spravodlivo požadovať, aby všetky informácie, ktoré poskytne Poskytovateľovi, alebo ktoré bude musieť poskytnúť Poskytovateľovi, boli v každom vecnom ohľade pravdivé, presné a nezavádzajúce. Poskytovateľ nebude zodpovedný za akékoľvek straty, škody ani nedostatky Služieb, vyplývajúce z nepresných, neúplných alebo inak závadných informácií alebo materiálov, ktoré dodal Objednávateľ, ak na nepresnosť, neúplnosť alebo závadnosť informácií alebo materiálov Objednávateľa písomne upozornil, pokiaľ Poskytovateľ nepresnosť, neúplnosť alebo závadnosť pri vynaložení odbornej starostlivosti zistil alebo mohol zistiť.

3.12 Ak Objednávateľ neposkytne Poskytovateľovi požadovanú súčinnosť v zmysle tohto článku bodov 3.10. a 3.11. Zmluvy, plynutie doby odstránenia problému, na ktorú bolo poskytnutie súčinnosti zo strany Objednávateľa potrebné, sa prerušuje; Plynutie doby odstránenia problému sa prerušuje i v prípadoch:

(a) dlhodobého výpadku elektrickej energie v mieste prevádzkovania primárnej lokality;

(b) živelnej pohromy v mieste prevádzkovania primárnej lokality;

(c) nefunkčnej sieťovej konektivity;

(d) totálneho softvérového poškodenia IS zavinené úmyselne Objednávateľom alebo tretími stranami, vrátane neznámych agresívnych vírusov alebo hackerských útokov;

(e) chyby softvérov tretích strán, na ktoré nie je k dispozícii záplata;

(f) straty alebo poškodenia zálohovacích nosičov (pások) nepredvídateľnou udalosťou, nesprávnou manipuláciou alebo ich vadou;

(g) poruchy zapríčinenej chybou prevádzkovej infraštruktúry;

(h) súčasného zničenia diskov obsahujúcich zrkadlové obrazy databáz a transakcií – straty údajov od poslednej zálohy; a/alebo

(i) súčasného zničenia diskov obsahujúcich zrkadlové obrazy databáz a transakcií a zálohovacích médií – straty všetkých údajov.

Poskytovateľ je však povinný v režime „best efforts", t.j. pri vynaložení náležitého úsilia a dostupných zdrojov, vykonať čo najskôr všetky úkony, ktoré je možné od neho spravodlivo požadovať za účelom minimalizácie následkov vzniknutého Problému, predovšetkým v podobe implementácie náhradného riešenia, ak je takéto napriek neposkytnutej súčinnosti zo strany Objednávateľa možné.

3.13 Poskytovateľ je povinný oboznámiť Objednávateľa so všetkými skutočnosťami, ktoré predstavujú porušenie informačnej bezpečnosti alebo môžu zásadne zvyšovať bezpečnostné riziko.

3.14 Objednávateľ poskytuje Poskytovateľovi bezodplatne súhlas na použitie častí IS Objednávateľa a/alebo dokumentácie, ktoré sú predmetom autorskoprávnej ochrany a vo vzťahu ku ktorým je Objednávateľ oprávnený takýto súhlas udeliť, a to výhradne v rozsahu potrebnom a nevyhnutnom na účely riadneho a včasného plnenia Zmluvy Poskytovateľom.

3.15 Zmluvné strany sa zaväzujú, že počas trvania Zmluvy budú navzájom spolupracovať a vyvinú súčinnosť potrebnú na dosiahnutie účelu Zmluvy.

3.16 Služba sa považuje za poskytnutú riadne a včas v lehote podľa tohto článku bod 3.1 Zmluvy Poskytovateľom, odovzdaním Preberacieho protokolu Objednávateľovi. Preberací protokol podpíšu oprávnené osoby za obe Zmluvné strany, ak bola Služba poskytnutá bez výhrad.

3.17 Poskytovateľ sa zaväzuje, že dodané komponenty vyrába výrobca predmetných komponentov, pričom Poskytovateľ je povinný preukázať, že dodané komponenty spĺňajú požiadavky na technické vlastnosti podľa predchádzajúcej vety, ak ho o to Objednávateľ požiada.

3.18 Poskytovateľ je povinný odovzdať Objednávateľovi spolu s komponentami súvisiace doklady potrebné na jeho prevzatie, a to najmä:

(a) vytlačené zadanie objednávky;

(b) dodací list; a

(c) všetky doklady, ktoré sa na dodané komponenty vzťahujú (ako napr. vyhlásenie o zhode, návod na použitie, informácie o manipulovaní a skladovaní a pod.).

3.19 Objednávateľ je povinný skontrolovať dodané komponenty pred ich použitím. Ak počas kontroly dodaných komponentov budú zistené podstatné vady dodaných komponentov, Objednávateľ si vyhradzuje právo odmietnuť použitie takýchto komponentov pri oprave. Komponenty majú podstatné vady, ak Poskytovateľ nedodrží dohodnutú akosť, štruktúru, vlastnosti alebo množstvo komponentov špecifikovaných objednávkou a/alebo Zmluvou.

3.20 V prípade, ak Objednávateľ pri kontrole komponentov zistí, že dodané komponenty majú zjavné podstatné vady, Objednávateľ môže odmietnuť Službu ako celok. Poskytovateľ zodpovedá v tomto prípade Objednávateľovi podľa ustanovení o zmluvnej pokute uvedenej v článku 8 bod 8.1 Zmluvy

3.21 Vlastnícke právo ku komponentom prechádza na Objednávateľa okamihom riadneho poskytnutia Služby Poskytovateľom bez výhrad podľa tohto článku bod 3.16 Zmluvy, ak nedošlo zo strany Objednávateľa k odmietnutiu poskytnutia Služby podľa tohto článku bodu 3.20 Zmluvy. V prípade odmietnutia poskytnutia služby zo strany Objednávateľa podľa tohto článku bod 3.20 Zmluvy zostávajú komponenty vo vlastníctve Poskytovateľa až do doby, kým Poskytovateľ neodstráni prekážku, ktorá bráni Poskytovateľovi riadne poskytnúť Službu.

4 CENA ZA SLUŽBY A PLATOBNÉ PODMIENKY

4.1 Cena je stanovená za poskytnutie Služby ako celku a je konečná, bez možnosti doúčtovania ďalších nákladov. V Cene bez DPH sú zahrnuté všetky náklady, ktoré sú spojené s poskytnutím Služby, vrátane nákladov na dopravu Poskytovateľa do/z Miesta plnenia. Pri DPH sa bude postupovať podľa osobitných predpisov.

4.2 Cena za Poskytnutie Služby je stanovená vo forme jednorazovej platby vo výške **124 795,70 EUR (slovom: stodvadsaťštyritisíc sedemstodeväťdesiat päť eur a sedemdesiat centov) bez DPH.** Jednorazová platba pokrýva všetky a akékoľvek náklady Poskytovateľa v rámci poskytovania Služby, a to bez ohľadu na množstvo prác, ktoré bude potrebné pri implementácii.

4.3 Poskytovateľ je oprávnený vystaviť faktúru za jednorazovú platbu za **Službu podľa bodu 4.2** do 30 dní odo dňa, kedy došlo k začatiu poskytovania Služby.

4.4 Záväzok Objednávateľa zaplatiť za poskytnutie Služby bude splnený pripísaním sumy peňažného záväzku (vrátane DPH) na účet Poskytovateľa.

4.5 Faktúra musí obsahovať všetky náležitosti účtovného dokladu podľa § 10 zákona č. 431/2002 Z. z. o účtovníctve v znení neskorších predpisov, náležitosti podľa § 74 zákona č. 222/2004 Z. z. o dani z pridanej hodnoty v znení neskorších predpisov, evidenčné číslo Zmluvy, pod ktorou je zmluva evidovaná Objednávateľom prípade, ak faktúra nebude spĺňať tieto náležitosti a náležitosti podľa tohto článku bod 4.2 Zmluvy je Objednávateľ oprávnený vrátiť faktúru na dopracovanie, resp. opravu. Taktiež v prípade, ak výška fakturovanej sumy nebude zodpovedať podkladom Objednávateľa, je Objednávateľ oprávnený vrátiť faktúru Poskytovateľovi na prepracovanie. Nová lehota splatnosti začína plynúť okamihom doručenia opravenej faktúry Objednávateľovi.

4.6 Cena je splatná do **60 (šesťdesiat) dní** odo dňa doručenia faktúry na adresu sídla Objednávateľa. Ak deň splatnosti Ceny pripadne na sobotu, nedeľu alebo sviatok, splatnosť takejto faktúry sa posúva na najbližší nasledujúci Pracovný deň. Cena sa považuje za zaplatenú dňom odpísania fakturovanej sumy vo výške Ceny z účtu Objednávateľa na účet Poskytovateľa uvedený v záhlaví Zmluvy.

5 ZODPOVEDNOSŤ ZA VADY, ZÁRUKA A ZÁRUČNÁ DOBA

5.1 Záručná doba na Komponenty a riešenia vytvorené a/alebo dodané Poskytovateľom, ktoré Poskytovateľ nainštaluje, nakonfiguruje, naprogramuje alebo nastaví v IS, je **36 mesiacov** odo dňa, keď Objednávateľ protokolárne prevezme Komponent/riešenie do rutinnej /produktívnej prevádzky, najdlhšie však Záručná doba trvá do dňa ukončenia poskytovania Služby podľa bodu 11.1 Zmluvy. Poskytovateľ sa zaručuje, že dodané Komponenty/riešenia neporušujú akékoľvek autorské práva, resp. iné práva, ako aj práva tretích osôb. Pre vylúčenie pochybností, záruka sa nevzťahuje na SW produkty 3. strán. Záručná doba sa predlžuje o dobu odo dňa uplatnenia reklamácie po deň odstránenia vád poskytnutej Služby.

5.2 Poskytovateľ ručí za to, že výsledky poskytnutej Služby budú mať počas celej záručnej doby vlastnosti dohodnuté Zmluvou, zodpovedajúce právnym a technickým normám a predpisom, že Služba bude poskytnutá bez vád, ktoré by rušili alebo znižovali jej kvalitu.

5.3 Poskytovateľ zodpovedá za riadne a včasné plnenie záväzkov vyplývajúcich zo Zmluvy. Poskytovateľ zodpovedá aj za skryté vady poskytnutej Služby, ktoré Objednávateľ zistil po poskytnutí Služby. Objednávateľ je povinný Poskytovateľovi písomne oznámiť vadu poskytnutej Služby bezodkladne po tom, čo ju zistil. V prípade, že sa preukáže zodpovednosť Poskytovateľa za skryté vady počas záručnej doby, je Poskytovateľ povinný v súlade s § 373 a nasl. Obchodného zákonníka nahradiť Objednávateľovi aj prípadnú, z takéhoto titulu, vzniknutú škodu.

5.4 Objednávateľ bez zbytočného odkladu písomne oznámi Poskytovateľovi vady poskytnutej Služby, ktoré sa vyskytli v rámci záručnej doby, pričom v oznámení popíše chyby a uvedie ako sa prejavujú. Na základe písomnej reklamácie Objednávateľa podľa predchádzajúcej vety je Poskytovateľ povinný na svoje náklady a bez zbytočného odkladu odstrániť počas záručnej doby reklamované vady poskytnutej Služby, a to aj v prípade, ak sa domnieva, že za reklamované vady nezodpovedá. V takom prípade, ak sa Zmluvné strany nedohodnú inak, až do doby právoplatného rozhodnutia súdu o reklamácii znáša náklady na odstránenie reklamovaných vád Poskytovateľ.

5.5 Poskytovateľ je povinný odstrániť vady poskytnutej služby **bezodkladne, najneskôr však do 5. Pracovného dňa nasledujúceho po dni** oznámenia písomnej reklamácie Objednávateľa podľa tohto článku bod 5.4 Zmluvy.

5.6 Pokiaľ Poskytovateľ nesplní svoju povinnosť odstrániť vady v lehote stanovenej v písomnom oznámení Objednávateľa podľa tohto článku bod 5.5 Zmluvy, je Objednávateľ oprávnený tieto vady sám alebo pomocou tretej osoby odstrániť a Poskytovateľ je povinný uhradiť náklady na odstránenie vád. Takýmto postupom Objednávateľa alebo inej oprávnenej osoby nie je dotknutá záruka poskytnutá Poskytovateľom.

5.7 Poskytovateľ nezodpovedá za chyby spôsobené dodržaním nevhodných pokynov zo strany Objednávateľa, ak na nevhodnosť týchto pokynov Poskytovateľ Objednávateľa písomne upozornil a Objednávateľ na ich dodržaní aj napriek tomu trval. Poskytovateľ nezodpovedá Objednávateľovi za škodu, ktorá mu bola spôsobená vyššou mocou. Za vyššiu moc sa považuje taká vonkajšia okolnosť, ktorú Poskytovateľ nemohol odvrátiť alebo prekonať, ani ju v dobe vzniku predvídať.

5.8 Zmluvné strany sa dohodli, že zodpovednosť za vady sa ďalej spravuje príslušnými ustanoveniami Obchodného zákonníka.

6 PRÁVO DUŠEVNÉHO VLASTNÍCTVA

6.1 Na každé Autorské dielo udeľuje Poskytovateľ Objednávateľovi časovo neobmedzenú (po dobu právnej ochrany majetkových práv trvajúcu), nevýhradnú a cenou podľa Zmluvy splatenú licenciu na akékoľvek použitie takého Autorského diela ako celku i jeho jednotlivých častí v neobmedzenom rozsahu, ktorý pre zamedzenie pochybností zahŕňa všetky známe spôsoby použitia tohto Autorského diela, ktorými sú najmä právo Autorské dielo spracovať (zmeniť a/alebo upraviť) alebo dať spracovať (zmeniť a/alebo upraviť) tretej osobe, vyhotovenie rozmnoženiny Autorského diela, verejné rozširovanie originálu Autorského diela alebo jeho rozmnoženiny predajom alebo inou formou prevodu vlastníckeho práva, verejné rozširovanie originálu autorského diela alebo jeho rozmnoženiny nájmom alebo vypožičaním, spracovanie, preklad Autorského diela a verejný prenos Autorského diela, a to ako Objednávateľom osobne, tak aj osobami ním poverenými s tým, že taká licencia zahŕňa aj výslovný súhlas na udelenie sublicencie na používanie Autorského diela pre akékoľvek tretie osoby, či na prevedenie takej licencie na tretie osoby verejnej správy.

6.2 Licenciu v rozsahu podľa tohto článku bodu 6.1 Zmluvy poskytuje Poskytovateľ Objednávateľovi s účinnosťou odo dňa podpisu akceptačného protokolu ohľadom plnenia, ktorého je také Autorské dielo súčasťou, s tým, že pre splnenie podmienky poskytnutia komentovaných zdrojových kódov a dátového modulu Autorského diela poskytne Poskytovateľ Objednávateľovi funkčnú špecifikáciu Autorského diela vo forme umožňujúcej jeho ďalšie použitie spôsobom definovaným licenciou.

6.3 V prípade, že akákoľvek tretia osoba, vrátane zamestnancov Poskytovateľa, bude mať akýkoľvek nárok voči Objednávateľovi z titulu porušenia jej autorských práv a/alebo práv priemyselného a/alebo iného duševného vlastníctva plnením Poskytovateľa podľa Zmluvy alebo akékoľvek iné nároky vzniknuté porušením jej práv Poskytovateľom pri plnení Zmluvy, Poskytovateľ sa zaväzuje:

(a) bezodkladne obstarať na svoje vlastné náklady a výdavky od takejto tretej osoby súhlas na používanie jednotlivých plnení dodaných, poskytnutých, vykonaných a/alebo vytvorených Poskytovateľom, alebo tretími osobami pre Objednávateľa, alebo upraviť jednotlivé plnenie(a) dodané, poskytnuté, vykonané a/alebo vytvorené Poskytovateľom, alebo tretími osobami pre Objednávateľa tak, aby už ďalej neporušovali autorské práva a/alebo práva priemyselného a/alebo iného duševného vlastníctva tretej osoby, alebo nahradiť jednotlivé plnenie(a) dodané, poskytnuté, vykonané a/alebo vytvorené Poskytovateľom, alebo tretími osobami pre Objednávateľa rovnakými alebo aspoň takými plneniami, ktoré majú aspoň podstatne podobné kvalitatívne, operačné a technické parametre a funkčnosti, alebo, ak sa jedná o plnenie poskytnuté na základe licencie tretej osoby, taký nárok vyriešiť v súlade s tým, čo pre taký prípad stanovujú jej licenčné podmienky uvedené v Zmluve, a ak ich niet, tak v súlade s týmito podmienkami;

(b) poskytnúť Objednávateľovi účinnú pomoc a uhradiť náklady a výdavky, ktoré vznikli/vzniknú Objednávateľovi v súvislosti s uplatnením vyššie uvedeného nároku tretej osoby; a

(c) nahradiť Objednávateľovi škodu, ktorá vznikne Objednávateľovi v dôsledku uplatnenia vyššie uvedeného nároku tretej osoby.

6.4 Objednávateľ sa však zaväzuje, že o každom nároku vznesenom takou treťou osobou v zmysle hore uvedeného bude bez zbytočného odkladu informovať Poskytovateľa, bude v súvislosti s takým nárokom postupovať podľa primeraných a opodstatnených pokynov Poskytovateľa a tak, aby sa predišlo vzniku a prípadne zvýšeniu škôd, nevykoná smerom k takej tretej osobe žiaden úkon, v dôsledku ktorého by sa jej postavenie v súvislosti s takým uplatnením nároku zlepšilo, a Poskytovateľovi udelí a po potrebnú dobu neodvolá plnomocenstvo s možnosťou splnomocniť ďalšiu osobu potrebné na to, aby sa Poskytovateľ mohol za Objednávateľa účinne takému nároku brániť a s takou treťou osobou rokovať o urovnaní sporu resp. spôsobom vhodným podľa opodstatneného uváženia Poskytovateľa postupovať v záujme ochrany práv oboch strán.

6.5 Poskytovateľ nenesie zodpovednosť za akúkoľvek Poskytovateľom neautorizovanú zmenu autorského diela vykonanú Objednávateľom alebo treťou osobou poverenou Objednávateľom. Spôsob autorizácie zmien je povinnou súčasťou dodávky Autorského diela.

7 BEZPEČNOSŤ A OCHRANA INFORMÁCIÍ

7.1 Zmluvné strany sa zaväzujú zachovávať mlčanlivosť o dôverných informáciách, o ktorých sa dozvedeli od druhej Zmluvnej strany pri plnení Zmluvy, resp. v rámci samotného plnenia predmetu Zmluvy. Ak nie je ďalej v Zmluve ustanovené inak, za dôvernú informáciu sa považuje akýkoľvek údaj, podklad, poznatok, dokument alebo akákoľvek iná informácia, bez ohľadu na formu jej zachytenia:

(a) ktorá sa týka Zmluvnej strany alebo Používateľa IS (informácie o jej činnosti, štruktúre, hospodárskych výsledkoch, všetky zmluvy, finančné, štatistické a účtovné informácie, informácie o jej majetku, aktívach a pasívach, pohľadávkach a záväzkoch, informácie o jej technickom a programovom vybavení, know-how, hodnotiace štúdie a správy, podnikateľské stratégie a plány, informácie týkajúce sa predmetov chránených právom priemyselného alebo iného duševného vlastníctva a všetky ďalšie informácie o zmluvnej strane alebo Používateľovi IS);

(b) ktorá bola poskytnutá Zmluvnej strane alebo získaná Zmluvnou stranou pred nadobudnutím účinnosti Zmluvy, pokiaľ sa týka jej predmetu a/alebo obsahu;

(c) ktorá je výslovne Zmluvnou stranou označená ako „dôverná", „confidential", „proprietary" alebo iným obdobným označením, a to od okamihu oznámenia tejto skutočnosti druhej zmluvnej strane; a/alebo

(d) pre ktorú je stanovený osobitnými predpismi osobitný režim nakladania (najmä obchodné tajomstvo, bankové tajomstvo, telekomunikačné tajomstvo, daňové tajomstvo, osobné údaje a utajované skutočnosti).

7.2 Dôvernou informáciou nie je Zmluva, vrátane jej príloh, informácie, ktoré sa bez porušenia Zmluvy stali verejne známymi, informácie získané oprávnene inak, ako od druhej Zmluvnej strany a informácie, ktoré je Objednávateľ povinný sprístupniť alebo zverejniť podľa zákona č. 211/2000 Z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (zákon o slobode informácií) v znení neskorších predpisov alebo iného osobitného predpisu.

7.3 Poskytovateľ sa zaväzuje, že v súlade s článkom 29 GDPR a so Zákonom o ochrane osobných údajov zabezpečí poverenie svojich zamestnancov a všetkých osôb, ktoré v rámci plnenia Zmluvy majú prístup na pracovisko Objednávateľa (miesto plnenia Zmluvy), ktorí pri plnení záväzkov z tejto Zmluvy môžu spracúvať osobné údaje, a to najmä s dôrazom na povinnosť mlčanlivosti (§ 79 Zákona o ochrane osobných údajov) a sankcie za porušenie povinnosti mlčanlivosti (§ 104 a nasl. Zákona o ochrane osobných údajov). Ustanovenia článku 28 GDPR týmto nie sú dotknuté.

7.4 Zmluvné strany sa zaväzujú užívať dôverné informácie druhej Zmluvnej strany výlučne na účel, na ktorý im boli poskytnuté, odovzdané, sprístupnené alebo akýmkoľvek iným spôsobom získané Zmluvnými stranami na základe Zmluvy. V prípade, že Objednávateľ poskytne Poskytovateľovi dôvernú informáciu v listinnej podobe, Poskytovateľ je povinný ju bezodkladne po pominutí účelu jej držania vrátiť Objednávateľovi.

7.5 Zmluvné strany sa zaväzujú, že dôverné informácie budú ochraňovať najmenej s rovnakou starostlivosťou ako ochraňujú vlastné dôverné informácie rovnakého druhu, vždy však najmenej v rozsahu primeranej odbornej starostlivosti, predovšetkým ich budú chrániť pred náhodným alebo neoprávneným poškodením a zničením, náhodnou stratou, zmenou alebo iným znehodnotením, nedovoleným prístupom alebo sprístupnením alebo zverejnením, pričom ak nie je v Zmluve ustanovené inak, zaväzujú sa, že bez predchádzajúceho písomného súhlasu druhej Zmluvnej strany neposkytnú, neodovzdajú, neoznámia alebo iným spôsobom nevyzradia, resp. nesprístupnia dôverné informácie druhej Zmluvnej strany tretej osobe.

7.6 Zmluvné strany sa zaväzujú, že upovedomia druhú Zmluvnú stranu o porušení povinnosti mlčanlivosti bez zbytočného odkladu po tom, ako sa o takomto porušení dozvedeli.

7.7 Povinnosť zachovávať mlčanlivosť sa nevzťahuje na prípady, ak Zmluvnej strane na základe osobitného predpisu alebo na základe rozhodnutia príslušného orgánu vznikla povinnosť sprístupniť alebo zverejniť dôvernú informáciu druhej Zmluvnej strany alebo jej časť. O vzniku takejto povinnosti sa budú Zmluvné strany vzájomne informovať bez zbytočného odkladu.

7.8 Ustanovenia jednotlivých bodov tohto článku Zmluvy ostávajú účinné aj po ukončení Zmluvy.

8 SANKCIE

8.1 Poskytovateľ sa zaväzuje, že:

(a) ak nedodrží v prevádzkových hodinách reakčnú dobu na Problém IS – kategória závažnosti kritický do termínov uvedených v Prílohe 1 Zmluvy, na výzvu Objednávateľa zaplatí Objednávateľovi zmluvnú pokutu vo výške 50 (slovom: päťdesiat) EUR za každú hodinu omeškania za všetky Problémy IS sumárne; a

(b) ak nedodrží termín poskytnutia Služby o dodaní, implementácii a službách podpory prevádzky a údržby komplexného nástroja pre Kybernetickú bezpečnosť zaplatí Objednávateľovi zmluvnú pokutu vo výške 150 (slovom: stopäťdesiat) EUR za každý kalendárny deň omeškania.

8.2 V prípade, ak sa Objednávateľ dostane do omeškania so zaplatením Ceny, Poskytovateľ je oprávnený od Objednávateľa požadovať zaplatenie úroku z omeškania vo výške 0,022 % z nezaplatenej Ceny za každý deň omeškania.

8.3 V prípade porušenia zmluvnej povinnosti Poskytovateľa vybaviť reklamáciu včas podľa článku 5 bod 5.6 Zmluvy, Objednávateľ je oprávnený požadovať od Poskytovateľa zaplatenie zmluvnej pokuty vo výške 150 (stopäťdesiat) EUR za každý deň omeškania, a to aj opakovane.

8.4 Poskytovateľ sa zaväzuje zaplatiť Objednávateľovi zmluvnú pokutu podľa tohto článku bod 8.1 alebo 8.3 Zmluvy. Zmluvné strany považujú takéto určenie zmluvnej pokuty za primerané a dostatočne určité. Zmluvnú pokutu sa zaväzuje Poskytovateľ uhradiť Objednávateľovi najneskôr do 10 (desiatich) Pracovných dní odo dňa doručenia výzvy Objednávateľa na zaplatenie zmluvnej pokuty Poskytovateľovi. Uplatnením zmluvnej pokuty nie je dotknuté právo Objednávateľa na náhradu škody.

8.5 Zmluvná strana zodpovedá za škodu, ktorú spôsobí druhej Zmluvnej strane porušením svojej povinnosti zo Zmluvy a je povinná ju nahradiť, okrem prípadov, kedy preukáže, že porušenie povinnosti bolo spôsobené okolnosťami vylučujúcimi zodpovednosť. Pri uplatnení a úhrade škôd a nákladov sa Zmluvné strany budú riadiť ustanoveniami § 373 a nasl. Obchodného zákonníka.

8.6 Objednávateľ si v prípade nároku na zaplatenie sankcie a/alebo nároku na náhradu škody môže sankciu a/alebo škodu odpočítať z akýchkoľvek čiastok splatných v prospech Poskytovateľa.

9 VYHLÁSENIA A ZÁRUKY

9.1 Poskytovateľ vyhlasuje a ubezpečuje Objednávateľa, že ku dňu podpisu Zmluvy Poskytovateľom:

(a) osoba konajúca za Poskytovateľa je v plnom rozsahu oprávnená dojednať, uzavrieť a podpísať Zmluvu a vykonávať práva a povinnosti v nej upravené;

(b) je spoločnosťou riadne založenou a existujúcou podľa právneho poriadku Slovenskej republiky, neexistuje žiaden dôvod neplatnosti spoločnosti, má všetky potrebné právomoci a oprávnenia na poskytnutie Služby, a riadne plní všetky povinnosti, porušenie ktorých by mohlo viesť k jeho zrušeniu;

(c) je zapísaný v Registri partnerov verejného sektora, pokiaľ sa naňho takáto povinnosť vzťahuje;

(d) uzatvorenie alebo plnenie Zmluvy Poskytovateľom nie je ukracujúcim alebo poškodzujúcim alebo zvýhodňujúcim alebo znevýhodňujúcim úkonom vo vzťahu k akémukoľvek svojmu veriteľovi, pričom v tejto súvislosti nie je najmä odporovateľným právnym úkonom; a

(e) nevedie sa voči nemu vyšetrovanie alebo zisťovanie zo strany štátnych alebo správnych orgánov, nevedie sa voči nemu resp. voči jeho majetku, súdny spor vrátane exekučného, daňového, konkurzného, rozhodcovského konania alebo akéhokoľvek obdobného konania a neexistujú skutočnosti, ktoré by mohli viesť k začatiu takýchto konaní proti nemu.

9.2 Poskytovateľ berie na vedomie, že ak by Objednávateľ mal v čase podpisovania Zmluvy vedomosť o tom, že ktorékoľvek z vyhlásení Poskytovateľa uvedené v tomto článku bod 9.1 Zmluvy je nepravdivé, Zmluvu by neuzatvoril, nakoľko uvedené vyhlásenia Objednávateľ považuje za skutočnosti, ktoré si vymienil.

9.3 Pokiaľ sa preukáže, že ktorékoľvek z vyhlásení Poskytovateľa uvedených v tomto článku bod 9.1 Zmluvy nebolo v čase uzatvorenia Zmluvy pravdivým, alebo v čase nasledujúcom po uzatvorení Zmluvy prestalo byť pravdivým v dôsledku konania Poskytovateľa, zaväzuje sa Poskytovateľ nahradiť škodu, ktorá vznikne Objednávateľovi v dôsledku skutočností, ktoré sú obsahom tohto vyhlásenia.

9.4 Objednávateľ vyhlasuje a ubezpečuje Poskytovateľa, že ku dňu podpisu Zmluvy Objednávateľom:

(a) má oprávnenie podpísať Zmluvu, vykonávať práva a plniť záväzky vyplývajúce pre neho zo Zmluvy;

(b) osoby konajúce za Objednávateľa sú v plnom rozsahu oprávnené dojednať, uzavrieť a podpísať Zmluvu a vykonávať práva a povinnosti v nej upravené; a

(c) je spoločnosťou riadne založenou a existujúcou podľa právneho poriadku Slovenskej republiky, neexistuje žiaden dôvod neplatnosti spoločnosti, má všetky potrebné právomoci a oprávnenia na objednanie Služby, a riadne plní všetky povinnosti, porušenie ktorých by mohlo viesť k jeho zrušeniu.

9.5 Pokiaľ nie je v Zmluve uvedené inak, akákoľvek komunikácia a iné úkony v súvislosti so Zmluvou a jej plnením, musia byť urobené v písomnej forme a doručené na adresy uvedené v záhlaví Zmluvy alebo na iné adresy alebo kontaktné osoby, ktoré si Zmluvné strany navzájom písomne oznámia.

10 KOMUNIKÁCIA

10.1 Pokiaľ nie je v Zmluve uvedené inak, akákoľvek komunikácia a iné úkony v súvislosti so Zmluvou a jej plnením, musia byť urobené v písomnej forme a doručené na adresy uvedené v záhlaví Zmluvy alebo na iné adresy alebo kontaktné osoby, ktoré si Zmluvné strany navzájom písomne oznámia.

10.2 Zmluvné strany sa dohodli, že akékoľvek oznámenie alebo iná formálna korešpondencia, pokiaľ nie je v Zmluve uvedené inak, sa budú pre účely Zmluvy považovať za doručené:

(a) v deň doručenia zásielky, ak bola zásielka doručená osobne alebo kuriérnou službou; alebo

(b) v 5. (piaty) Pracovný deň nasledujúci po dni podania zásielky na pošte, ak bola zásielka poslaná doporučenou poštou alebo v deň doručenia zásielky, podľa toho, čo nastane skôr; alebo

(c) v deň potvrdeného doručenia e-mailu, ak bol tento e-mail doručený do 15.00 hod v ktorýkoľvek Pracovný deň a v ostatných prípadoch v Pracovný deň nasledujúci po dni doručenia e-mailu, avšak s výnimkou prípadov, v ktorých bude adresátovi e-mailu doručený príslušný e-mail v čase, kedy bude mať tento adresát nastavenú automatickú odpoveď týkajúcu sa jeho neprítomnosti.

10.3 Zmeny identifikačných údajov uvedených v Zmluve, sú si Zmluvné strany povinné oznámiť do 5 (piatich) Pracovných dní od realizácie týchto zmien.

11 TRVANIE A ZÁNIK ZMLUVY

11.1 Zmluva sa uzatvára na dobu určitú, **a to** na dobu 36 (tridsaťšesť) mesiacov odo dňa účinnosti Zmluvy.

11.2 Zmluva môže byť ukončená aj skôr ako je uvedené v tomto článku bod 11.1 Zmluvy, a to jednostranným odstúpením od Zmluvy, písomnou výpoveďou, alebo písomnou dohodou Zmluvných strán.

11.3 Zmluvu môže Objednávateľ vypovedať aj bez udania dôvodu zaslaním písomnej výpovede Poskytovateľovi, pričom výpovedná lehota je 3 (tri) mesiace a začína plynúť prvým dňom mesiaca nasledujúceho po mesiaci, v ktorom bola výpoveď doručená Poskytovateľovi.

11.4 V prípade, ak dôjde k ukončeniu Zmluvy výpoveďou, pravidlá ohľadom vysporiadania plnení, ktoré neboli riadne ukončené ku dňu zániku Zmluvy, v zmysle tohto článku bodu 11.9 Zmluvy sa použijú rovnako.

11.5 Každá zo Zmluvných strán je oprávnená odstúpiť od tejto Zmluvy v prípade, ak jej takéto právo vyplýva z osobitného predpisu alebo Zmluvy, a to výlučne z dôvodov a za podmienok ustanovených v príslušnom osobitnom predpise (napr. § 19 Zákona o verejnom obstarávaní, § 15 ods. 1 zákona č. 315/2016 Z. z. o registri partnerov verejného sektora a o zmene a doplnení niektorých zákonov v znení neskorších predpisov; podstatné porušenie Zmluvy je posudzované v zmysle § 345 Obchodného zákonníka) alebo výslovne podľa kritérií uvedených nižšie v Zmluve.

11.6 Za podstatné porušenie Zmluvy Poskytovateľom sa považuje, ak je Poskytovateľ v omeškaní s plnením objednávky v zmysle článku 3 bod 3.1 Zmluvy o viac ako 3 (tri) Pracovné dni.

11.7 Objednávateľ je oprávnený odstúpiť od Zmluvy aj v prípade, ak:

(a) Poskytovateľ sa stane spoločnosťou v kríze;

(b) Poskytovateľ vstúpi do likvidácie;

(c) sa proti Poskytovateľovi začne exekučné konanie;

(d) bude nepochybné, že ani po uplynutí doby v zmysle článku 12 bodu 12.4. Zmluvy Poskytovateľ preukázateľne nie je oboznámený s IS Objednávateľa v rozsahu potrebnom na riadne a včasne poskytovanie Služieb v zmysle Zmluvy; alebo

(e) Poskytovateľ predá svoj podnik alebo časť podniku a podľa Objednávateľa sa tým zhorší vymožiteľnosť práv a povinností zo Zmluvy.

11.8 Za podstatné porušenie Zmluvy Objednávateľom sa považuje, ak je Objednávateľ v omeškaní s platením svojich peňažných záväzkov po dobu dlhšiu než 30 (tridsať) dní a Objednávateľ neuhradí svoje peňažné záväzky ani v dodatočnej primeranej lehote, ktorú mu v písomnej výzve spolu s výzvou na úhradu peňažného záväzku Poskytovateľ poskytne.

11.9 Odstúpením od Zmluvy niektorou zo Zmluvných strán sa Zmluva zrušuje ku dňu doručenia odstúpenia druhej Zmluvnej strane, pričom účinky odstúpenia sa spravujú príslušnými ustanoveniami Obchodného zákonníka. V prípade odstúpenia od Zmluvy si Zmluvné strany ponechajú doposiaľ poskytnuté plnenia, vykonané v súlade s podmienkami uvedenými v Zmluve a jej prílohách a úhrady za tieto plnenia. Ohľadom plnení, ktoré neboli riadne ukončené ku dňu zániku Zmluvy, pripraví Poskytovateľ ich inventarizáciu a Objednávateľ bude oprávnený, ale nie povinný, ich prevziať, pokiaľ uhradí príslušnú časť ceny plnenia zodpovedajúcej miere rozpracovanosti podľa dohody Zmluvných strán.

11.10 Zmluvné strany sa zároveň výslovne dohodli, že Poskytovateľ je povinný v lehotách určených Objednávateľom poskytnúť Objednávateľovi súčinnosť, ktorú bude od neho Objednávateľ opodstatnene požadovať za účelom plynulej zmeny, resp. nahradenia poskytovateľa Dodaním a implementáciou komplexného nástroja pre Kybernetickú bezpečnosť s požadovanými funkciami a Službami podpory prevádzky a údržby komplexného nástroja pre Kybernetickú bezpečnosť, a zabezpečenia kontinuálnej prevádzky a to po dobu posledných troch (3) mesiacov pred ukončením Zmluvy.

11.11 Zánik Zmluvy nemá vplyv na práva a povinnosti Zmluvných strán, ktoré vznikli počas existencie Zmluvy a podľa svojej povahy majú trvať naďalej, predovšetkým na záväzky súvisiace s bezpečnosťou a ochranou informácií, ako ani dojednania Zmluvných strán vo vzťahu k zmluvným pokutám pre prípad omeškania a/alebo neposkytnutia súčinnosti Poskytovateľom v zmysle vyššie cit. ustanovení Zmluvy.

11.12 Zmluva zaniká aj na základe písomnej dohody Zmluvných strán.

12 OSOBITNÉ DOJEDNANIA

12.1 Poskytovateľ bude poskytovať Služby podľa Zmluvy v sídle Objednávateľa alebo prostredníctvom vzdialeného prístupu, ak sa Zmluvné strany nedohodnú inak.

12.2 Objednávateľ je povinný dodať Poskytovateľovi aktuálnu dokumentáciu k IS Objednávateľa do 10 (desiatich) Pracovných dní odo dňa účinnosti Zmluvy.

12.3 V prípade ak Poskytovateľ pred uzatvorením Zmluvy predložil Objednávateľovi uzatvorenú zmluvu o poistení zodpovednosti za škodu spôsobenú podnikateľom, ktorá je uzatvorená na dobu neurčitú, je Poskytovateľ povinný na výzvu Objednávateľa predložiť mu bezodkladne aktuálne potvrdenie o zaplatení poistného alebo aktuálny poistný certifikát.

12.4 Zmluvné strany sa výslovne dohodli, že do času, kým nebude mať Objednávateľ za preukázané, resp. nebude zo skutkových okolností nepochybné, že Poskytovateľ je, resp. by už mal byť oboznámený s IS Objednávateľa v rozsahu nevyhnutnom na poskytovanie Služieb v zmysle Zmluvy, najdlhšie však po dobu 3 (troch) mesiacov odo dňa poskytnutia dokumentácie v zmysle tohto článku bodu 12.2. Zmluvy, nevzniká Objednávateľovi právo odstúpiť od Zmluvy v prípade, ak sa Poskytovateľ omešká s reakčnou dobou na Problém.

12.5 Ustanovenie tohto článku bodu 12.4. Zmluvy sa nepoužije v prípade závažného porušenia povinnosti zo strany Poskytovateľa, predovšetkým však v prípade, ak Poskytovateľ neodstraňuje problém vôbec, ako aj v prípade, ak Poskytovateľ nevynaloží všetky zdroje a všetko úsilie, ktoré je možné od neho spravodlivo požadovať, za účelom riadneho a včasného odstránenia Problému.

12.6 Ustanovenia bodov tohto článku 12.4. a 12.5. článku Zmluvy platia rovnako aj v prípade, ak sa kedykoľvek v lehote do 3 (troch) mesiacov odo dňa poskytnutia dokumentácie v zmysle tohto článku bod 12.2. Zmluvy preukáže, resp. Poskytovateľ zistí, že IS Objednávateľa nezodpovedá aktuálnym špecifikáciám funkčných a nefunkčných požiadaviek v súlade s aktuálnou dokumentáciou k IS Objednávateľa ku dňu uzatvoreniu Zmluvy.

13 ZÁVEREČNÉ USTANOVENIA

13.1 Zmluva nadobúda účinnosť dňom nasledujúcim po dni jej zverejnenia podľa § 47a Občianskeho zákonníka.

13.2 Vzťahy upravené Zmluvou, ako aj vzťahy vznikajúce zo Zmluvy sa spravujú právnym poriadkom Slovenskej republiky.

13.3 Zmluvné strany sa dohodli, že akýkoľvek spor vzniknutý na základe Zmluvy alebo v súvislosti so Zmluvou, vrátane otázok platnosti, účinnosti alebo výkladu Zmluvy bude rozhodnutý príslušným súdom v Slovenskej republike.

13.4 Práva a povinnosti zo Zmluvy prechádzajú na právnych nástupcov Zmluvných strán. Poskytovateľ môže svoje pohľadávky voči Objednávateľovi vyplývajúce zo Zmluvy postúpiť len s predchádzajúcim písomným súhlasom Objednávateľa.

13.5 Zmluvné strany sa dohodli v rozsahu, v akom to právne predpisy pripúšťajú, že vylučujú právo Poskytovateľa započítať bez súhlasu Objednávateľa akúkoľvek svoju pohľadávku voči Objednávateľovi oproti akejkoľvek pohľadávke Objednávateľa voči Poskytovateľovi.

13.6 Objednávateľ môže kedykoľvek započítať pohľadávku, ktorú má voči Poskytovateľovi proti akejkoľvek pohľadávke (bez ohľadu na to, či je v čase započítania splatná alebo nie), ktorú má Poskytovateľ voči Objednávateľovi. Ak sú započítavané pohľadávky denominované v rôznych menách, Objednávateľ je oprávnený pre účely započítania prepočítať čiastku ktorejkoľvek pohľadávky do meny druhej pohľadávky, pričom použije výmenný kurz stanovený v kurzovom lístku publikovanom Európskou centrálnou bankou.

13.7 Zmluvu možno meniť a dopĺňať ju len písomne, a to na základe dohody Zmluvných strán podpísanej Zmluvnými stranami a v súlade so Zákonom o verejnom obstarávaní.

13.8 V prípade, ak sa niektoré z ustanovení Zmluvy stane neplatným alebo nevymáhateľným, nemá takáto neplatnosť alebo nevymáhateľnosť niektorého z ustanovení Zmluvy vplyv na platnosť a vymáhateľnosť ostatných ustanovení Zmluvy. Zmluvné strany sú v takomto prípade povinné bez zbytočného odkladu uzatvoriť dodatok k Zmluve, ktorý nahradí neplatné alebo nevymáhateľné ustanovenie Zmluvy iným ustanovením, ktoré ho v právnom aj obchodnom zmysle najbližšie nahradzuje tak, aby bola vôľa Zmluvných strán vyjadrená v nahrádzaných ustanoveniach Zmluvy zachovaná.

13.9 Žiadna zo Zmluvných strán nezodpovedá za omeškanie alebo nesplnenie svojej zmluvnej povinnosti, pokiaľ dôjde k nepredvídateľnej udalosti, ktorú povinná Zmluvná strana nemôže ovplyvniť, najmä k živelnej pohrome, vojne, občianskym nepokojom, nedostatku surovín na trhu, sabotáži, štrajku, alebo inému prípadu tzv. „vyššej moci". Povinná Zmluvná strana sa zaväzuje omeškanie alebo nemožnosť plnenia zmluvnej povinnosti druhej Zmluvnej strane bezodkladne oznámiť a vyvinúť maximálne úsilie k odstráneniu takejto udalosti, pokiaľ to bude možné. Po odstránení tejto udalosti sa povinná Zmluvná strana zaväzuje vyvinúť maximálne úsilie k splneniu omeškanej zmluvnej povinnosti.

13.10 Zmluvné strany zhodne prehlasujú, (i) že si Zmluvu riadne prečítali, (ii) v plnom rozsahu porozumeli jej obsahu, ktorý je pre ne dostatočne zrozumiteľný a určitý, (iii) že táto vyjadruje ich slobodnú a vážnu vôľu bez akýchkoľvek omylov a (iv) že táto nebola uzavretá ani v tiesni, ani za nápadne nevýhodných podmienok plynúcich pre ktorúkoľvek Zmluvnú stranu, na znak čoho ju týmto vlastnoručne podpisujú.

13.11 Zmluva je vyhotovená v 3 (troch) rovnopisoch, s tým, že všetky rovnopisy majú platnosť originálu, pričom Objednávateľ dostane 2 (dva) jej rovnopisy a Poskytovateľ dostane 1 (jeden) jej rovnopis.

Prílohy:
Príloha č. 1: Parametre a podmienky poskytovania Služieb
Príloha č. 2: Cena
Príloha č. 3: Plán realizácie

Príloha č. 1
Parametre a podmienky poskytovania Služieb

Príloha č. 1 – Opis predmetu zákazky, tejto Výzvy

„Dodanie, implementácia a služby podpory prevádzky a údržby Kyberbezpečnostných systémov Endpoint Protection Platform (EPP) a Endpoint Detection and Response (EDR) vrátane dohľadových služieb 24/7 s kontrolou incidentov z prostredí objednávateľskej organizácie, poskytované výrobcom riešenia, s priamym riešením a uzatváraním týchto incidentov a s analýzou prvotnej príčiny incidentov. _CP22/2024"

Opis predmetu zákazky

Úvod:

Predmetom zákazky je **„Dodanie, implementácia a služby podpory prevádzky a údržby Kyberbezpečnostných systémov Endpoint Protection Platform (EPP) a Endpoint Detection and Response (EDR) vrátane dohľadových služieb 24/7 s kontrolou incidentov z prostredí objednávateľskej organizácie, poskytované výrobcom riešenia, s priamym riešením a uzatváraním týchto incidentov a s analýzou prvotnej príčiny incidentov.** " ktorého cieľom je ochrana počítačovej siete, koncových zariadení, informačných aktív a naplnenie požiadaviek legislatívy na riešenie kybernetických bezpečnostných incidentov a opatrení pre oblasť ochrany, monitorovania, testovania bezpečnosti, riešenia a analýzy incidentov a bezpečnostných auditov /ďalej ako EPPEDR/ , 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:

Dodanie a implementáciu komplexného nástroja pre EPPEDR s požadovanými funkciami a službami vrátane podpory prevádzky a údržby dodaného komplexného nástroja EPPEDR pre zaistenie spoľahlivej, kontinuálnej a bezpečnej prevádzky v súlade s dokumentáciou systému a aktuálnymi požiadavkami Objednávateľa, vrátane riešenia Problémov a Incidentov

1. Kapacitné požiadavky na komplexný systém

Definovanie vstupných zdrojov verejného obstarávateľa

Lokalít	Počet AD užívateľov	Počet AD administrátorov	Počet serverov (virtualizačné + virtuálne) a počet fyzických serverov	Počet pracovných staníc
12	560	5	60	500

Počet koncových zariadení pre implementáciu komplexného nástroja EPPEDR s riešením problémov a incidentov je **560.** To sú zariadenia na ktorých bude EPPEDR nainštalovaný a prevádzkovaný a na ktorých budú riešený dohľad, problémy a incidenty **24/7 na obdobie 36 mesiacov** .

2. Špecifikácia požadovaných služieb

2.1. Dodanie a implementáciu komplexného nástroja EPPEDR s požadovanými funkciami, ktorými sú

Singularity Platform. Access to the Singularity Platform, includes initial XDR Ingest
Complete Protection Platform (Per Workstation). EPP + EDR, with NGAV (AI), Rogues IoT, Firewall Control, Device Control, Remote Shell, EDR Hunting and Investigation and up to 100 concurrent STAR Rules, Standard Support Plan
Complete Cloud Workload Security (Per Server). EPP + EDR, with NGAV (AI), Rogues IoT, Firewall Control, Device Control, Remote Shell, EDR Hunting and Investigation and up to 100 concurrent STAR Rules, Standard Support Plan
Ranger Attack Surface Management Platform (per Endpoint). Enterprise-wide Discovery of IT/IoT, Attack Surface Reduction, Peer-to-Peer Deployment Capability for SentinelOne Agents
Singularity Ranger AD (Per User). Cloud-based enterprise wide active directory and Azure AD Assessment and real time attack detection
Vigilance Respond Pro (Per Endpoint). Vigilance Respond Pro: 24x7 MDR, and incident response

Pre realizáciu činností

Endpoint Protection Platform (EPP) a Endpoint Detection and Response (EDR) vrátane dohľadových služieb 24/7 s kontrolou incidentov z prostredí objednávateľskej organizácie, poskytované výrobcom riešenia, s priamym riešením a uzatváraním týchto incidentov a s analýzou prvotnej príčiny incidentov spolu so softvérovými licenciami pre Komplexný nástroj alebo predplatenými službami na poskytovanie Komplexného nástroja na obdobie **36 mesiacov** pre **560** koncových staníc z ktorých je **60** serverov.

2.1.1. Funkčné požiadavky na EPPEDR

The proposed solution must identify rogue devices discovery capability to reduce the potential attack surface.	Navrhované riešenie musí mať schopnosť identifikovať neautorizované zariadenia na redukciu bodov, ktoré by mohli byť využité na potencionálny útok.
The proposed solution must provide a software/application inventory for the environment	Navrhované riešenie musí poskytovať inventár softvéru/aplikácií pre prostredie.
	Navrhované riešenie musí umožňovat inštaláciu agentov metódou Peer-to-Peer
Dashboards & Reporting	Dashboards & Reporting
The proposed solution should report all known vulnerabilities in programs installed on an endpoint, along with export option	Navrhované riešenie musí hlásiť všetky známe zraniteľnosti v programoch nainštalovaných na koncovom bode, spolu s možnosťou exportu dát.
The proposed solution have option to export data into 3rd party reporting tools such as Tableau or PowerBI	Navrhované riešenie musí mať možnosť exportovať dáta do nástrojov na správu dát tretích strán, ako sú Tableau alebo PowerBI.
The proposed solution must have customizable dashboards as per user	Navrhované riešenie musí mať možnosť prispôsobiteľných informačných panelov podľa požiadaviek používateľa.
Compliance	Compliance
	Výrobca navrhovaného riešenia musí byť zaradený podľa nezávislého a medzinárodne uznávaného hodnotenia jednotlivých bezpečnostných produktov spoločností Gartner, Inc., Magic Quadrant for Endpoint Protection Platforms do kategórie „Leaders", minimálne posledné dva roky.
The proposed solution must be fulfilling following compliances such as HIPAA compliant ,PCI compliant,GDPR compliant,ISO27001 compliant	Navrhované riešenie musí spĺňať súladové požiadavky, ako sú súlad s HIPAA, súlad s PCI, súlad s GDPR. SaaS platforma výrobcu musí byť certifikovaná podľa SOC 2 Type II.
Integrations	Integrácia
The proposed solution should support integration with Active Directory	Navrhované riešenie musí podporovať integráciu s Active Directory.
The proposed solution should have integrations to Virus Total or similar tools	Navrhované riešenie musí mať integrácie s nástrojmi ako Virus Total alebo podobnými.
The proposed solution should have native integrations/integrations with SIEM solutions such as Splunk, Qradar & etc.	Navrhované riešenie musí mať natívne integrácie alebo integrácie so SIEM riešeniami ako Splunk, Rapid 7, Qradar a podobnými.
The proposed solution should have option to send event logs via Syslog.	Navrhované riešenie musí mať možnosť odoslať udalostné protokoly cez protokol Syslog.
	Bezpečnost Active Directory
	Riešenie musí vykonávať testy na detekciu zraniteľností Active Directory spojených s autentifikáciou, autorizáciou, nastavením účtu, certifikačnými službami, oprávneniami/delegáciami a bezpečnostnými problémami priamo súvisiacimi so zabezpečením Domain Controller(ov) a Azure AD.
	Riešenie musí kategorizovať testy do najmenej štyroch závažností od najkritickejších po najnižšiu
	Riešenie musí byť schopné príjmať oznámenia z on-premise AD (provozné udalosti) v reálnom čase.
	Riešenie nesmie vyžadovať plné administrátorské oprávnenia na Active Directory alebo Domain Controlleroch.
	Riešenie musí obsahovať bezpečnostné hodnotenia pre on-premise a Azure AD.
	Riešenie musí mať možnosť nasadenia on-premise.
	Overenia on-prem AD musia byť vykonávané jediným zariadením pripojeným k doméne.
	Riešenie nesmie vyžadovať VPN pripojenie medzi on-prem komponentmi a cloudovou konzolou.

	Riešenie musí byť schopné automaticky objaviť viaceré domény a zahrnúť ich do rozsahu testov a ochrany.
	Riešenie musí byť schopné vykonávať overenia Azure-AD prostredníctvom API poskytovaného spoločnosťou Microsoft.
• The solution must be able to detect attacks against the AD, including: o 'Low and slow' brute force attempts like 'Password Spray' o Mass account lockouts o Mass Password changes o Mass account disabling/deletion o Suspicious password changes for sensitive accounts o Reactivation of disabled privileged accounts o DCSync attacks o Rouge Domain Controller attacks (DCShadow) o Use of the default "Administrator" account o Suspicious service creation on Domain Controller(s)	Riešenie musí byť schopné detegovať útoky voči Active Directory, vrátane: Low and slow pokusy o hrubú silu, ako je Password Spray, Hromadné uzamknutie účtov, Hromadná zmena hesiel, Hromadné vypnutie/zmazanie účtov, Podozrivé zmeny hesiel pre citlivé účty, Znovuaktivácia deaktivovaných privilegovaných účtov, Útoky DCSync, Útoky na rouge Domain Controller (DCShadow), Použitie default účtu Administrator, Podozrivé vytváranie služieb na Domain Controller(och).
• Threat detection must not rely on scheduled AD replication to minimize impact on the AD.	Detekcia hrozieb nesmie spočívať v plánovanom replikovaní AD, aby sa minimalizovalo zaťaženie na AD
	Riešenie musí umožnovať externé spracovanie detekcie hrozieb do riešení SIEM, SOAR a XDR
	Riešenie musí poskytovať podrobné usmernenia na odstránenie zistených zraniteľností, vrátane Odkazy na taktiky a techniky MITRE Att&ack, Kroky na prípravu remediacie, Kroky na vykonanie remediacie, Odkazy na doplnkové informácie od širšej komunity pre zabezpečenie AD.
	Riešenie musí byť schopné generovať skripty na remediaciu, ktoré možno vykonať v príslušných doménach s nasledujúcimi schopnosťami: Podrobný výber zraniteľností na odstránenie, Podrobný výber objektov, na ktorých sa bude remediacia vykonávať, História remediacie o stave procesu remediacie (vygenerovaný skript, stiahnutý, vykonaný s výsledkom úspechu alebo zlyhania), Skripty na vrátenie zmien pri bývalej remediacii na základe skriptu.
	Riešenie musí byť schopné automaticky spúšťať celý testovací cyklus v konfigurovateľnom rozvrhu používateľa (napr. každých X dní), pridať výsledky do svojej databázy a generovať podrobné testovacie správy bez ďalšieho zásahu používateľa.
	Riešenie musí podporovať ad-hoc spustenia celého testovacieho cyklu a prezentovať výsledky v GUI a v podrobných správach.
	Riešenie musí podporovať spustenie individuálnych testov ad-hoc, bez potreby spúšťať celý testovací cyklus.
	Systém musí podporovať vytváranie a dokumentovanie výnimiek pre budúce testovacie behy na nasledujúcich úrovniach: Domény, Jednotlivé testy pre doménu, Jednotlivé objekty (užívateľ alebo skupina) pre test a doménu.
	Riešenie musí podporovať vytváranie týchto výnimiek na centrálnej lokalite v GUI alebo priamo z príslušných testov/výsledkov s možnosťou pridávania komentárov k tomu, prečo boli tieto výnimky vytvorené.

	Riešenie musí obsahovať informačný panel, ktorý poskytuje rýchle informácie o výsledkoch testov, ako sú: Počet testov podľa závažnosti a ich výsledky (úspech/zlyhanie/skipované) celkom a pre testované domény, Zistená topológia domény a vzťahy medzi doménami, Skóre zdravia a priradená úroveň rizika celkovo a individuálne pre jednotlivé domény, Najkritickejšie/závažné zistenia a počet ovplyvnených objektov, Grafická reprezentácia zlyhaných testov v posledných behoch, ktorá umožňuje používateľovi rýchlo vidieť zmeny v zabezpečení v čase.
• The solution must provide extensive filtering capabilities of test results including at least: o Previous tests o Severity o Domain name o Forest name o Detection name o Acknowledgement status o Vulnerability status o Computer(s) affected o Group(s) affected o User(s) affected	Riešenie musí poskytovať rozsiahle možnosti filtrovania výsledkov testov, vrátane aspoň: Predchádzajúce testy, Závažnosť, Názov domény, Názov forest, Názov zistenia, Stav potvrdenia, Stav zraniteľnosti, Počítač(y) ovplyvnené/postihnute, Skupina(y) ovplyvnená/postihnuta, Užívateľ(ia) ovplyvnení/postihnuty.
	Riešenie musí byť schopné porovnávať výsledky testov s predchádzajúcimi .
	Riešenie musí poskytovať minimálne nasledujúce podrobnosti o každom vykonanom teste: Popis testu, Odkaz na relevantné webové stránky MITRE Att&ck, Mitigačné kroky, Nástroje na útok, ktoré môžu využívať zistenú zraniteľnosť, Odkazy na relevantné články od komunity pre zabezpečenie AD.
	Riešenie musí poskytovať podrobné informácie o dôvodoch zistenia zraniteľností, vrátane: Typy objektov, napr. Užívateľ alebo Skupina, Názvy objektov, Porušené nastavenia na úrovni objektu, napr. aké oprávnenia boli zistené.
	Služby a podpora
	Súčasťou riešenia musia byť dohľadové služby MDR - Managed Detection and Response, kontrola incidentov z prostredí zákazníka poskytované výrobcom riešenia.
	Výrobca musí poskytovať aj voliteľnú možnosť priameho riešenia a uzatvárania týchto incidentov MDR týmom.
	V rámci služby musí byť k dispozícii analýza prvotnej príčiny incidentu dostupná na vyžiadanie.
	Služba musí byť poskytovaná v režime 24x7
	Súčasťou služby musí byť ročný balík konzultačných hodín, ktorý zákazník môže použiť podľa potreby na podrobné vyšetrovanie, alebo proaktívné služby spojené s bezpečnosťou.

Alebo ekvivalentné riešenie.

2.1.2 Implementácia komplexného EPPEDR nástroja v rozsahu

- nastavenie a konfigurácia prostredí verejného obstarávateľa,
  - konfigurácia Windows systémov
  - overenie funkčných a výkonových parametrov Windows agentov,
  - konfigurácia Linux systémov
  - overenie funkčných a výkonových parametrov Linux agentov,
  - predvedenie vytvorenia a uloženia vlastného dashboardu a reportu,
  - predvedenie vytvorenia a uloženia užívateľsky definovaného parseru,
  - konfigurácia cloudovej služby
- 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,

3. **Služby podpory prevádzky a údržby dodaného komplexného nástroja pre EPPEDR**

- post-implementačná podpora v rozsahu **10 človekodeň na obdobie 36 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

4. **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: support@airo.sk, v prípade nedostupnosti e-mailom na +421 905 634 205. 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.

2) 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.
3) 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.
4) Oprávnená osoba Objednávateľa po vykonaní služieb pracovníkom Poskytovateľa v priestoroch Objednávateľa alebo na diaľku vzdialeným pripojením, potvrdí poskytnutie služby a funkčnosť riešenia v Helpdesku.
5) 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.

4.1 Služby podpory prevádzky a údržby dodaného komplexného nástroja softvéru

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

4.1.1. 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

4.1.2. 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.

4.1.3. 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,
- o vykonaných Službách podpory aplikačného programového vybavenia a systémového softvéru evidovaných v Helpdesku uzatvorených v danom mesiaci.

– Špecifikácia požiadaviek a vlastností komplexného nástroja

o Funkčné požiadavky systému pre EPPERP:

Číslo.	Management Console	Manažment	Konkrétne a zrozumiteľne popíšte akým

			spôsobom napĺňate uvedenú požadovanú funkcionalitu.
1	The proposed solution should support either saas based platform or on-premises deployment (Solution should have management infrastructure, operational monitoring, upgrades, reporting, notifications & 24x7 support.)	Navrhované riešenie musí podporovať platformu založenú na službe SaaS (Software as a Service) alebo lokálne nasadenie (on-premises). (Riešenie musí mať riadiacu infraštruktúru, operačný monitoring, aktualizácie, správy, oznámenia a podporu 24x7.)	áno
2		Navrhované riešenie musí poskytovať všetky funkcie, nástroje a strojové informácie v rámci jednej konzoly.	áno
3	The proposed solution should provide a web-based console and should allow administrators to access the management interface from any machine, without installing additional software Unified Web-based console for all functionalities	Navrhované riešenie musí poskytovať webovú konzolu a umožňovať administrátorom prístup k riadiacemu rozhraniu z akéhokoľvek počítača, bez potreby inštalácie dodatočného softvéru. Jednotná webová konzola pre všetky funkcie.	áno
4	The proposed solution should support multi-site configuration and multi-tenancy without any additional cost.	Navrhované riešenie musí podporovať konfiguráciu viacerých lokalít a multi-tenancy bez dodatočných nákladov.	áno
5	The proposed solution should have Policy inheritance from Top to bottom (like parent/child, group/sub-group, site/group, etc) with the ability to inheritance if needed and should also provide the flexibility to have individual policies for every group.	Navrhované riešenie musí umožňovať dedičnosť politík z hora na dol (nadradený/podradený, skupina/podskupina, lokalita/skupina atď.) s možnosťou dedičnosti, ak je to potrebné, a malo by tiež ponúkať flexibilitu, aby bolo možné mať individuálne politiky pre každú skupinu.	áno
6	The proposed solution should have Integrated KB/documentation into the management console without requiring logging in to another system / URL.	Navrhované riešenie musí mať integrovanú znalostnú bázu/dokumentáciu do riadiacej konzoly bez potreby prihlásenia sa do iného systému/URL.	áno
7	The proposed solution console should be easy to understand and navigate with simple work flows. The console's focus should be on incident response workflows vs feature configuration and management	Navrhovaná konzola musí byť jednoducho pochopiteľná a ľahko sa ňou navigovať s jednoduchými pracovnými postupmi. Konzola by sa mala sústrediť na pracovné postupy reakcie na incidenty a nie na konfiguráciu a riadenie funkcií.	áno
8	The proposed solution should have support role based access control (RBAC)	Navrhované riešenie musí mať podporu pre riadenie prístupu na základe rolí (RBAC).	áno
9	The proposed solution should support two factor or single sign on solutions for the management console and sensitive functions such as remote shell.	Navrhované riešenie musí podporovať dvojfaktorovú autentifikáciu alebo jednorazové prihlásenie pre riadiacu konzolu a citlivé funkcie, ako je vzdialený prístup cez shell.	áno
10	The proposed solution should have capability of centralized auditing and logging of activity should be maintained in the management console.	Navrhované riešenie musí mať schopnosť centralizovaného auditovania a udržiavať záznamy o aktivitách v riadiacej konzole.	áno
11	The proposed solution should have capability logged and audited the management activity ,with the ability to send logs to an external source (like SIEM etc.)	Navrhované riešenie musí mať schopnosť zaznamenávať a auditovať riadiace aktivity, s možnosťou odosielania záznamov do externého zdroja (ako SIEM atď.).	áno
	Operating System Support	**Podpora operačných systémov**	

12	The proposed solution should have support the following versions of windows Windows Server Core 2012, 2016, 2019 & 2022 Windows Server 2022, 2019, 2016, 2012 R2, 2012, 2008 R2 SP1 Windows Storage Server 2016, 2012 R2, 2012 Windows 7 SP1, 8, 8.1, 10, 11	Navrhované riešenie musí podporovať nasledujúce verzie systému Windows: Windows Server Core 2012, 2016, 2019 a 2022 Windows Server 2022, 2019, 2016, 2012 R2, 2012, 2008 R2 SP1 Windows Storage Server 2016, 2012 R2, 2012 Windows 7 SP1, 8, 8.1, 10, 11	áno
13	The proposed solution should have support the following virtual environments Citrix XenApp Citrix XenDesktop Microsoft Hyper-V Oracle VirtualBox VMware Fusion VMware Horizon VMware vSphere VMware Workstation	Navrhované riešenie musí podporovať nasledujúce virtuálne prostredia: Citrix XenApp Citrix XenDesktop Microsoft Hyper-V Oracle VirtualBox VMware Fusion VMware Horizon VMware vSphere VMware Workstation	áno
14	The proposed solution should have support the following macOS macOS Catalina macOS Big Sur macOS Monterey macOS Ventura	Navrhované riešenie musí podporovať prinajmenším nasledujúce verzie systému macOS: macOS Monterey macOS Ventura macOS Sonoma	áno
15	The proposed solution should have support the following the following (add if any other Linux platforms are supported) Amazon CentOS Debian Fedora Oracle Red Hat Enterprise Linux (RHEL) SUSE Linux Enterprise Server Ubuntu Virtuozzo	Navrhované riešenie musí podporovať nasledujúce platformy Linux: Amazon CentOS Debian Fedora Oracle Red Hat Enterprise Linux (RHEL) SUSE Linux Enterprise Server Ubuntu Virtuozzo	áno
16	The proposed solution should support native cloud deployments, AWS, Azure, Google Cloud etc.	Navrhované riešenie musí podporovať nasadzovanie v native cloud prostrediach, ako sú AWS, Azure, Google Cloud atď.	áno
17	The proposed solution should support cloud workloads protection (Azure, AWS and Google Cloud).	Navrhované riešenie musí podporovať ochranu cloudových pracovných workloadov (Azure, AWS a Google Cloud).	áno
18	The proposed solution vendor must provide support for the latest major OS Updates/Versions within 60 days of release.	Poskytovateľ navrhovaného riešenia musí zabezpečiť podporu pre najnovšie hlavné aktualizácie/verzie operačných systémov do 60 dní od ich uvedenia na trh.	áno
	Agent	**Agent**	
19	The proposed solution must have EPP and EDR capabilities available in a single agent without requiring multiple software packages to be installed.	Navrhované riešenie musí mať funkcie EPP (Endpoint Protection Platform) a EDR (Endpoint Detection and Response) dostupné v jednom agentovi bez potreby inštalovať viacero softvérových balíkov.	áno
20	The proposed solution agent size should be less then 100 MB.	Veľkosť inštalačného balíka agenta navrhovaného riešenia musi byť menšia ako 100 MB.	áno
21	The proposed solution must have strong anti-tamper capabilities (Ensure that an end user (even with local admin credentials) can not remove, disable or modify the product in any way.)	Navrhované riešenie musí mať silné schopnosti proti zasahovaniu (zabezpečiť, že koncový používateľ (aj s miestnymi správcovskými oprávneniami) nemôže produkt odstrániť, zakázať alebo akýmkoľvek spôsobom upravovať).	áno

22	The proposed solution must have ability to kick off On-Demand Scans to look for malware, or ensure a threat has been remediated (from console and/or endpoint)	Navrhované riešenie musí mať schopnosť spustiť skenery na požiadanie na vyhľadávanie malvéru alebo na zabezpečenie, že hrozba bola odstránená (z konzoly a/alebo koncového bodu).	áno
23	The proposed solution should be signtureless (No need of daily signature updates) to detect all types of Malware without compromising the security posture.	Navrhované riešenie by malo byť bez signatúr (bez potreby denných aktualizácií signatúr) pre detekciu všetkých typov malvérov bez ohrozenia bezpečnostnej pozície.	áno
24	The proposed solution must have ability to schedule agent upgrades from the management console	Navrhované riešenie musí mať schopnosť plánovať aktualizácie agenta z riadiacej konzoly.	áno
25	The proposed solution must have ability to limit the amount of agents that can download an update at any given point of time.	Navrhované riešenie musí mať schopnosť obmedziť množstvo agentov, ktoré môžu sťahovať aktualizácie v akomkoľvek danom čase.	áno
26	The proposed solution must have Ability to upgrade agents with no impact to the end user	Navrhované riešenie musí mať schopnosť aktualizovať agentov bez vplyvu na koncového používateľa.	áno
27	The proposed solution should not stop functioning if license count is exceeded.	Navrhované riešenie nesmie prerušiť svoju činnosť v prípade prekročenia počtu licencií.	áno
28	The proposed solution should automatically remove old agents from console, if agent haven't communicated to the management console for a configurable period of time	Navrhované riešenie musí automaticky odstraňovať starých agentov z konzoly, ak sa agent neprihlásil do riadiacej konzoly po konfigurovateľnom období.	áno
29	The proposed solution should have minimal impact on system performance.	Navrhované riešenie by malo mať minimálny vplyv na výkonnosť systému	áno
30	The proposed solution should must have capability to uninstalled agents remotely from the management console directly or through script.	Navrhované riešenie musí mať schopnosť odinštalovať agentov vzdialene z konzoly priamo alebo cez skript.	áno
31	The proposed solution should capability to temporarily disabled via the management console for temporary troubleshooting or testing.	Navrhované riešenie musí mať schopnosť dočasne zakázať agenta cez riadiacu konzolu na dočasné ladenie alebo testovanie.	áno
32	The proposed solution agents should have ability to communicate with Management Console via a proxy	Agenti navrhovaného riešenia musia mať schopnosť komunikovať s riadiacou konzolou cez proxy.	áno
33	The proposed solution must support linux agent running solely in user space to avoid kernel panics and tainted kernels that invalidate support	Navrhované riešenie musí podporovať linuxových agentov, ktorí bežia výhradne v užívateľskom priestore, aby sa zabránilo nestabilite a problémom s verziami kernelu.	áno
34	The proposed solution should not required any downtime while installing/upgrading Linux agents	Navrhované riešenie nesmie vyžadovať žiadny výpadok počas inštalácie/aktualizácie linuxových agentov.	áno
35	The proposed solution should provide ability to send notification messages to the end user computer.	Navrhované riešenie musí poskytovať možnosť posielať oznámenia používateľom počítača.	áno
	Threat Prevention	**Threat Prevention**	
36	The proposed solution should provide prevention capability across all major Operating Systems – Windows, MacOS & Linux.	Navrhované riešenie musí poskytovať schopnosť prevencie na všetkých hlavných operačných systémoch - Windows, MacOS a Linux.	áno
37	The proposed solution must provide protection against known and unknown malware	Navrhované riešenie musí poskytovať ochranu pred známym a neznámym malvérom.	áno
38	The proposed solution must have capability to checked the files for any infection for both on write and execute.	Navrhované riešenie musí mať schopnosť kontroly súborov na prítomnosť infekcie pri zápise aj pri vykonávaní.	áno
39	The proposed solution must be effective against Zero-Day Attacks by Analysing	Navrhované riešenie musí byť efektívne proti útokom typu Zero-Day tým, že analyzuje	áno

	Behaviours on an endpoint, rather than only looking at daily signatures	správanie na koncovom bode, namiesto toho, aby sa iba pozeralo na denné signatúry.	
40	The proposed solution must protect the endpoint against malware, even when the system is not connected to the network. The agent needs to be fully autonomous meaning it does not need to have any dependency on Management Server or Cloud or ANY resources external from the Agent to detect and respond appropriately to sophisticated threats (Zero Day, File-less , Memory based, Zero Day exploits, Ransomware, Miners, Lateral movement, APT) in real time as the threats are detected.	Navrhované riešenie musí chrániť koncový bod pred malvérom aj v prípade, keď nie je pripojený k sieti. Agent musí byť plne autonómny, čo znamená, že nepotrebuje žiadnu závislosť na riadiacom serveri, cloude ani žiadnych externých prostriedkoch na detekciu a adekvátnu reakciu na sofistikované hrozby (Zero Day, bezsúborové, založené na pamäti, Zero Day útoky, vydieračský softvér, ťažiari, laterálne pohyby, APT) v reálnom čase pri ich detekcii.	áno
41	The proposed solution should have capacity to detect dormant threats	Navrhované riešenie musí mať kapacitu na detekciu neaktívnych hrozieb.	áno
42	The proposed solution should leverage Artificial Intelligence or Machine Learning to analyse files pre-execution & behaviours while a file is running	Navrhované riešenie musí využívať umelú inteligenciu alebo strojové učenie na analýzu súborov pred ich vykonaním a na správanie súborov počas ich behu.	áno
43	The proposed solution should protect from malicious scripts and documents	Navrhované riešenie musí chrániť pred škodlivými skriptami a dokumentami.	áno
44	The proposed solution should monitor and protect from lateral movement	Navrhované riešenie musí monitorovať a chrániť pred laterálnym pohybom.	áno
45	The proposed solution should monitor and protect from exploits and fileless attacks	Navrhované riešenie musí monitorovať a chrániť pred útokmi a bezsúborovými útokmi (fileless attacks).	áno
46	The proposed solution should look for potentially unwanted programs	Navrhované riešenie musí vyhľadávať potenciálne nežiaduce programy.	áno
47	The proposed solution should monitor and protect from insider threats	Navrhované riešenie musí monitorovať a chrániť pred hrozbami od vnútorných útočníkov.	áno
48	The proposed solution should provide the flexibility to safely download of malicious or convicted file from the management console	Navrhované riešenie musí poskytovať flexibilitu pre bezpečné stiahnutie škodlivého súboru alebo súboru označeného ako hrozba z manažment konzoly.	áno
49	The proposed solution must have ability to store the malicious/alert data for at least 365 days without any additional charge	Navrhované riešenie musí mať schopnosť uchovávať dáta o zistených malvéroch a upozorneniach aspoň 365 dní bez ďalších poplatkov.	áno
50	The proposed solution must have ability to correlate together automatically if incident elated to the same attack and not create separate alerts.	Navrhované riešenie musí mať schopnosť automaticky korelovať incidenty, ak súvisia s tým istým útokom, a nemá vytvárať samostatné upozornenia.	áno
51	The proposed solution must have ability to store raw data / telemetry s for a minimum of 180 days	Navrhované riešenie musí mať schopnosť uchovávať surové dáta / telemetriu aspoň 180 dní.	áno
	EDR/Forensic Functionality	**EDR/Forenzná funkcionalita**	
52	The proposed solution must have ability to store EDR data centrally for hunting and forensic purposes .	Navrhované riešenie musí mať schopnosť uchovávať EDR dáta centrálne na účely vyhľadávania a forenzného vyšetrovania.	áno
53	The proposed solution must provide EDR telemetry data for Windows, Mac & Linux	Navrhované riešenie musí poskytovať EDR telemetrické dáta pre systémy Windows, Mac a Linux.	áno
54	The proposed solution should provide the flexibility for the data should be searched even if the originating system is offline or has been removed from console.	Navrhované riešenie musí poskytovať flexibilitu pre vyhľadávanie dát, aj keď pôvodný systém je offline alebo bol odstránený z konzoly.	áno
55	The proposed solution should support threat hunting workflows.	Navrhované riešenie musí podporovať pracovné postupy hľadania hrozieb.	áno

56	The proposed solution must have Threat hunting queries configurability as custom rules to automatically trigger detections.	Navrhované riešenie musí mať možnosť konfigurovateľných hľadacích dotazov pre hľadanie hrozieb a automatické spúšťanie detekcií ako vlastné pravidlá. Navrhované riešenie musí mať možnosť vytvárania vlastných pravidiel pomocou dotazov, ktoré budú automaticky detegovať hrozby.	áno
57	The proposed solution should by default group all related alerts together	Navrhované riešenie musí predvolene zoskupovať všetky súvisiace upozornenia dohromady.	áno
58	The proposed solution should provide a visual process tree browser	Navrhované riešenie musí poskytovať vizuálny prehliadač stromu procesov.	áno
59	The proposed solution should provide the flexibility to mark an entire group of events as a threat and take response or remediation actions accordingly	Navrhované riešenie musí umožniť označiť celú skupinu udalostí ako hrozbu a podniknúť následné kroky na odstránenie alebo riešenie.	áno
60	The proposed solution should provide the option to mark discovered items as suspicious or threats during threat hunting.	Navrhované riešenie musí ponúkať možnosť označiť objavené položky ako podozrivé alebo hrozby počas vyhľadávania hrozieb.	áno
61	The proposed solution should have option to search for MITRE ATT&CK Indicator for instances of Initial Access, Execution, Persistence, etc. in a single search string	Navrhované riešenie musí mať možnosť vyhľadávať MITRE ATT&CK Indikátory pre prípady Initial Access, Execution, Persistence atď. v jednom vyhľadávacom reťazci.	áno
62	The proposed solution should have option to search for MITRE ATT&CK Indicators based onInitial AccessCredential AccessDiscoveryLateral MovementCollectionCommand & ControlExfiltrationImpactIndicators	Navrhované riešenie musí mať možnosť vyhľadávania MITRE ATT&CK Indikátorov na základe: Initial Access Credential Access Discovery Lateral Movement Collection Command & Control Exfiltration Impact Indicators	áno
63	The proposed solution should have search capabilities for the following (add if any more search capabilities available): Hostnames Operating System File name Date creation Date modified Hash (MD5,SHA1,SHA256) Registry Information File path URL IP address Port traffic and or Traffic source	Navrhované riešenie musí mať schopnosť vyhľadávania pre nasledujúce: Hostname (názov hostiteľa) Operačný systém Názov súboru Dátum vytvorenia Dátum úpravy Hash (MD5, SHA1, SHA256) Informácie o registri Cesta k súboru URL (internetová adresa) IP adresa Port prenosu a/zdroj prenosu	áno
	Response & Remediation Capabilities	**Reakcia a funkcie remediácie**	
64	Solution should support a full remote shell for all OS (Windows, Linux & Mac) and not limit or restrict to set of commands.	Riešenie musí podporovať plný remote shell pre všetky operačné systémy (Windows, Linux a Mac) a nesmie obmedzovať alebo zakazovať dostupné príkazy	áno
65	The proposed solution should track all remote shell commands and logged during a remote shell session	Navrhované riešenie musí sledovať všetky príkazy remote shellu a zaznamenávať ich počas relácie.	áno
66	The proposed solution should alert on both suspicious and malicious threat behaviour	Navrhované riešenie musí vydávať upozornenia na podozrivé aj malvérové správanie.	áno
67	The proposed solution should have ability to kill and quarantine an offending process	Navrhované riešenie musí mať schopnosť ukončiť a izolovať proces, ktorý predstavuje hrozbu.	áno

68	The proposed solution should able to unquarantine a file from the management interface or API	Navrhované riešenie musí byť schopné zrušiť izoláciu súboru z rozhrania riadenia alebo cez API.	áno
69	The proposed solution should have ability to remediate all operating system changes and perform corrective action in machine speed. Tool should also be able to undo any system level changes related to the attack such as Registry edits, configuration changes etc.	Navrhované riešenie musí mať schopnosť odstrániť všetky zmeny v operačnom systéme a vykonávať korekčné opatrenia v rýchlosti stroja. Nástroj musí byť schopný vrátiť všetky úpravy na úrovni systému týkajúce sa útoku, ako sú úpravy registra, zmeny konfigurácie atď.	áno
70	The proposed solution should reverse destructive data event including but not limited to ransomware,The tool should also recover files that were deleted or encrypted as part of an attack and restore files to their pre-attack state	Navrhované riešenie musí byť schopné obnoviť znehodnotené dáta vrátane, ale nie obmedzené na, ransomware. Nástroj musí tiež byť schopný obnoviť súbory, ktoré boli vymazané alebo zašifrované ako súčasť útoku, a obnoviť súbory do ich stavu pred útokom.	áno
71	The proposed solution should provide option to network quarantine a device and provide flexibility to configure the same.	Navrhované riešenie musí poskytovať možnosť izolovať zariadenie v sieti a umožniť prispôsobiť konfiguráciu tejto izolácie.	áno
72	The proposed solution should have automated threat response capabilities.	Navrhované riešenie musí mať automatizované schopnosti na reakciu na hrozby.	áno
73	The proposed solution should have capability to take the remediation actions on multiple systems or events at once	Navrhované riešenie musí mať schopnosť vykonávať remediačné kroky na viacerých systémoch alebo udalostiach naraz.	áno
74	The proposed solution should have ability for an analyst to add notes/comments to an event	Navrhované riešenie musí umožňovať analytikovi pridávať poznámky/komentáre k udalosti.	áno
75	The proposed solution should have options to set the status of an issue or event (i.e. resolved, in progress, unresolved)	Navrhované riešenie musí mať možnosť nastaviť stav problému alebo udalosti (napr. vyriešené, v riešení, neriešené)	áno
	Policy & Installation	**Politiky a inštalácia**	
76	The proposed solution should provide ability to support policy inheritance across the endpoints.	Navrhované riešenie by malo poskytovať možnosť podpory dedenia politík na koncových bodoch.	áno
77	The proposed solution should have the option to provide dynamic policy assignment based on device attributes	Navrhované riešenie musí mať možnosť poskytovať dynamické priradenie politík na základe vlastností zariadenia.	áno
78	The proposed solution should cappabilty to placed the installed devices directly into a specific device group at time of installation	Navrhované riešenie musí byť schopné umiestňovať inštalované zariadenia priamo do špecifických skupín zariadení v čase inštalácie.	áno
79	The proposed solution policy context should provide the option to turn ON or OFF unique engines or by Type of engine (Pre-Execution and Run-Time Engines).	Politiky navrhovaného riešenia musia poskytovať možnosť zapnúť alebo vypnúť jedinečné moduly alebo typy modulov (moduly pred spustením a moduly počas behu).	áno
80	The proposed solution policy modifications should be applied in near real time	Zmeny politík navrhovaného riešenia musia byť aplikované v takmer reálnom čase.	áno
	Exclusions	**Výnimky**	
81	The proposed solution should have predefined list of known or recommended exclusions	Navrhované riešenie musí mať preddefinovaný zoznam známych alebo odporúčaných výnimiek.	áno
82	The proposed solution should include workflows to easily exclude false positives	Navrhované riešenie musí zahŕňať pracovné postupy na jednoduché vylúčenie falošných pozitívnych výsledkov.	áno
83	The proposed solution should provide the option for the administrators to make policy exclusions of the console at multiple levels.	Navrhované riešenie musí poskytovať možnosť administrátorom vylúčiť politiky z konzoly na viacerých úrovniach.	áno

84	The proposed solution have capability to exclusions configured by the administrator to handle performance issues down to specific paths or single executables by reducing or disabling monitoring of parent processes and/or parent processes and all of their spawned child processes	Navrhované riešenie musí mať možnosť konfigurácie výnimiek správcom na riešenie problémov s výkonom, nastavením konkrétnej cesty alebo spustiteľného súboru s obmedzením alebo zakázaním monitorovania týchto procesov alebo týchto procesov a všetkých ich podradených procesov.	áno
	Device Control, Network Control and Application Visibility Discovery	Device Control, Network Control and Application Visibility Discovery	
85	The proposed solution device Control capabilities should be available on Windows	Navrhované riešenie musí mať schopnosť kontroly zariadení dostupnú na systémoch Windows.	áno
86	The proposed solution device Control should support block, read only and allow read-write on USB /Bluetooth.	Kontrola zariadenia v navrhovanom riešení musí podporovať blokovanie, read only a read-write prístup na USB/Bluetooth	áno
87	The proposed solution should have granular device control capability which can be applied to a Class, Serial Number Product ID or Type of Device.	Navrhované riešenie musí mať detailnú schopnosť kontroly zariadení, ktorá sa môže aplikovať na triedu, sériové číslo, identifikátor produktu alebo typ zariadenia.	áno
88	The proposed solution should have provide Firewall Control for Windows / Linux.	Navrhované riešenie musí mať kontrolu firewallu pre systémy Windows/Linux.	áno
89	The proposed solution should have Firewall rules be built to apply to a specific group of devices (leveraging tagging or policy groups)	Pravidlá firewallu musia byť v navrhovanom riešení vytvorené tak, aby sa uplatňovali na konkrétnu skupinu zariadení (s využitím označovania alebo skupín politík).	áno
90	The proposed solution should have location aware firewall rules to apply different policies when on or off network	Navrhované riešenie musí mať pravidlá firewallu citlivé na umiestnenie, aby sa mohli aplikovať rôzne politiky pri pripojení a odpojení od siete.	áno
91	The proposed solution must identify rogue devices discovery capability to reduce the potential attack surface.	Navrhované riešenie musí mať schopnosť identifikovať neautorizované zariadenia na redukciu bodov, ktoré by mohli byť využité na potentionálny útok.	áno
92	The proposed solution must provide a software/application inventory for the environment	Navrhované riešenie musí poskytovať inventár softvéru/aplikácií pre prostredie.	áno
93		Navrhované riešenie musí umožňovat inštaláciu agentov metódou Peer-to-Peer	áno
	Dashboards & Reporting	Dashboards & Reporting	
94	The proposed solution should report all known vulnerabilities in programs installed on an endpoint, along with export option	Navrhované riešenie musí hlásiť všetky známe zraniteľnosti v programoch nainštalovaných na koncovom bode, spolu s možnosťou exportu dát.	áno
95	The proposed solution have option to export data into 3rd party reporting tools such as Tableau or PowerBI	Navrhované riešenie musí mať možnosť exportovať dáta do nástrojov na správu dát tretích strán, ako sú Tableau alebo PowerBI.	áno
96	The proposed solution must have customizable dashboards as per user	Navrhované riešenie musí mať možnosť prispôsobiteľných informačných panelov podľa požiadaviek používateľa.	áno
	Compliance	Compliance	
97		Výrobca navrhovaného riešenia musí byť zaradený podľa nezávislého a medzinárodne uznávaného hodnotenia jednotlivých bezpečnostných produktov spoločností Gartner, Inc., Magic Quadrant for Endpoint Protection Platforms do kategórie „Leaders“, minimálne posledné dva roky.	áno
98	The proposed solution must be fulfilling following compliances such as HIPAA compliant ,PCI compliant,GDPR compliant,ISO27001 compliant	Navrhované riešenie musí spĺňať súladové požiadavky, ako sú súlad s HIPAA, súlad s PCI, súlad s GDPR. SaaS platforma výrobcu musí byť certifikovaná podľa SOC 2 Type II.	áno
	Integrations	Integrácia	

99	The proposed solution should support integration with Active Directory	Navrhované riešenie musí podporovať integráciu s Active Directory.	áno
100	The proposed solution should have integrations to Virus Total or similar tools	Navrhované riešenie musí mať integrácie s nástrojmi ako Virus Total alebo podobnými.	áno
101	The proposed solution should have native integrations/integrations with SIEM solutions such as Splunk, Qradar & etc.	Navrhované riešenie musí mať natívne integrácie alebo integrácie so SIEM riešeniami ako Splunk, Rapid 7, Qradar a podobnými.	áno
102	The proposed solution should have option to send event logs via Syslog.	Navrhované riešenie musí mať možnosť odoslať udalostné protokoly cez protokol Syslog.	áno
		Bezpečnost Active Directory	
103		Riešenie musí vykonávať testy na detekciu zraniteľností Active Directory spojených s autentifikáciou, autorizáciou, nastavením účtu, certifikačnými službami, oprávneniami/delegáciami a bezpečnostnými problémami priamo súvisiacimi so zabezpečením Domain Controller(ov) a Azure AD.	áno
104		Riešenie musí kategorizovať testy do najmenej štyroch závažností od najkritickejších po najnižšiu	áno
105		Riešenie musí byť schopné príjmať oznámenia z on-premise AD (provozné udalosti) v reálnom čase.	áno
106		Riešenie nesmie vyžadovať plné administrátorské oprávnenia na Active Directory alebo Domain Controlleroch.	áno
107		Riešenie musí obsahovať bezpečnostné hodnotenia pre on-premise a Azure AD.	áno
108		Riešenie musí mať možnosť nasadenia on-premise.	áno
109		Overenia on-prem AD musia byť vykonávané jediným zariadením pripojeným k doméne.	áno
110		Riešenie nesmie vyžadovať VPN pripojenie medzi on-prem komponentmi a cloudovou konzolou.	áno
111		Riešenie musí byť schopné automaticky objaviť viaceré domény a zahrnúť ich do rozsahu testov a ochrany.	áno
112		Riešenie musí byť schopné vykonávať overenia Azure-AD prostredníctvom API poskytovaného spoločnosťou Microsoft.	áno
113	• The solution must be able to detect attacks against the AD, including: o 'Low and slow' brute force attempts like 'Password Spray' o Mass account lockouts o Mass Password changes o Mass account disabling/deletion o Suspicious password changes for sensitive accounts o Reactivation of disabled privileged accounts o DCSync attacks o Rouge Domain Controller attacks (DCShadow) o Use of the default "Administrator" account o Suspicious service creation on Domain Controller(s)	Riešenie musí byť schopné detegovať útoky voči Active Directory, vrátane: Low and slow pokusy o hrubú silu, ako je Password Spray, Hromadné uzamknutie účtov, Hromadná zmena hesiel, Hromadné vypnutie/zmazanie účtov, Podozrivé zmeny hesiel pre citlivé účty, Znovuaktivácia deaktivovaných privilegovaných účtov, Útoky DCSync, Útoky na rouge Domain Controller (DCShadow), Použitie default účtu Administrator, Podozrivé vytváranie služieb na Domain Controller(och).	áno
114	• Threat detection must not rely on scheduled AD replication to minimize impact on the AD.	Detekcia hrozieb nesmie spočívať v plánovanom replikovaní AD, aby sa minimalizovalo zaťaženie na AD	áno

115		Riešenie musí umožnovať externé spracovanie detekcie hrozieb do riešení SIEM, SOAR a XDR	áno
116		Riešenie musí poskytovať podrobné usmernenia na odstránenie zistených zraniteľností, vrátane Odkazy na taktiky a techniky MITRE Att&ack, Kroky na prípravu remediacie, Kroky na vykonanie remediacie, Odkazy na doplnkové informácie od širšej komunity pre zabezpečenie AD.	áno
117		Riešenie musí byť schopné generovať skripty na remediaciu, ktoré možno vykonať v príslušných doménach s nasledujúcimi schopnosťami: Podrobný výber zraniteľností na odstránenie, Podrobný výber objektov, na ktorých sa bude remediacia vykonávať, História remediacie o stave procesu remediacie (vygenerovaný skript, stiahnutý, vykonaný s výsledkom úspechu alebo zlyhania), Skripty na vrátenie zmien pri bývalej remediacii na základe skriptu.	áno
118		Riešenie musí byť schopné automaticky spúšťať celý testovací cyklus v konfigurovateľnom rozvrhu používateľa (napr. každých X dní), pridať výsledky do svojej databázy a generovať podrobné testovacie správy bez ďalšieho zásahu používateľa.	áno
119		Riešenie musí podporovať ad-hoc spustenia celého testovacieho cyklu a prezentovať výsledky v GUI a v podrobných správach.	áno
120		Riešenie musí podporovať spustenie individuálnych testov ad-hoc, bez potreby spúšťať celý testovací cyklus.	áno
121		Systém musí podporovať vytváranie a dokumentovanie výnimiek pre budúce testovacie behy na nasledujúcich úrovniach: Domény, Jednotlivé testy pre doménu, Jednotlivé objekty (užívateľ alebo skupina) pre test a doménu.	áno
122		Riešenie musí podporovať vytváranie týchto výnimiek na centrálnej lokalite v GUI alebo priamo z príslušných testov/výsledkov s možnosťou pridávania komentárov k tomu, prečo boli tieto výnimky vytvorené.	áno
123		Riešenie musí obsahovať informačný panel, ktorý poskytuje rýchle informácie o výsledkoch testov, ako sú: Počet testov podľa závažnosti a ich výsledky (úspech/zlyhanie/skipované) celkom a pre testované domény, Zistená topológia domény a vzťahy medzi doménami, Skóre zdravia a priradená úroveň rizika celkovo a individuálne pre jednotlivé domény, Najkritickejšie/závažné zistenia a počet ovplyvnených objektov, Grafická reprezentácia zlyhaných testov v	áno

		posledných behoch, ktorá umožňuje používateľovi rýchlo vidieť zmeny v zabezpečení v čase.	
124	• The solution must provide extensive filtering capabilities of test results including at least: o Previous tests o Severity o Domain name o Forest name o Detection name o Acknowledgement status o Vulnerability status o Computer(s) affected o Group(s) affected o User(s) affected	Riešenie musí poskytovať rozsiahle možnosti filtrovania výsledkov testov, vrátane aspoň: Predchádzajúce testy, Závažnosť, Názov domény, Názov forest, Názov zistenia, Stav potvrdenia, Stav zraniteľnosti, Počítač(y) ovplyvnené/postihnute, Skupina(y) ovplyvnená/postihnuta, Užívateľ(ia) ovplyvnení/postihnuty.	áno
125		Riešenie musí byť schopné porovnávať výsledky testov s predchádzajúcimi .	áno
126		Riešenie musí poskytovať minimálne nasledujúce podrobnosti o každom vykonanom teste: Popis testu, Odkaz na relevantné webové stránky MITRE Att&ck, Mitigačné kroky, Nástroje na útok, ktoré môžu využívať zistenú zraniteľnosť, Odkazy na relevantné články od komunity pre zabezpečenie AD.	áno
127		Riešenie musí poskytovať podrobné informácie o dôvodoch zistenia zraniteľností,vrátane: Typy objektov, napr. Užívateľ alebo Skupina, Názvyobjektov, Porušené nastavenia na úrovni objektu, napr. aké oprávnenia boli zistené.	áno
		Služby a podpora	
128		Súčasťou riešenia musia byť dohľadové služby MDR - Managed Detection and Response, kontrola incidentov z prostredí zákazníka poskytované výrobcom riešenia.	áno
129		Výrobca musí poskytovať aj voliteľnú možnosť priameho riešenia a uzatvárania týchto incidentov MDR týmom.	áno
130		V rámci služby musí byť k dispozícii analýza prvotnej príčiny incidentu dostupná na vyžiadanie.	áno
131		Služba musí byť poskytovaná v režime 24x7	áno
132		Súčasťou služby musí byť ročný balík konzultačných hodín, ktorý zákazník môže použiť podľa potreby na podrobné vyšetrovanie, alebo proaktívné služby spojené s bezpečnosťou.	áno

Príloha č. 2
Cena

Návrh na plnenie kritéria

Obchodné meno uchádzača:	**airo, s. r. o.**
Adresa uchádzača:	**Ivanská cesta 30/B, 821 04 Bratislav**
Meno osoby oprávnenej konať za uchádzača:	**Mgr. Jakub Čeles, Ing. Tomáš Nečas, Ladislav Liščák**
Meno kontaktnej osoby a jej funkcia:	**Mgr. Jakub Čeles, konateľ**
Číslo tel. kontaktnej osoby:	**+421 915 493 566**
E-mail kontaktnej osoby:	**Jakub.celes@airo.sk**

Kritérium I. –Cena za dodanie a implementáciu, služby podpory prevádzky a údržby dodaného komplexného nástroja pre EPPEDR s požadovanými funkciami a riešením incidentov s požadovanými funkciami

Položka	Popis	Merná jednotka		Množstvo [mesiac]	Jednotková cena [v EUR bez DPH]	Jednotková cena [v EUR s DPH]	Cena za množstvo [v EUR bez DPH]	Sadzba DPH [v %]	Výška DPH [v EUR]	Cena za množstvo (Kritérium I.) [v EUR bez DPH]
	A	B		C	D	E	(CxD)	F	(CxE) - (CxD)	(CxD)
1	Jednorázový poplatok za SW licencie alebo predplatené služby na **36** mesiacov vrátane implementácie a riešenia incidentov počas **36** mesiacov	Služba		1	124795,7	149754,84	149754,84	20	24959,14	**124795,7**
	Kritérium I. - Cena za dodanie a implementáciu komplexného nástroja EPPEDR v EUR bez DPH									124795,70

Príloha č. 3
Plán realizácie

Implementácia komplexného EPPEDR nástroja v rozsahu

- nastavenie a konfigurácia prostredí verejného obstarávateľa,
  - konfigurácia Windows systémov
  - overenie funkčných a výkonových parametrov Windows agentov,
  - konfigurácia Linux systémov
  - overenie funkčných a výkonových parametrov Linux agentov,
  - predvedenie vytvorenia a uloženia vlastného dashboardu a reportu,
  - predvedenie vytvorenia a uloženia užívateľsky definovaného parseru,
  - konfigurácia cloudovej služby
- 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,

Služby podpory prevádzky a údržby dodaného komplexného nástroja pre EPPEDR

post-implementačná podpora v rozsahu 10 človekodeň na obdobie 36 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

PODPISY ZMLUVNÝCH STRÁN

V Bratislave dňa 19.11.2024

Dopravný podnik Bratislava, akciová spoločnosť

Meno: Ing. Milan Donoval
Funkcia: podpredseda predstavenstva - CTO

Meno: Mgr. Gabriela Dikošová
Funkcia: člen predstavenstva

V Bratislave dňa 20.11.2024

airo, s. r. o.

Meno: Mgr. Jakub Čeles
Funkcia: konateľ

airo, s.r.o.
Ivanská cesta 30/B
821 04 Bratislava
info@airo.sk
IČO: 48286621 DIČ: 2120122488

Meno: Ladislav Liščák
Funkcia: konateľ

Meno: Ing. Tomáš Nečas
Funkcia: konateľ