Zmluva na poskytovanie služieb monitoring kybernetickej bezpečnosti č. C-NBS1-000-106-915

uzatvorená podľa § 269 ods. 2 zákona č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov
(ďalej len „Zmluva")

ZMLUVNÉ STRANY

Objednávateľ:
Názov**:** Národná banka Slovenska
Sídlo: Imricha Karvaša 1, 813 25 Bratislava
Zastúpený:
IČO: 30844789
DIČ: 2020815654
IČ DPH: SK2020815654
Bankové spojenie:
Č. účtu v tvare IBAN:
(ďalej len „objednávateľ" alebo „NBS")

a

Poskytovateľ:
Obchodné meno: **ANECT a.s.**
Sídlo: Jarošova 1, 831 03 Bratislava
Zastúpený:
IČO: 35 787 546
IČ DPH: SK2020256579
DIČ: 2020256579
Bankové spojenie:
Číslo účtu v tvare IBAN:
Zapísaný: v Obchodnom registri Mestského súdu Bratislava III, Oddiel: Sa, Vložka číslo: 2431/B
(ďalej len „poskytovateľ")

(objednávateľ a poskytovateľ spolu aj ako „Zmluvné strany")

PREAMBULA

A. Objednávateľ ako verejný obstarávateľ vyhlásil oznámením o vyhlásení verejného obstarávania – všeobecná smernica, zverejneným vo Vestníku verejného obstarávania 58/2025 pod číslom 5418 - MSS dňa 21.03.2025, nadlimitnú zákazku podľa zákona č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon o verejnom obstarávaní") s názvom „*Monitoring kybernetickej bezpečnosti*".

B. Na základe vyhodnotenia ponúk bola ponuka poskytovateľa vyhodnotená ako ponuka úspešného uchádzača. Vzhľadom na túto skutočnosť a predloženú ponuku poskytovateľa sa zmluvné strany na základe slobodnej vôle a v súlade s právnymi predpismi platnými na území Slovenskej republiky rozhodli uzatvoriť túto Zmluvu.

C. V roku 2023 NBS obstarala formou verejnej súťaže poskytovanie služieb podpory činností prevádzky a vyhodnocovania monitorovania bezpečnosti informačných systémov. V rámci tejto podpory sú poskytované nasledovné služby: *Služba Monitoring bezpečnosti IT, Služba Monitoring SIEMu, Služba Prevádzka SIEMu, Služba Rozvoj SIEMu, Služba Optimalizácia SIEMu, Služba Sledovanie IT hrozieb a zraniteľností, Služba „Forenzná analýza a Exit služba*. Tieto služby, okrem Exit služby, sú poskytované do 31.08.2025.

ČLÁNOK I
ÚČEL ZMLUVY A PREDMET PLNENIA

1. Účelom Zmluvy je zabezpečiť kontinuitu poskytovania služieb monitoringu kybernetickej bezpečnosti aj **po 31. auguste 2025** a zároveň rozšíriť pravidelné poskytované služby o službu skenovanie zraniteľností a BAS služby. Služby sú poskytovateľom poskytované v minimálne zmluvne určenej kvalite. Počas trvania Zmluvy bude poskytovateľ pokračovať v rozvoji poskytovaných služieb podľa požiadaviek objednávateľa. Tieto ciele chce objednávateľ dosiahnuť prostredníctvom poskytovateľových kapacít a efektívnym využitím existujúcich technológií, licencií objednávateľa a jeho kapacít. Existujúce objednávateľove technológie, licencie a kapacity nie sú garantované počas trvania tejto Zmluvy.

2. Poskytovateľ sa zaväzuje poskytovať objednávateľovi tieto služby:

a) **Službu Monitoring bezpečnosti IT (SOC),** ktorej cieľom je vyhľadávanie a prešetrenie podozrivých log záznamov, udalostí a alarmov a spolupodieľanie na riešení bezpečnostných incidentov, bližšia špecifikácia a podmienky tejto služby sú upravené v Prílohe 1 tejto Zmluvy, pričom tieto služby sú poskytované v režime 15/5 (počet hodín zo dňa/počet dní v týždni) a v prípade uplatnenia opcie objednávateľom je možné tieto služby poskytovať po uplynutí prvých 24 mesiacov od účinnosti tejto Zmluvy v režime 24/7 namiesto režimu 15/5 na dobu 36 mesiacov v cene dohodnutej v Prílohe 3 tejto Zmluvy;

b) **Službu Monitoring a prevádzka MBIT (SIEM a NDR),** ktorej cieľom je monitorovanie a zabezpečenie dostupnosti, výkonu a funkčnosti komponentov MBIT, nepretržitého zberu a spracovania logov a sieťových tokov, vykonávanie bežných prevádzkových činností MBIT za účelom zabezpečenia funkčnosti a aktuálnosti jednotlivých komponentov MBIT a zabezpečenia nepretržitého zberu a spracovania logov z monitorovaných zariadení. Bližšia špecifikácia a podmienky tejto služby sú upravené v Prílohe 1 tejto Zmluvy, pričom tieto služby sú poskytované v režime 15/5 (počet hodín zo dňa/počet dní v týždni) a v prípade uplatnenia opcie objednávateľom je možné tieto služby poskytovať po uplynutí prvých 24 mesiacov od účinnosti tejto Zmluvy v režime 24/7 namiesto režimu 15/5 na dobu 36 mesiacov v cene dohodnutej v Prílohe 3 tejto Zmluvy;

c) **Službu Skenovanie zraniteľností**, ktorej cieľom je zabezpečiť výkon činností procesu riadenia zraniteľností v IT infraštruktúre spravovanej NBS; bližšia špecifikácia a podmienky tejto služby sú upravené v Prílohe 1 tejto Zmluvy;

d) **Služba Sledovanie IT hrozieb a zraniteľností,** cieľom služby je sledovanie aktuálnych zraniteľností publikovaných na overených externých zdrojoch s cieľom identifikovať potenciálne bezpečnostné hrozby pre IT NBS. Bližšia špecifikácia a podmienky tejto služby sú upravené v Prílohe 1 tejto Zmluvy;

e) **Služba BAS**, ktorej cieľom je zabezpečiť pravidelnú, systematickú a konzistentnú kontrolu stavu bezpečnosti IT infraštruktúry formou simulácie prienikov a útokov na IT infraštruktúru NBS metodikou MITRE ATT&CK (nie skutočný malvér na skutočnú infraštruktúru). Odhaliť slabé miesta ochrany bezpečnosti IT, resp. uskutočniteľnosť potenciálneho útoku. Účinnosť jestvujúcich ochranných prvkov, resp. námety na zlepšenie ich konfigurácie. Efektívnosť detekčných nástrojov, t.j. relevantnosť logovaných informácií do SIEMu. Spôsob vyhodnotenia v SIEMe. Reakcia SOC tímu a odozva na incident. Opakovaná automatická kontrola účinnosti jestvujúcich ochranných prvkov, najmä po zmenách v IT infraštruktúre a po zmenách nastaveniach ochranných prvkov. Bližšia špecifikácia a podmienky tejto služby sú upravené v Prílohe 1 tejto Zmluvy;

f) **Služba Rozvoj a optimalizácia MBIT** cieľom služby je tvorba a úprava konfigurácie komponentov MBIT, vytváranie nových a údržba existujúcich use casov a zároveň pravidelné vyhľadávanie anomálií v nazbieraných dátach, stavu parsovania udalostí a posudzovanie kvality fungovania vyhodnocovania bezpečnostných udalostí komponentmi MBIT za dlhšie časové obdobie, vypracovávanie odporúčaní a návrhov na zlepšenie kvality fungovania zberu a vyhodnocovania bezpečnostných udalostí bližšia. Bližšia špecifikácia a podmienky tejto služby sú upravené v Prílohe 1 tejto Zmluvy;

g) **Služba „Forenzná analýza“,** ktorej cieľom služby je vyšetrenie bezpečnostných incidentov tak, aby získané fakty a dôkazy boli použiteľné v právnych sporoch, poskytla pred súdom znalecké posudky alebo materiál na ďalšie vyšetrovanie počítačovej kriminality. Cieľom služby nie je analýza softvérového kódu. Bližšia špecifikácia a podmienky tejto služby je v Prílohe 1 tejto Zmluvy. Poskytovaná služba – Forenzná analýza je poskytovaná na základe vystavenej objednávky objednávateľa;

h) **Konzultačné a implementačné služby,** ktorých cieľom je vytvoriť možnosť priebežného rozvoja poskytovaných služieb počas trvania tejto Zmluvy a možnosť osobitných konzultácií k poskytovaným službám. Bližšia špecifikácia a podmienky tejto služby je v Prílohe 1 tejto Zmluvy. Poskytované Konzultačné a implementačné služby sú poskytované na základe vystavenej objednávky objednávateľa;

i) **Exit služba**, ktorej cieľom je zabezpečiť plynulý prechod v poskytovaní služieb medzi pôvodným poskytovateľom a novým poskytovateľom služieb tak, aby nebola narušená kontinuita monitorovania IT bezpečnosti NBS. Bližšia špecifikácia služby je upravená v Prílohe 1 tejto Zmluvy. Poskytovaná služba – Exit služba je poskytovaná na základe vystavenej objednávky objednávateľa (ďalej spolu ako „predmet plnenia“ alebo „poskytované služby“).

3. Predmetom plnenia nie je:

a) dodanie hardvéru objednávateľovi a
b) dodanie softvéru objednávateľovi.

4. Objednávateľ sa zaväzuje za podmienok dohodnutých v tejto Zmluve za riadne poskytnutý predmet plnenia zaplatiť poskytovateľovi dohodnutú cenu podľa článku IV tejto Zmluvy. Spôsob riadneho poskytnutia predmetu plnenia je upravený v Prílohe 1 tejto Zmluvy.

5. Poskytovateľ sa zaväzuje poskytovať predmet plnenia prostredníctvom osôb (expertov/kľúčových pracovníkov), identifikovaných a určených v Prílohe 7 tejto Zmluvy.

6. Poskytovateľ sa zaväzuje poskytovať predmet plnenia v súlade s požiadavkami podľa Prílohy 1, pričom sú v nej upravené požiadavky na predmet plnenia t. j. požiadavky na technológie, ktoré poskytovateľ použije na plnenie poskytovaných služieb, časový harmonogram poskytovaných služieb, požiadavky na rozvoj a optimalizáciu poskytovaných služieb, spôsob monitorovania a vyhodnocovania poskytovaných služieb, požiadavky na odbornú spôsobilosť pracovníkov poskytovateľa.

ČLÁNOK II
ČAS POSKYTOVANIA POSKYTOVANÝCH SLUŽIEB

1. Časový harmonogram poskytovaných služieb je upravený v Prílohe 6 Zmluvy. Začiatok poskytovania poskytovaných služieb je odo dňa nadobudnutia účinnosti tejto Zmluvy, pričom poskytovateľ začne s realizáciou, poskytovaním predmetu plnenia podľa Článku I bod 1.1 písm. g),h),i) až po objednávateľovom vystavení písomnej záväznej objednávky, ktorá je poskytovateľovi doručená podľa článku II bod 4 tejto Zmluvy.

3. V prípade oneskorenia začatia poskytnutia poskytovaných služieb, ktoré nebude spôsobené poskytovateľovým zavinením, sa lehota na plnenie primerane predĺži písomnou dohodou zmluvných strán, najmenej však o dobu omeškania nezavineného poskytovateľom.

4. Písomná objednávka na poskytované služby – Konzultačné a implementačné služby, Exit služby, Služba – Forenzná analýza sa prioritne zadáva prostredníctvom kontaktného e-mailu, ktorý si zmluvné strany písomne oznámia do 5 dní odo dňa nadobudnutia účinnosti tejto Zmluvy . Vo vystavenej písomnej objednávke sa uvedú najmä základné požiadavky na poskytovanú službu, a to identifikácia poskytovanej služby, požadovaný rozsah poskytovanej služby napr. vyjadrený v osobohodinách, začiatok poskytovania poskytovaných služieb a kalkuláciu ceny, ktorá vychádza z ceny dohodnutej v tejto Zmluve.

5. Poskytovateľ sa zaväzuje z pohľadu dodržiavania podmienok poskytovania poskytovaných služieb písomne vyhodnotiť poskytnuté poskytované služby objednávateľovi spolu s ich zoznamom, a to za každý kalendárny mesiac trvania tejto Zmluvy. Toto vyhodnotenie a tento zoznam dodá objednávateľovi prostredníctvom výkazu podľa Prílohy 8 Zmluvy v elektronickej podobe do 10. dňa nasledujúceho kalendárneho mesiaca za mesiac v ktorom boli poskytované služby poskytnuté, pokiaľ sa Zmluvné strany písomne nedohodnú inak.

6. Objednávateľ do piatich pracovných dní odsúhlasí predložené podklady a výkaz podľa Prílohy 8 Zmluvy alebo zašle poskytovateľovi pripomienky, ktoré je poskytovateľ povinný akceptovať.

7. Po zapracovaní pripomienok objednávateľa poskytovateľom do výkazu podľa Prílohy 8 Zmluvy alebo po odsúhlasení predložených podkladov a výkazu podľa Prílohy 8 Zmluvy objednávateľom, objednávateľ vystaví a potvrdí protokol o vyhodnotení služieb a výkaz podľa prílohy 8 Zmluvy.

8. Poskytovateľ splní svoju povinnosť poskytnúť predmet plnenia v prípade, ak okrem záväzku poskytnúť služby splní aj minimálne podmienky monitorovania a vyhodnocovania poskytnutých služieb stanovené v Prílohe 1 Zmluvy.

9. Ak poskytovateľ nesplní minimálne podmienky poskytnutých služieb (Monitorovanie a vyhodnocovanie poskytovaných služieb) stanovené v Prílohe 1 Zmluvy, tak sa poskytovateľ zaväzuje poskytnúť objednávateľovi zľavu z mesačného paušálneho poplatku príslušnej služby, pri ktorej neboli splnené minimálne podmienky (Monitorovanie a vyhodnocovanie poskytnutých služieb) vo výške 50 % z príslušnej paušálnej mesačnej platby konkrétnej služby. V takomto prípade, je poskytovateľ povinný vystaviť faktúru na poskytnuté služby vo výške zníženej o príslušnú zľavu z ceny služby.

10. Objednávateľ je oprávnený požiadať poskytovateľa a ten je povinný písomne akceptovať zmenu rámcového plánu uvedeného v Prílohe 6 Zmluvy. V prípade takejto zmeny rámcového plánu nie je potrebné uzatvárať písomný dodatok k tejto Zmluve.

ČLÁNOK III
MIESTO A TERMÍN DODANIA PREDMETU PLNENIA

1. Miestom plnenia poskytovaných služieb podľa ustanovení tejto Zmluvy je sídlo objednávateľa nachádzajúce sa na adrese Národná banka Slovenska, Imricha Karvaša 1, 813 25 Bratislava, Slovenská republika.

2. Ďalším miestom plnenia poskytovaných služieb podľa ustanovení tejto Zmluvy sú nasledujúce miesta objednávateľa:

1.	Národná banka Slovenska, Rybničná 40, Bratislava, Slovenská republika (Záložné pracovisko NBS - ZPB)
2.	Národná banka Slovenska, Kopčianska 92, Bratislava, Slovenská republika (Záložné technologické pracovisko NBS - ZTP)

3. Ak to technické podmienky umožňujú, tak prednostne platí, že poskytovateľ poskytuje predmet plnenia prostredníctvom vzdialeného prístupu zabezpečeného sieťového VPN spojenia. Poskytovateľ sa zaväzuje rešpektovať všetky bezpečnostné, organizačné a technické opatrenia a ďalšie relevantné predpisy objednávateľa spojené s prácou v priestoroch objednávateľa i so vzdialeným prístupom k informačným technológiám a sieti objednávateľa v zmysle článku V Prílohy 2 Všeobecné podmienky k Zmluve ako aj v zmysle platných predpisov a štandardov objednávateľa, ktoré poskytovateľovi zabezpečí oprávnená osoba objednávateľa počas celej doby trvania Zmluvy. Objednávateľ oboznámi poskytovateľa so všetkými takýmito predpismi, o čom bude spísaný záznam.

4. Miesto plnenia sa môže zmeniť, ak sa na tom zmluvné strany písomne dohodnú. Táto písomná zmena Zmluvy sa môže vykonať bez uzatvorenia dodatku k tejto Zmluve.

ČLÁNOK IV
CENA ZA POSKYTOVANÉ SLUŽBY A ICH PLATOBNÉ PODMIENKY

1. Ceny za Poskytované služby podľa Zmluvy si objednávateľ a poskytovateľ dohodli v súlade so zákonom NR SR č. 18/1996 Z. z. o cenách v znení neskorších predpisov a vyhlášky Ministerstva

financií SR č. 87/1996 Z. z. v znení neskorších predpisov, ktorou sa vykonáva zákon č. 18/1996 Z. z. o cenách v znení neskorších predpisov sú uvedené v Prílohe 3 tejto Zmluvy. Ceny za poskytovanie predmetu plnenia zahŕňajú všetky náklady poskytovateľa spojené s poskytovaním poskytovaných služieb vrátane dopravy. Objednávateľ sa zaväzuje zaplatiť poskytovateľovi za poskytované služby poskytnuté na základe tejto Zmluvy ceny podľa Prílohy 3 tejto Zmluvy.

2. Fakturácia služieb sa bude vykonávať prostredníctvom mesačných faktúr vystavených vždy po skončení kalendárneho mesiaca po vyhodnotení poskytnutých služieb v danom kalendárnom mesiaci a objednávateľovom písomnom potvrdení protokolu o vyhodnotení služieb a výkazu podľa prílohy č. 8 tejto Zmluvy. Poskytovateľ je oprávnený fakturovať cenu za Poskytované služby tejto Zmluvy mesačne za každý kalendárny mesiac v posledný deň mesiaca, za ktorý boli poskytované služby poskytnuté.

3. Poskytovateľ bude vystavovať pre všetky služby poskytnuté v priebehu jedného kalendárneho mesiaca iba jednu spoločnú mesačnú faktúru.

4. Prílohou faktúry bude protokol o vyhodnotení služieb potvrdený objednávateľom (vlastnoručne podpísaný oprávnenou osobou objednávateľa podľa článku VI Zmluvy).

5. Zmluvné strany sa v súlade s § 18 ods. 1 písm. a) zákona o verejnom obstarávaní dohodli, že poskytovateľ má právo na zmenu ceny v priebehu plnenia Zmluvy za podmienok uvedených a špecifikovaných v nasledujúcich bodoch tohto článku.

6. Ceny položiek vedené v Tabuľke 1 Prílohy 3 Zmluvy:

Položka číslo	**Popis služby**	**Čo podlieha inflácii**
S1	Paušálna mesačná platba za službu **„SOC" – režim 15/5**	Cena mesačného paušálneho poplatku v eurách bez DPH za mesiac
S2	Paušálna mesačná platba za službu **„MBIT" – režim 15/5**	Cena mesačného paušálneho poplatku v eurách bez DPH za mesiac
S3	Paušálna mesačná platba za službu **„SOC" – režim 24/7**	Cena mesačného paušálneho poplatku v eurách bez DPH za mesiac
S4	Paušálna mesačná platba za službu **„MBIT" – režim 24/7**	Cena mesačného paušálneho poplatku v eurách bez DPH za mesiac
S5	Paušálna mesačná platba za službu **„Skenovanie zraniteľností" – režim 8/5**	Cena mesačného paušálneho poplatku v eurách bez DPH za mesiac
S6	Paušálna mesačná platba za službu **„Sledovanie IT hrozieb a zraniteľností" – režim 8/5**	Cena mesačného paušálneho poplatku v eurách bez DPH za mesiac
S7	Paušálna mesačná platba za službu **„BAS" – režim 8/5**	Cena mesačného paušálneho poplatku v eurách bez DPH za mesiac
S8	Paušálna mesačná platba za službu **„Rozvoj a optimalizácia MBIT" – režim 8/5**	Cena mesačného paušálneho poplatku v eurách bez DPH za mesiac
S9	Hodinová sadzba za osobohodinu služby „**Forenzná analýza**"	Cena osobohodiny v eurách bez DPH
S10	Hodinová sadzba za osobohodinu služby „**Exit služba**"	Cena osobohodiny v eurách bez DPH
S11	Hodinová sadzba za osobohodinu služby „**konzultačné a implementačné služby**"	Cena osobohodiny v eurách bez DPH

možno na žiadosť poskytovateľa navýšiť z dôvodu inflácie, a to každý kalendárny rok nasledujúci po roku, v ktorom uplynie 1 (jeden) rok od účinnosti Zmluvy, až do doby konca trvania Zmluvy. Žiadosť je poskytovateľ povinný doručiť objednávateľovi do 15.2. príslušného roku (príklad: Zmluva nadobudne účinnosť 1.9.2025, jeden rok od účinnosti zmluvy je 1.9.2026, nasledujúci rok je 2027, poskytovateľ musí do 15.2.2026 požiadať o navýšenie ceny).Navýšenie z dôvodu inflácie nie je možné vykonávať spätne.

7. Paušálne mesačné ceny a hodinové sadzba za osobohodiny je možné zvýšiť iba vtedy, keď inflácia presiahne v jednotlivom roku výšku 3 % a maximálne o čiastku vo výške 8 % ceny mesačného paušálu alebo hodinovej sadzby za osobohodinu.

8. Infláciou sa rozumie zverejnená medziročná miera inflácie vyjadrená prírastkom harmonizovaného indexu spotrebiteľských cien pre Eurozónu za 12 mesiacov predchádzajúceho kalendárneho roka, zverejňovaného Štatistickým úradom Európskych spoločenstiev (http://ec.europa.eu/eurostat).

9. Zmena Zmluvy podľa tohto článku sa vykoná písomne, pričom sa nemusí uzatvoriť písomný dodatok k tejto Zmluve. Každá zmena podľa tohto článku musí byť písomne potvrdená a odsúhlasená objednávateľom.

10. Zmluvné strany sa dohodli a výslovne súhlasia s tým, že poskytovateľ bude zasielať len elektronické faktúry z e-mailovej adresy poskytovateľa xxx na e-mailovú adresu objednávateľa xxx vo formáte PDF. Zmluvné strany vyhlasujú, že majú výlučný prístup k uvedeným e-mailovým adresám. Zmluvné strany sú oprávnené zmeniť e-mailové adresy a to len písomne s uvedením novej e-mailovej adresy, pričom z dôvodu tejto zmeny nie je potrebné uzatvoriť dodatok k tejto Zmluve. Poskytovateľ nie je povinný podpísať elektronickú faktúru kvalifikovaným elektronickým podpisom. Elektronická faktúra musí spĺňať všetky náležitosti faktúry podľa § 74 zákona č. 222/2004 Z. z. o dani z pridanej hodnoty v znení neskorších predpisov. Zmluvné strany sú povinné bezodkladne písomne oznámiť druhej strane akúkoľvek zmenu, ktorá by mohla mať vplyv na doručovanie elektronických faktúr, najmä zmenu kontaktnej e-mailovej adresy.

11. Ceny sú uvedené bez DPH. Faktúry za predmet plnenia budú obsahovať aj vyčíslenie DPH podľa všeobecne záväzných právnych predpisov platných ku dňu splnenia predmetu Zmluvy.

12. V prípade, že faktúra nebude obsahovať všetky údaje podľa § 74 ods. 1 zákona č. 222/2004 Z. z. o dani z pridanej hodnoty v znení neskorších predpisov, resp. nebude po stránke vecnej alebo formálnej správne vystavená, objednávateľ ju vráti poskytovateľovi na doplnenie (prepracovanie) a nová lehota splatnosti začne plynúť dňom doručenia doplnenej (prepracovanej) faktúry objednávateľovi.

13. Poskytovateľ, ktorý uvedie na faktúre daň, sa zaväzuje, že odvedie daň správcovi dane v lehote ustanovenej v § 78 ods. 1 zákona č. 222/2004 Z. z. o dani z pridanej hodnoty v znení neskorších predpisov. Porušenie tejto povinnosti je podstatným porušením Zmluvy a dôvodom na okamžité odstúpenie objednávateľa od tejto Zmluvy.

14. Poskytovateľ najneskôr do doby vyhotovenia prvej faktúry predloží objednávateľovi originál potvrdenia o mieste svojej daňovej rezidencie, alebo jeho úradne overenú fotokópiu. Počas trvania Zmluvy poskytovateľ predmetné potvrdenie predloží objednávateľovi na začiatku každého nového zdaňovacieho obdobia. Poskytovateľ vyhlasuje a zaväzuje sa, že v prípade vzniku stálej prevádzkarne na území Slovenskej republiky počas trvania Zmluvy bude o tejto skutočnosti objednávateľa bezodkladne písomne informovať.

15. Faktúra je splatná do 30 dní odo dňa jej doručenia objednávateľovi bezhotovostným prevodom na účet poskytovateľa. Za deň splnenia peňažného záväzku sa považuje deň odpísania dlžnej sumy z účtu objednávateľa v prospech poskytovateľa.

16. Poskytovateľ ďalej nie je oprávnený postúpiť a ani založiť akékoľvek svoje pohľadávky voči objednávateľovi vzniknuté na základe alebo v súvislosti s touto Zmluvou alebo s plnením záväzkov podľa Zmluvy bez predchádzajúceho písomného súhlasu objednávateľa. Poskytovateľ nie je oprávnený jednostranne započítať akúkoľvek svoju pohľadávku voči objednávateľovi vzniknutú z akéhokoľvek dôvodu proti pohľadávke objednávateľa voči poskytovateľovi vzniknutej na základe alebo v súvislosti so Zmluvou bez predchádzajúceho písomného súhlasu objednávateľa.

ČLÁNOK V
DOBA TRVANIA ZMLUVY

Táto Zmluva sa uzatvára na dobu určitú, a to od 1. septembra 2025 do 31. augusta 2030, pričom Exit služba a konzultačné a implementačné služby sa môžu uplatniť vystavením objednávky u poskytovateľa až do 6 mesiacov po 31. auguste 2030.

ČLÁNOK VI
KONTAKTNÉ OSOBY PRE PLNENIE TEJTO ZMLUVY

Zmluvné strany sú povinné si navzájom najneskôr do 7 pracovných dní od nadobudnutia účinnosti tejto Zmluvy písomne (e-mailom) navzájom doručiť zoznam osôb oprávnených konať vo veciach zmluvných (zadávanie a prijímanie prípadných písomných objednávok na poskytovanie predmetu plnenia, opcie, nahlasovanie reklamácií, uplatnení práv zo záruk atď.) vrátane osôb určených na plnenie predmetu Zmluvy, a to v rozsahu: meno a priezvisko, funkcia, telefónne číslo, emailová adresa (ďalej len „zoznam oprávnených osôb zmluvnej strany"). Zmena oprávnenej osoby musí byť zaslaná druhej zmluvnej strane formou doporučeného listu podpísaného oprávneným zástupcom zmluvnej strany najneskôr 7 dní pred vykonaním zmeny.

ČLÁNOK VII
PRÁVA DUŠEVNÉHO VLASTNÍCTVA

1. Výsledky poskytnutia poskytovaných služieb podľa tejto Zmluvy, ktorých vytvorenie bolo zabezpečené špecificky na účely plnenia tejto Zmluvy, môžu mať povahu autorského diela v zmysle zákona č. 185/2015 Z. z. Autorský zákon v znení neskorších predpisov (ďalej len „Autorský zákon"). Autorským dielom sa na účely tejto Zmluvy rozumejú najmä dokumentácia, počítačové programy vrátane ich všetkých súčastí alebo každý update/upgrade informačného systému, databázy, súvisiaca dokumentácia, alebo akéhokoľvek iné autorské dielo vytvorené poskytovateľom spĺňajúce znaky autorského diela (ďalej len ako „dielo").

2. Poskytovateľ vyhlasuje, že vykonáva majetkové práva autora k dielu vytvorenému a dodanému na základe tejto Zmluvy a žiadna tretia osoba nie je oprávnená vykonávať majetkové práva autora k dielu alebo s dielom v zmysle Autorského zákona. Poskytovateľ vyhlasuje, že je oprávnený udeliť objednávateľovi licenciu v rozsahu a v súlade s touto Zmluvou. V prípade, ak tretia strana sa bude voči objednávateľovi domáhať porušenia svojich autorských práv je poskytovateľ povinný bezodkladne vysporiadať s takouto treťou stranou autorské práva, aby zodpovedali jeho vyhláseniam a udelenej licencii v tejto Zmluve a zároveň zodpovedá za všetku škodu, ktorá objednávateľovi tým vznikla.

3. Zmluvné strany sa dohodli, že pokiaľ poskytovateľ vytvorí v rámci plnenia tejto Zmluvy dielo, poskytovateľ na akékoľvek takéto dielo udeľuje objednávateľovi výhradnú, počas celej doby trvania majetkových práv, územne, vecne neobmedzenú a v cene za poskytnuté služby splatnú licenciu. Licencia zahŕňa všetky spôsoby použitia diela podľa § 19 ods. 4 Autorského zákona. Pre vylúčenie pochybností licencia zahŕňa právo dielo spracovať (dokončenie diela, zmenu diela, začlenenia do iných diel alebo iný zásah do diela), vrátane v rovnakom rozsahu výkonu autorských práv k strojovým a zdrojovým kódom najmä právo ich kopírovania, prekladania, prispôsobovania, modifikovania, upravovania a začleňovania do iných diel, a to prostredníctvom objednávateľa alebo tretej osoby. Poskytovateľ nie je oprávnený využívať dielo alebo ktorúkoľvek jeho časť diela pre vlastné produkty a služby, ak sa zmluvné strany písomne nedohodnú inak. Objednávateľ je oprávnený udeliť sublicenciu tretím osobám. Licencia je účinná dňom odovzdania diela, pričom poskytovateľ odovzdá objednávateľovi dielo najneskôr do 31. augusta 2030.

4. Poskytovateľ najneskôr v prvý deň plynutia posledných siedmich kalendárnych mesiacov trvania Zmluvy poskytne objednávateľovi všetky a úplné komentované zdrojové kódy k dielu vytvorené alebo zmenené na základe Zmluvy. Uvedeným nie je dotknuté právo objednávateľa kedykoľvek požiadať o vydanie všetkých zdrojových kódov alebo ktoréhokoľvek z nich. V prípade predčasného ukončenia Zmluvy táto povinnosť vzniká dňom požiadania objednávateľa o ich vydanie.

5. Vlastníkom veci, prostredníctvom ktorej je dielo vytvorené, sa stáva objednávateľ odovzdaním diela.

ČLÁNOK VIII
AUDIT, POISTENIE, KĽÚČOVÍ PRACOVNÍCI

1. Poskytovateľ sa zaväzuje bezodplatne umožniť objednávateľovi vykonať audit bezpečnosti, technického riešenia a kapacít a zároveň dodržiavanie poskytovania predmetu plnenia v súlade so zmluvnými požiadavkami objednávateľa, prípadne poskytnúť objednávateľovi výstupy

z takýchto auditov, vykonaných nezávislým audítorom. Poskytovateľ sa zaväzuje poskytnúť objednávateľovi alebo ním poverenému vykonávateľovi auditu potrebnú súčinnosť, vrátane všetkých informácií, ktoré si audit bude vyžadovať, najmä dokumentácie preukazujúce skutočné technické a prevádzkové vlastnosti riešenia, dokumentácie prevádzkových postupov a organizačného zabezpečenia prevádzky, nevyhnutného fyzického prístupu do priestorov, kde je zabezpečená podpora alebo prevádzka riešenia (technológie, ktorými poskytovateľ zabezpečuje poskytované služby), záznamov z prevádzky (listinná alebo elektronická podoba). Poskytovateľ sa zaväzuje viesť relevantné záznamy o prevádzke a výpadkoch systému. Poskytovateľ sa zaväzuje zabezpečiť realizáciu odporúčaní (zabezpečiť nápravu zistení) auditu v rozsahu a stanovenej lehote písomne odsúhlasenej objednávateľom a poskytovateľom.

2. Poskytovateľ sa zaväzuje mať najneskôr do 10 pracovných dní odo dňa nadobudnutia účinnosti tejto Zmluvy uzatvorené poistenie všeobecnej zodpovednosti za škodu s minimálnou poistnou sumou vo výške 100.000,- eur (slovom sto tisíc eur). Poistením musia byť kryté nároky všeobecnej zodpovednosti za škodu na veciach a na zdraví, vrátane ušlého zisku, spôsobené pri výkone činností poskytovateľa na základe tejto Zmluvy spôsobenej objednávateľovi alebo tretím osobám. Poskytovateľ je povinný kedykoľvek na písomnú výzvu objednávateľa preukázať v lehote 3 pracovných dní od doručenia písomnej výzvy objednávateľa splnenie povinnosti podľa tohto bodu Zmluvy. Porušenie ktorejkoľvek povinnosti poskytovateľa podľa tohto bodu Zmluvy sa považuje za podstatné porušenie tejto Zmluvy.

3. Poskytovateľ sa zaväzuje do 31. augusta 2030 dodať kompletnú a aktualizovanú dokumentáciu:

1) denník bezpečnostných zistení,
2) prevádzkový denníka SIEM, a to k vytvoreným novým use casom a vykonaným zmenám v existujúcich use casoch, ku konfigurácii použitých nástrojov tretích strán a k vytvoreným custom nástrojom a skriptom.

4. Poskytovateľ sa zaväzuje poskytovať predmet plnenia prostredníctvom kľúčových pracovníkov uvedených v zozname (Príloha 7 Zmluvy), t. j. fyzické osoby označené poskytovateľom, prostredníctvom ktorých poskytovateľ preukazoval splnenie podmienok účasti a fyzické osoby označené poskytovateľom, ktoré boli predmetom hodnotenia kritérií vo verejnom obstarávaní, ktorého výsledkom je táto Zmluva.

5. V prípade zmeny kľúčového pracovníka poskytovateľa uvedeného v Prílohe 7 tejto Zmluvy musí byť počas celej doby trvania Zmluvy zabezpečená minimálne rovnocenná úroveň odbornosti, kvalifikácie a skúseností, ktorú bude objednávateľ posudzovať rovnakým spôsobom, aký bol použitý pre účely vyhodnotenia ponúk vo verejnom obstarávaní zákazky, z ktorej vzišla táto Zmluva. Zmena v osobe kľúčového pracovníka sa vykonáva písomne, pričom nie je potrebné k takejto zmene uzatvoriť dodatok k Zmluve.

6. Nedodržanie týchto požiadaviek podľa bodu 4 tohto článku Zmluvy oprávňuje objednávateľa odstúpiť od tejto Zmluvy ku dňu doručenia písomného odstúpenia od Zmluvy z dôvodu podstatného porušenia Zmluvy.

ČLÁNOK IX
ZMLUVNÉ POKUTY

1. V prípade neposkytnutia predmetu plnenia v súlade so stanovenými požiadavkami, a to aj jednotlivou požiadavkou, na poskytované služby podľa Prílohy 1 Zmluvy, okrem Služby Monitoring bezpečnosti IT (SOC), Služby Monitoring a prevádzka MBIT (SIEM a NDR), Služby Rozvoj a optimalizácia MBIT a Služby „Forenzná analýza“, je objednávateľ oprávnený požadovať od poskytovateľa zmluvnú pokutu vo výške 300 eur bez DPH, a to za každé jednotlivé porušenie záväzku, pričom v prípade neposkytnutia Služby Monitoring bezpečnosti IT (SOC), Služby Monitoring a prevádzka MBIT (SIEM a NDR), Služby Rozvoj a optimalizácia MBIT alebo Služby „Forenzná analýza“ v súlade so stanovenými požiadavkami, a to aj jednotlivou požiadavkou podľa Prílohy 1 Zmluvy je objednávateľ oprávnený požadovať od poskytovateľa zmluvnú pokutu vo výške 1000 eur bez DPH, a to za každé jednotlivé porušenie záväzku. Zároveň sa minimálne raz opakované porušenie záväzku poskytovať Službu Monitoring bezpečnosti IT (SOC), Službu Monitoring a prevádzka MBIT (SIEM a NDR), Službu Rozvoj a optimalizácia MBIT alebo Službu

„Forenzná analýza“ v minimálnych podmienkach (aj čo i len jednej podmienke) upravených v Prílohe 1 tejto Zmluvy považuje za podstatné porušenie Zmluvy.

2. V prípade omeškania poskytovateľa s včasným plnením poskytovaných služieb podľa Časového harmonogramu uvedeného v Prílohe 1 Zmluvy, je objednávateľ oprávnený požadovať od poskytovateľa zmluvnú pokutu vo výške 0,5 % z príslušnej ceny predmetu plnenia bez DPH, s ktorým je v omeškaní za každý začatý deň omeškania.

3. Splatnosť zmluvných pokút v zmysle tejto Zmluvy je do 30 dní odo dňa doručenia príslušného daňového dokladu, ktorým zmluvná strana uplatňuje zaplatenie zmluvnej pokuty u druhej Zmluvnej strany.

4. V prípade omeškania platby za predmet plnenia má poskytovateľ právo fakturovať objednávateľovi úrok z omeškania vo výške určenej v zmysle § 369 ods. 2 Obchodného zákonníka.

5. Ak sa objednávateľ dostane do omeškania s úhradou faktúry po lehote jej splatnosti je poskytovateľ oprávnený od objednávateľa požadovať zaplatenie úroku z omeškania v sadzbe určenej nariadením vlády č. 21/2013 Z. z., ktorým sa vykonávajú niektoré ustanovenia Obchodného zákonníka.

6. Zaplatením zmluvnej pokuty nestráca druhá zmluvná strana nárok na náhradu škody vzniknutej porušením zmluvnej povinnosti.

7. Zodpovednosť za škodu vzniknutú zmluvným stranám v dôsledku porušenia tejto Zmluvy sa riadi ustanoveniami § 373 a nasl. Obchodného zákonníka.

ČLÁNOK X
MLČANLIVOSŤ

Poskytovateľ sa zaväzuje zabezpečiť, aby v súvislosti s poskytnutím predmetu plnenia nedošlo k sprístupneniu dát objednávateľa a jeho zamestnancov tretím stranám a rovnako sa zaväzuje k takému konaniu, ktoré bude minimalizovať kontakt s dátami na mieru čo najnižšiu, avšak postačujúcu k riadnemu plneniu tejto Zmluvy. Táto povinnosť mlčanlivosti sa vzťahuje aj na subdodávateľov poskytovateľa, nezaniká ani po ukončení tejto Zmluvy, nie je možné sa jej nijako zbaviť. V prípade porušenia tohto záväzku je poskytovateľ povinný uhradiť objednávateľovi Zmluvnú pokutu vo výške 10 000,- eur za každý dokázaný prípad zneužitia objednávateľových interných informácií a údajov, pričom uhradením pokuty nie je dotknutý nárok objednávateľa na náhradu škody. Táto Zmluvná pokuta je splatná do 30 dní od písomného oznámenia objednávateľa o zistení porušenia záväzku podľa tohto bodu Zmluvy.

ČLÁNOK XI
OSOBITNÉ USTANOVENIA

1. Poskytovateľ sa zaväzuje používať pri poskytovaní predmetu plnenia Trellix EDR (Endpoint Detection and Response). Zároveň sa poskytovateľ zaväzuje do 6 mesiacov od účinnosti Zmluvy mať minimálne tri (3) vyškolené osoby na technológiu Trellix EDR, čo na písomnú žiadosť objednávateľa preukáže kópiou jedným z týchto certifikátov: Trellix Certified Architect: Endpoint Detection and Response (EDR), Trellix Service Provider: Endpoint Detection and Response (EDR), Technical Specialist Certifications: Trellix Endpoint Security, Exam: Endpoint Detection and Response.

2. Všetky dokumenty, oznámenia, žiadosti, správy, výzvy, požiadavky a ostatné písomnosti určené druhej Zmluvnej strane (ďalej len „písomnosti“) musia byť doručené na adresu jej sídla, ak táto Zmluva neustanovuje inak, a to v listinnej podobe prostredníctvom pošty doporučene, pričom za deň doručenia sa považuje deň prevzatia zásielky, alebo osobne do sídla druhej Zmluvnej strany.

3. V prípade zmeny ktoréhokoľvek z údajov uvedených v záhlaví tejto Zmluvy alebo v kontaktných osobách Zmluvných strán podľa tejto Zmluvy je príslušná Zmluvná strana povinná túto zmenu bezodkladne písomne oznámiť druhej Zmluvnej strane. Ak Zmluvná strana nesplní túto

oznamovaciu povinnosť, platia posledné známe identifikačné údaje alebo aktuálne údaje podľa príslušného verejného registra.

4. V prípade, ak adresát odmietne písomnosť prevziať, za deň doručenia sa považuje deň odmietnutia prevzatia písomnosti. V prípade, ak si adresát neprevezme písomnosť v úložnej lehote na pošte, písomnosť sa považuje za doručenú dňom jej vrátenia odosielateľovi, a to aj vtedy, ak sa adresát o tom nedozvie. V prípade, ak sa písomnosť vráti odosielateľovi s označením pošty „adresát neznámy" alebo s inou poznámkou podobného významu, za deň doručenia sa považuje deň vrátenia zásielky odosielateľovi.

5. Poskytovateľ je povinný zabezpečiť komunikáciu so zamestnancami objednávateľa v súvislosti s plnením podľa tejto Zmluvy v slovenskom alebo českom jazyku.

6. V prípade podstatného porušenia Zmluvy poskytovateľom je objednávateľ oprávnený vykonať zmenu Zmluvy spočívajúcu v zmene osoby poskytovateľa, a to nahradením pôvodného poskytovateľa (ďalej len "Pôvodný poskytovateľ") novým poskytovateľom v súlade s § 18 zákona č. 343/2015 Z. z. Zmenu v osobe poskytovateľa je objednávateľ oprávnený vykonať nahradením pôvodného poskytovateľa subjektom, ktorý ako uchádzač vo Verejnom obstarávaní k zákazke s názvom „*Monitoring kybernetickej bezpečnosti*" splnil podmienky účasti, všetky požiadavky na predmet zákazky, vrátane splnenia povinností v zmysle súťažných podkladov vo Verejnom obstarávaní a umiestnil sa na druhom mieste v poradí v rámci Verejného obstarávania (ďalej len "Nový poskytovateľ"). Na vysporiadanie plnení medzi Pôvodným poskytovateľom a objednávateľom sa primerane aplikujú ustanovenia bodu 9 tohto článku Zmluvy. Na vysporiadanie plnení medzi Novým poskytovateľom a objednávateľom sa vykonajú primerané úpravy Zmluvy.

7. Poskytovateľ súhlasí s takouto zmenou Zmluvy, ak objednávateľ nahradí Pôvodného poskytovateľa Novým poskytovateľom podľa bodu 5 tohto článku Zmluvy. Poskytovateľ súhlasí s tým, že nadobudnutím účinnosti zmeny v osobe poskytovateľa prestáva byť zmluvnou stranou tejto Zmluvy a zmluvou stranou tejto Zmluvy sa stáva Nový poskytovateľ.

8. Pôvodný poskytovateľ je povinný bezodkladne, najneskôr do 10 pracovných dní od oznámenia objednávateľa za účelom zmeny Zmluvy podľa bodu 5 tohto článku Zmluvy poskytnúť objednávateľovi všetku potrebnú súčinnosť, najmä vykonať úkony, ktoré sú nevyhnutné na riadne plnenie Zmluvy do okamihu zmeny v osobe poskytovateľa, odovzdať objednávateľovi všetky potrebné informácie a dokumenty v súvislosti s dodaným plnením tak, aby nedošlo k vzniku škody alebo inej ujmy objednávateľovi.

9. V prípade omeškania Pôvodného poskytovateľa s plnením povinnosti podľa bodu 8 tohto článku Zmluvy (neposkytnutie súčinnosti) vzniká objednávateľovi za každý aj začatý deň omeškania nárok na zaplatenie Zmluvnej pokuty zo strany Pôvodného poskytovateľa vo výške 100 eur (slovom: sto eur). Povinnosť nahradiť škodu vzniknutú v dôsledku porušenia povinnosti zabezpečenej zmluvnou pokutou ostáva zaplatením Zmluvnej pokuty nedotknutá, a to aj v rozsahu prevyšujúcom zmluvnú pokutu.

10. V prípade odstúpenia od tejto Zmluvy si zmluvné strany ponechajú doposiaľ akceptované plnenia, vykonané v súlade s podmienkami uvedenými v Zmluve a jej prílohách a úhrady za ne. 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 zodpovedajúcej miere rozpracovanosti podľa dohody zmluvných strán.

11. Objednávateľ si vyhradzuje právo uplatniť opciu u poskytovateľa na: a) poskytovanie predmetu plnenia – Služby Monitoringu bezpečnosti IT za cenu, v rozsahu a podmienok upravených v tejto Zmluve, b) poskytovanie predmetu plnenia – Služby Monitoringu a prevádzka MBIT (SIEM a NDR) za cenu, v rozsahu a podmienok upravených v tejto Zmluve.

12. Pre zamedzenie pochybností, objednávateľ je oprávnený (nie povinný) uplatniť opciu, pričom opcia môže byť objednávateľom uplatnená u poskytovateľa najneskôr do uplynutia 24 mesiacov od účinnosti tejto Zmluvy.

13. Pokiaľ sa objednávateľ rozhodne využiť právo z opcie, je povinný tak urobiť písomným oznámením o uplatnení opcie doručeným poskytovateľovi prostredníctvom kontaktných osôb a ich kontaktných e-mailov podľa článku V tejto Zmluvy.

14. Objednávateľ si vyhradzuje právo uplatniť zmluvnú pokutu, ak poskytovateľ nedodrží záväzok poskytnúť služby v súlade s opciou uplatnenou objednávateľom podľa tejto zmluvy vo výške 15 000 eur bez DPH.

15. Poskytovateľ vyhlasuje, že osoba alebo osoby, ktoré sú v registri partnerov verejného sektora zapísané ako jeho koneční užívatelia výhod, nie sú osobami uvedenými v § 11 ods. 1 písm. c) zákona o verejnom obstarávaní, medzi ktoré patrí prezident Slovenskej republiky, člen vlády, vedúci ústredného orgánu štátnej správy, ktorý nie je členom vlády, vedúci orgánu štátnej správy s celoslovenskou pôsobnosťou, sudca Ústavného súdu Slovenskej republiky alebo sudca, generálny prokurátor Slovenskej republiky alebo prokurátor, verejný ochranca práv, predseda Najvyššieho kontrolného úradu Slovenskej republiky a podpredseda Najvyššieho kontrolného úradu Slovenskej republiky, štátny tajomník, generálny tajomník služobného úradu, prednosta okresného úradu, primátor hlavného mesta Slovenskej republiky Bratislavy, primátor krajského mesta alebo primátor okresného mesta a predseda vyššieho územného celku. Poskytovateľ tiež vyhlasuje, že v prípade, ak na plnenie tejto zmluvy použije subdodávateľa alebo subdodávateľov, ktorí majú povinnosť zapisovať sa do registra partnerov verejného sektora, tak tento subdodávateľ alebo títo subdodávatelia k dátumu podpisu tejto zmluvy nemajú v registri partnerov verejného sektora zapísaného konečného užívateľa výhod, ktorým je osoba podľa § 11 ods. 1 písm. c) zákona o verejnom obstarávaní.

ČLÁNOK XII
VYŠŠIA MOC

1. Za porušenie Zmluvy sa nepovažuje, ak ktorákoľvek zo zmluvných strán nemôže plniť svoje zmluvné povinnosti z dôvodu prekážky, ktorá nastala nezávisle od vôle povinnej zmluvnej strany a bráni jej v splnení jej povinnosti, ak nemožno rozumne predpokladať, že by povinná zmluvná strana túto prekážku alebo jej následky odvrátila alebo prekonala, a že by v čase vzniku záväzku túto prekážku predvídala (napr. vojna, celoštátny štrajk, zemetrasenie, záplava, požiar, teroristický útok, havária počas transportu).

2. Pokiaľ sa zmluvné strany písomne nedohodnú inak, zmluvne dohodnuté termíny sa predlžujú o dobu trvania okolností vylučujúcich zodpovednosť (vis maior). Na požiadanie zmluvnej strany, ktorej boli oznámené okolnosti vyššej moci je povinná dotknutá zmluvná strana predložiť hodnoverný dôkaz. Poskytovateľ je povinný preukázať nepriaznivé poveternostné podmienky písomným potvrdením Slovenského hydrometeorologického ústavu.

ČLÁNOK XIII
ZÁVEREČNÉ USTANOVENIA

1. Vzájomné práva a povinnosti zmluvných strán sú tiež upravené vo všeobecných podmienkach uvedených v Prílohe 1 Zmluvy. V prípade rozporu medzi ustanoveniami tejto Zmluvy a ustanoveniami uvedenými vo všeobecných podmienkach majú odchylné ustanovenia tejto Zmluvy prednosť.

2. Táto Zmluva môže byť menená v súlade s príslušnými ustanoveniami zákona o verejnom obstarávaní.

3. Písomné zmeny Zmluvy sa vykonávajú formou písomných a očíslovaných dodatkov, ktoré budú schválené a podpísané oprávnenými zástupcami oboch Zmluvných strán, ak nie je v Zmluve uvedené inak.

4. Pojmy, výrazy, skratky uvedené v Zmluve a v jej prílohách, pokiaľ z obsahu Zmluvy nevyplýva niečo iné, majú význam definovaný v Prílohe 4 - Slovník pojmov, ktorá tvorí neoddeliteľnú súčasť Zmluvy.

5. Zmluva je uzavretá podľa právneho poriadku Slovenskej republiky, pričom práva, povinnosti a vzťahy Zmluvných strán v tejto Zmluve neupravené sa budú spravovať príslušnými ustanoveniami zákona č. 513/1991 Zb. Obchodného zákonníka v znení neskorších predpisov a ďalších všeobecne záväzných právnych predpisov.

6. Zmluvné strany sa zaväzujú, že budú postupovať v súlade s oprávnenými záujmami druhej strany a že vykonajú všetky právne úkony, ktoré sa ukážu byť nevyhnutné pre realizáciu činností upravených touto Zmluvou. Záväzok súčinnosti sa vzťahuje len na také úkony, ktoré prispejú alebo majú prispieť k dosiahnutiu účelu tejto Zmluvy.

7. Poskytovateľ sa zaväzuje prípadné zmeny právneho stavu, ktoré by mohli mať vplyv na plnenie podmienok tejto Zmluvy, oznámiť písomne druhej zmluvnej strane najneskôr 30 dní pred predpokladanou zmenou..

8. V prípade sporného výkladu ustanovení tejto Zmluvy alebo neplnenia záväzkov zmluvných strán sa obidve zmluvné strany budú snažiť prednostne dosiahnuť vzájomnú dohodu. Pokiaľ sa zmluvné strany nedohodnú, budú sa snažiť dosiahnuť súdny zmier. Prípadné spory týkajúce sa výkladu a realizácie tejto Zmluvy budú riešené vecne a miestne príslušnými súdmi Slovenskej republiky.

9. V prípade rozporu medzi ustanoveniami tejto Zmluvy a dispozitívnymi ustanoveniami všeobecne záväzných právnych predpisov právneho poriadku Slovenskej republiky, platia ustanovenia tejto Zmluvy. V prípade rozporu medzi ustanoveniami tejto Zmluvy a ustanoveniami všeobecne záväzných právnych predpisov právneho poriadku Slovenskej republiky, ktoré je možné dohodou zmluvných strán vylúčiť, platia ustanovenia tejto Zmluvy a uvedené ustanovenia všeobecne záväzných právnych predpisov právneho poriadku Slovenskej republiky sa považujú za výslovne vylúčené.

10. V prípade, ak sa niektoré ustanovenie tejto Zmluvy stane neplatným, neúčinným alebo nevykonateľným, nie sú tým dotknuté ostatné ustanovenia tejto Zmluvy. Príslušné ustanovenie Zmluvy sa nahradí takým platným a účinným zákonným ustanovením, ktoré je mu svojím významom a účelom najbližšie.

11. Objednávateľ pri spracúvaní osobných údajov, poskytnutých poskytovateľom pre účely plnenia tejto Zmluvy, postupuje v súlade so zákonom č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov a nariadenia Európskeho parlamentu a Rady (EÚ) č. 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. Informácia o podmienkach spracúvania osobných údajov dotknutých osôb je zverejnená na webovom sídle objednávateľa: https://www.nbs.sk/sk/ochrana-osobnych-udajov.

12. Táto Zmluva je vyhotovená a uzavretá v (4) štyroch rovnopisoch, pričom objednávateľ dostane (3) tri rovnopisy a poskytovateľ dostane (1) jeden rovnopis. Všetky rovnopisy sú považované za rovnocenné.

13. Táto Zmluva (vrátane jej prípadných dodatkov) patrí medzi povinne zverejňované Zmluvy podľa ustanovení § 5a zákona o slobodnom prístupe k informáciám (zákona č. 211/2000 Z. z. v znení neskorších predpisov) v spojení s ustanoveniami § 1 ods. 2 Obchodného zákonníka a ustanoveniami § 47a Občianskeho zákonníka (zákona č. 40/1964 Zb. v znení neskorších predpisov). Poskytovateľ berie na vedomie zverejnenie tejto Zmluvy (vrátane jej prípadných dodatkov) a faktúr poskytovateľa doručených objednávateľovi, a to zverejnenie objednávateľom počas trvania jeho povinnosti podľa § 5a ods. 1, 7 a 10 a § 5b zákona o slobodnom prístupe k informáciám.

14. Táto Zmluva nadobúda platnosť a je pre Zmluvné strany záväzná odo dňa jej podpísania oprávnenými zástupcami oboch Zmluvných strán; ak oprávnení zástupcovia oboch Zmluvných strán nepodpíšu túto Zmluvu v ten istý deň, tak rozhodujúci je deň neskoršieho podpisu. Táto Zmluva nadobúda účinnosť dňom nasledujúcim po dni jej zverejnenia na webovom sídle (internetovej stránke) objednávateľa v súlade s § 47a ods. 1 Občianskeho zákonníka v spojení s § 1 ods. 2 Obchodného zákonníka a s § 5a ods. 1, 6 a 9 zákona o slobodnom prístupe k informáciám.

15. Neoddeliteľnou súčasťou tejto Zmluvy sú prílohy:
Príloha 1: Špecifikácia poskytovaných služieb a ich štandardy
Príloha 2: Všeobecné podmienky Zmluvy
Príloha 3: Špecifikácia ceny poskytovaných služieb
Príloha 4: Slovník pojmov
Príloha 5: Zoznam subdodávateľov
Príloha 6: Rámcový plán
Príloha 7: Zoznam kľúčových pracovníkov poskytovateľa
Príloha 8: Vzor výkazu

Za objednávateľa:
Národná banka Slovenska
V Bratislave, dňa 30.7.2025

.....
xxx

Za poskytovateľa:
ANECT a.s.
V Bratislave, dňa 24.7.2025

.....
xxx

Príloha 2 k zmluve č. C-NBS1-000-106-915

Všeobecné podmienky k Zmluve

(ďalej aj „všeobecné podmienky“, alebo „podmienky“)

A. Tieto všeobecné podmienky tvoria ako Príloha 2 neoddeliteľnú súčasť Zmluvy na poskytovanie služieb IT monitoring bezpečnosti č. C-NBS1-000-106-915.
(ďalej len „zmluva“).

B. Všeobecné podmienky obsahujú časť obsahu zmluvy v zmysle ustanovení § 273 zákona č. 513/1991 Z. z. Obchodný zákonník v znení neskorších predpisov.

C. Odchylné dojednania v Zmluve majú prednosť pred ustanoveniami uvedenými v týchto všeobecných podmienkach.

Článok I
Zdrojový kód

1. V prípade, ak v zmluve nie je upravené inak a v prípade ak je výsledkom poskytovaných služieb autorské dielo majúce povahu počítačového programu, tak platí, že objednávateľ bezodkladne odovzdá, po dodaní dodaného informačného systému podľa zmluvy o dielo a uzatvorení tejto zmluvy poskytovateľovi, výlučnú kontrolu nad funkčným vývojovým a produkčným prostredím dodaného informačného systému, vrátane jeho úplného, aktuálneho zdrojového kódu, a to na základe písomného preberacieho protokolu.
2. Poskytovateľ zároveň umožní objednávateľovi prístup na verziu vývojovej časti dodaného informačného systému určenú len na čítanie („read only“), z ktorej nie je možné vstupovať do žiadneho z prostredí dodaného informačného systému.
3. Poskytovateľ sa zaväzuje odovzdať objednávateľovi funkčné vývojové a produkčné prostredie, vrátane úplného aktuálneho zdrojového kódu pri ukončení tejto zmluvy.
4. Úplný zdrojový kód sa skladá zo zdrojového kódu každého počítačového programu tvoriaceho dodaný informačný systém, ktorý bol poskytovateľom vytvorený pri plnení podľa zmluvy (ďalej ako „vytvorený zdrojový kód“) a zo zdrojového kódu každého počítačového programu vytvoreného nezávisle od diela dodaného zmluvou (ďalej ako „preexistentný zdrojový kód“).
5. Poskytované služby v rámci plnenia zmluvy môžu zahŕňať poskytovateľove vytvorenie nasledovného, vopred definovaného, a od zvyšku dodaného informačného systému, oddeliteľného, modulu (časť), ktorý je bez úpravy použiteľný aj tretími osobami, aj na iné alebo podobné účely, ako je účel vyplývajúci z tejto zmluvy.
6. Zdrojový kód musí byť v podobe, ktorá zaručuje možnosť overenia, že je kompletný a v správnej verzii, tzn. umožňujúcej kompiláciu, inštaláciu, spustenie a overenie funkcionality, a to vrátane kompletnej dokumentácie zdrojového kódu (napr. interfejsov a pod.) takejto časti dodaného informačného systému. Zdrojový kód dodaný poskytovateľom musí byť bez obfuskácie.
7. Povinnosti poskytovateľa uvedené v tomto článku zmluvy sa primerane použijú aj pre akékoľvek opravy, zmeny, doplnenia, upgrade alebo update zdrojového kódu jednotlivého čiastkového plnenia tvoriaceho dodaný informačný systém, ku ktorému dôjde pri plnení tejto zmluvy alebo v rámci záručných opráv (ďalej len „zmena zdrojového kódu“). Dokumentácia zmeny zdrojového kódu musí obsahovať podrobný popis a komentár každého zásahu do zdrojového kódu.

Článok II
Preberacie podmienky

1. O prevzatí poskytnutých Poskytovaných služieb objednávateľom zmluvné strany vyhotovia písomný odovzdávací a preberací protokol, ktorý bude dokladom o splnení predmetu plnenia. Odovzdávací a preberací protokol musí byť podpísaný zástupcami oboch zmluvných strán (oprávnenými osobami).
2. Poskytovateľ je povinný najneskôr v deň ukončenia poskytnutých Poskytovaných služieb odovzdať objednávateľovi všetky doklady v slovenskom jazyku, potrebné na prevzatie poskytnutej služby.
3. Poskytnutie Poskytovaných služieb sa považuje za splnené až po overení kvality poskytnutej služby a úplnosti sprievodných dokladov. V prípade ich nesúladu s písomnou objednávkou má objednávateľ právo poskytnutú službu odmietnuť.
4. Vady poskytnutia Poskytovaných služieb sa delia do nasledovných skupín:
   a) za zásadné vady sa považuje, ak sa výsledok poskytnutých Poskytovaných služieb alebo primárne časti vytvoreného výsledku nedajú využívať pre pôvodne plánovaný účel definovaný v zmluve alebo spôsobujú nepoužiteľnosť dodaného informačného systému na stanovený účel;
   b) o menej zásadné vady ide v prípadoch, ak je funkcia a plánovaná použiteľnosť poskytnutých Poskytovaných služieb odlišná od špecifikácie a požiadaviek podľa tejto zmluvy, avšak nie je podstatne ovplyvňované pôvodne plánované použitie vytvoreného výsledku. Menej zásadné vady poskytovateľ odstráni úpravou.
5. Výskyt menej zásadných vád nebráni akceptácii Poskytovaných služieb. Poskytovateľ sa zaväzuje menej zásadné vady odstrániť v lehote dohodnutej oboma zmluvnými stranami, ktorá môže byť

dohodnutá ako kratšia než 7 pracovných dní, ktorá je určená pri vadách všeobecne a to úpravou alebo zmenou verzie v zmysle dodatočného zlepšenia.

6. V prípade výskytu zásadných vád k akceptácii Poskytovaných služieb nedochádza a zmluvné strany sa zaväzujú určiť ďalší postup vzájomnou dohodou. Výskyt podstatných vád sa považuje za podstatné porušenie zmluvy.
7. Postup akceptácie jednotlivých Poskytovaných služieb je upravený v príslušnej prílohe zmluvy.
8. Poskytovateľ sa zaväzuje prípadné vady Poskytovaných služieb odstrániť bezodplatne, bez zbytočného odkladu najneskôr však do 7 pracovných dní po uplatnení oprávnenej reklamácie objednávateľom. Objednávateľ sa zaväzuje, že prípadnú reklamáciu vady služby uplatní bezodkladne po jej zistení písomnou formou. Objednávateľ a poskytovateľ sa môžu písomne dohodnúť na dlhšej lehote na odstránenie vád služby.
9. Reklamácia sa považuje za vybavenú odstránením vady Poskytovaných služieb alebo jej časti riadne a včas, s potvrdením zo strany objednávateľa o prevzatí opravenej služby alebo jej časti formou preberacieho protokolu.
10. Poskytovateľ vyhlasuje, že ním poskytnutá služba nie je zaťažená právami tretích osôb.
11. Nebezpečenstvo škody a vlastnícke právo ku všetkým častiam plnenia poskytovateľa na základe tejto zmluvy prechádza na objednávateľa dňom akceptácie príslušnej služby.

Článok III
Záruka a odstraňovanie vád

1. Poskytovateľ zodpovedá za to, že Poskytované služby poskytnuté na základe tejto zmluvy budú mať vlastnosti a funkcionalitu požadovanú objednávateľom, budú poskytnuté v dohodnutom čase a ich poskytnutím nebude ohrozená prevádzka dodaného informačného systému.
2. Poskytovateľ zodpovedá za to, že poskytnuté Poskytované služby sú ku dňu podpisu akceptačného protokolu a počas záručnej doby bez vád.
3. Záručná doba na Poskytované služby dodané poskytovateľom, je 24 (dvadsaťštyri) mesiacov odo dňa podpisu akceptačného protokolu. Nároky z vád je objednávateľ povinný oznámiť bez zbytočného odkladu.
4. Poskytovateľ zaručuje, že poskytnuté Poskytované služby v čase ich poskytnutia/odovzdania nemajú vecné a právne vady, predovšetkým nie sú zaťažené právami tretích osôb z autorského alebo iného práva duševného vlastníctva.
5. Objednávateľ je oprávnený požadovať od poskytovateľa bezplatné a bezodkladné odstránenie vady na ktorú sa vzťahuje záruka podľa tejto zmluvy. Lehota na odstránenie vady sa stanovuje na 7 pracovných dní odo dňa ich písomného uplatnenia. Na uplatnenia tohto nároku sa použije IS Service Desk objednávateľa, ak sa zmluvné strany písomne nedohodnú inak. Poskytovateľ je povinný prijatie nahlásenia vady bez zbytočného odkladu potvrdiť. Zmluvné strany sa zaväzujú potvrdiť odstránenie vady v zápisnici o odstránení vady podpísanej oboma zmluvnými stranami, v ktorej uvedú aj predmet vady, spôsob a čas jej odstránenia, alebo prostredníctvom IS Service Desk objednávateľa.
6. Nároky z vád sa nedotýkajú nároku na náhradu škody a nároku na zmluvnú pokutu.
7. Za účelom odstránenia pochybností sa stanovuje, že treba rozlišovať medzi:
   a) vadou dodaného informačného systému (diela), ktorá bola spôsobená nezávisle od poskytnutých Poskytovaných služieb v zmysle tejto zmluvy, na ktorú sa vzťahuje záručná doba v zmysle zmluvy o dielo a práva a povinnosti zmluvných strán sa budú riadiť zmluvou o dielo;
   b) vadou Poskytovaných služieb spôsobenou neposkytnutím Poskytovaných služieb podľa tejto zmluvy riadne (napr. vada služby spôsobí nefunkčnosť dodaného informačného systému alebo iného diela zodpovedajúcu vade úrovne a alebo b), a v takom prípade sa budú práva a povinnosti zmluvných strán v súvislosti s takou vadou riadiť touto zmluvou.

Článok IV
Oprávnené osoby

1. Poskytovateľ sa zaväzuje do piatich (5) pracovných dní od podpisu tejto zmluvy vymenovať oprávnenú osobu, ktorá bude počas trvania tejto zmluvy oprávnená konať za poskytovateľa v

záležitostiach súvisiacich s plnením tejto zmluvy, a v tej istej lehote písomne oznámiť objednávateľovi jej meno a kontaktné údaje.

2. Objednávateľ sa zaväzuje do piatich (5) pracovných dní od podpisu tejto zmluvy vymenovať oprávnenú osobu, ktorá bude počas účinnosti tejto zmluvy oprávnená konať za objednávateľa v záležitostiach súvisiacich s plnením tejto zmluvy, a v tej istej lehote písomne oznámiť objednávateľovi jej meno a kontaktné údaje.
3. Prostredníctvom určených oprávnených osôb zmluvné strany:
   a) uskutočnia všetky organizačné záležitosti s ohľadom na všetky aktivity a činnosti súvisiace s plnením podľa tejto zmluvy;
   b) zabezpečia koordináciu jednotlivých aktivít a činností zmluvných strán súvisiacich s plnením podľa tejto zmluvy;
   c) sledujú priebeh plnenia tejto zmluvy;
   d) navrhujú potrebné zmeny technických riešení a technickej povahy v zmysle tejto zmluvy;
   e) zabezpečia vzájomnú spoluprácu a súčinnosť,
   f) vzdialene pristupujú k IKT (informačným a komunikačným technológiám) objednávateľa v mene poskytovateľa.
4. Každá zo zmluvných strán môže zmeniť oprávnené osoby. Takáto zmena je účinná dňom doručenia písomného oznámenia (prednostne kontaktným e-mailom) o zmene obsahujúceho aj meno a kontaktné údaje novej oprávnenej osoby druhej zmluvnej strane.
5. V prípade vzniku konfliktu alebo rozporov medzi oprávnenými osobami objednávateľa a poskytovateľa je ktorákoľvek z dotknutých strán povinná neodkladne eskalovať takúto situáciu na nadriadené autority:
   a. V prípade Objednávateľa je to riaditeľ odboru informačných technológií (OIT), ktorý má rozhodovaciu právomoc v rozsahu podpory a prevádzky predmetnej služby,
   b. V prípade Poskytovateľa je to štatutárny zástupca, ktorý má rozhodovaciu právomoc v prebiehajúcom zmluvnom vzťahu.
6. Komunikačný kanál pre eskaláciu takejto kritickej situácie sú oprávnené osoby, ktoré majú povinnosť uvedenú skutočnosť neodkladne predložiť svojim nadriadeným.
7. Eskalačná procedúra:
   a. Konflikt, resp. rozpor bude vyriešený vzájomnou dohodou v rozsahu aktuálne platnej zmluvy
   b. Konflikt, resp. rozpor bude vyriešený vzájomnou dohodou nad rámec aktuálne platnej zmluvy a bude iniciované konanie na uzatvorenie dodatku zmluvy na strane Objednávateľa aj Poskytovateľa
   c. Konflikt, resp. rozpor nie je možné vyriešiť vzájomnou dohodou a bude postúpený na riešenie súdnou cestou na strane Objednávateľa aj Poskytovateľa v súlade s platnou legislatívou SR

Článok V
Vzdialený prístup

1. Objednávateľ umožní poskytovateľovi vzdialený prístup k dodanému informačnému systému s využitím systému pre vzdialený prístup objednávateľa. Tento vzdialený prístup bude pre poskytovateľa zriadený v nevyhnutnom rozsahu, v ktorom je potrebný na plnenie tejto zmluvy.
2. Poskytovateľ bude využívať vzdialený prístup v dňoch a časoch, ako je stanovené v popisoch pre dostupnosť služieb v prílohe č. 2 tejto zmluvy a to výlučne na realizáciu Poskytovaných služieb poskytovaných poskytovateľovom na základe tejto zmluvy.
3. Objednávateľ poskytuje vzdialený prístup pre poskytovateľa bez akýchkoľvek záruk a vyhradzuje si právo dočasne prerušiť poskytovanie vzdialeného prístupu v prípade podozrenia na jeho zneužitie alebo aj bez udania dôvodu. Takéto prerušenie poskytovania vzdialeného prístupu nemôže byť chápané ako prekážka vo výkone poskytovania vzdialeného prístupu alebo porušenie tejto zmluvy a poskytovateľ si z tohto titulu nemôže nárokovať akúkoľvek náhradu škody alebo zľavy v ostatných zmluvných vzťahoch medzi objednávateľom a poskytovateľom.
4. Objednávateľ poskytuje poskytovateľovi podporu pre systém pre vzdialený prístup v pracovných dňoch v čase 8:00 h až 16:00 h.

5. Poskytovateľ je oprávnený požiadať o zriadenie prístupového účtu externého používateľa pre osoby prostredníctvom ktorých poskytuje Poskytované služby a pre oprávnené osoby.
6. Poskytovateľ je oprávnený požiadať o vzdialený prístup k IKT objednávateľa prostredníctvom kontaktnej osoby stanovenej podľa článku IV týchto všeobecných podmienok. Schvaľovanie vzdialeného prístupu externého používateľa prebieha podľa osobitných vnútorných právnych predpisov objednávateľa, s ktorými bude poskytovateľ oboznámený.
7. Poskytovateľ sa zaväzuje, že zabezpečí, aby externí používatelia pri vzdialenom prístupe dodržiavali všetky zmluvné a všeobecne záväzné právne predpisy vzťahujúce sa k vzdialenému prístupu k IKT objednávateľa. Poskytovateľ sa ďalej zaväzuje, že po nadobudnutí účinnosti tejto zmluvy sa riadne a preukázateľne oboznámi so všetkými relevantnými vnútornými právnymi predpismi objednávateľa týkajúcimi sa informačnej bezpečnosti.
8. Poskytovateľ sa zaväzuje, že zabezpečí, aby jeho externí používatelia dodržiavali povinnosti externých používateľov uvedené v tomto bode. Externý používateľ je povinný:
   a) dodržiavať pravidlá a postupy podľa bodu 10. až 16. tohto článku,
   b) požiadať kontaktnú osobu objednávateľ o neodkladné zablokovanie svojho prístupového účtu v prípade výskytu akejkoľvek udalosti, v dôsledku ktorej by mohlo dôjsť k zneužitiu vzdialeného prístupu zriadeného externému používateľovi,
   c) pri výskyte závažnej udalosti týkajúcej sa chránených informácií neodkladne informovať kontaktnú (oprávnenú) osobu objednávateľa,
   d) upozorniť kontaktnú osobu objednávateľa na zistené nedostatky, ktoré sa vyskytnú počas vzdialeného prístupu,
   e) poskytnúť súčinnosť pri riešení incidentov týkajúcich sa vzdialeného prístupu,
   f) vrátiť hardvérový token alebo iný fyzický prostriedok, ktorý mu bol pridelený pri zriadení používateľského účtu a ktorý sa využíva pre potreby viacfaktorovej autentifikácie, pri zrušení alebo ukončení využívania vzdialeného prístupu.
9. Porušenie záväzkov poskytovateľa uvedených (aj jednotlivo určených) v bodoch , 7., 8., 11., 12., 13., 14., 15., 16., 17. tohto článku zmluvy sa považuje za podstatné porušenie tejto zmluvy.
10. Zmluvné strany sa dohodli, že zriadenie a prevádzka prístupových účtov pre externých používateľov poskytovateľa sa nespoplatňuje. Vzdialený prístup nie je zo strany poskytovateľa nárokovateľný a poskytovateľ rešpektuje právo objednávateľa zriaďovať vzdialené prístupy v rozsahu, ktorý objednávateľ považuje za potrebný.
11. Externý používateľ pri využívaní vzdialeného prístupu postupuje podľa používateľskej dokumentácie, ktorá mu bude dodaná po zriadení jeho prístupového účtu. Dokumentácia obsahuje:
   a) Postup pre kontrolu výpočtovej techniky pred pripojením,
   b) Postup pre vzdialené pripojenie a odpojenie,
   c) Postup pre nahlasovanie incidentov,
   d) Poučenie používateľov vzdialeného prístupu.
12. Externý používateľ smie na vzdialené pripojenie do NBS používať iba schválenú výpočtovú techniku uvedenú v žiadosti o zriadenie/zrušenie prístupového účtu externého používateľa s aktualizovaným operačným systémom a inštalovaným a aktuálnym antivírusovým softvérom.´
13. Nie je dovolené vzdialene sa pripájať k IKT objednávateľa z výpočtovej techniky, ktorá obsahuje alebo obsahovala počítačový vírus alebo škodlivý softvér, o ktorom bol externý používateľ notifikovaný antivírusovým softvérom a ktorý nebol odborne odstránený.
14. Externý používateľ nesmie hardvérový token, alebo iný fyzický prostriedok, ktorý sa využíva pre potreby viacfaktorovej autentifikácie poskytnúť inej osobe a je povinný v najkratšom možnom čase ohlásiť jeho stratu alebo odcudzenie kontaktnej osobe objednávateľa.
15. Externý používateľ nesmie počas využívania vzdialeného prístupu opustiť pripojenú výpočtovú techniku, dovoliť iným osobám prístup k tejto technike, alebo sledovanie jej aktívnej obrazovky.
16. Externý používateľ smie vzdialene pristupovať výhradne k IS a infraštruktúram IS, ktoré sú definované v bode 1 tohto článku.
17. Externý používateľ nesmie na virtuálne PC inštalovať žiadny dodatočný softvér. V prípade potreby inštalácie dodatočného softvéru na virtuálne PC o jej vykonanie požiada kontaktnú osobu objednávateľa.

18. Poskytovateľ sa zaväzuje, že vráti objednávateľovi všetky technické prostriedky a vybavenie, ktoré mu boli zo strany objednávateľa poskytnuté za účelom vzdialeného prístupu, najneskôr do 5 dní od dňa ukončenia platnosti tejto zmluvy.

19. V prípade nedodržania záväzku poskytovateľa podľa bodu 18., bude objednávateľ oprávnený uplatniť voči poskytovateľovi zmluvnú pokutu, ktorú sa poskytovateľ zaväzuje uhradiť. Zmluvná pokuta sa vypočíta ako súčin poplatku 200 eur s DPH (ktorý pokrýva náklady objednávateľa na technické vybavenie jedného používateľa) a počtu používateľov poskytovateľa.

20. Poskytovateľ sa zaväzuje objednávateľovi uhradiť zmluvnú pokutu do 14 pracovných dní od doručenia písomného uplatnenia zmluvnej pokuty (výzvou resp. doručením faktúry) zo strany objednávateľa. Čiastku zmluvnej pokuty uhradí poskytovateľ objednávateľovi bezhotovostným prevodom. Údaje pre vykonanie bezhotovostného prevodu zmluvnej pokuty oznámi objednávateľ poskytovateľovi v písomnom uplatnení zmluvnej pokuty.

Článok VI
Informačná bezpečnosť

1. Poskytovateľ sa v súvislosti s plnením predmetu tejto zmluvy zaväzuje dodržiavať pri podpore prevádzky dodaného informačného systému bezpečnostnú politiku objednávateľa a objednávateľom vydané platné bezpečnostné smernice a štandardy.

2. Oprávnené osoby a pracovníci poskytovateľa, ktorí budú vykonávať pre objednávateľa činnosti súvisiace s plnením tejto zmluvy, musia byť poučení o povinnostiach podľa predchádzajúceho bodu tohto článku a o tomto poučení musí poskytovateľ vytvoriť záznam, ktorý bude podpísaný poučenou osobou a osobou, ktorá poučenie vykonala. Za riadne poučenie zodpovedá poskytovateľ. Poskytovateľ je povinný predložiť objednávateľovi potvrdenie o oboznámení zamestnancov a subdodávateľov s platnými bezpečnostnými štandardmi objednávateľa, a to podľa vzoru objednávateľa, ak poskytovateľovi takýto vzor poskytne.

3. Poskytovateľ sa zaväzuje v priebehu trvania podpory prevádzky priebežne sledovať a vyhodnocovať bezpečnosť a odolnosť dodaného informačného systému voči aktuálne známym typom útokov, resp. poskytovať súčinnosť objednávateľovi pri zaisťovaní bezpečnosti odolnosti.

4. Poskytovateľ sa zaväzuje v priebehu trvania podpory prevádzky pred odovzdaním akejkoľvek zmeny dodaného informačného systému vykonať testovanie na prítomnosť známych zraniteľnosti. V prípade zistenia zraniteľností sa poskytovateľ zaväzuje tieto zraniteľnosti odstrániť, vykonať opätovné testovanie a zdokumentovaný výsledok testovania odovzdať objednávateľovi v súlade s bezpečnostnými štandardmi objednávateľa.

5. Poskytovateľ sa zaväzuje poskytnúť objednávateľovi kontaktnú osobu zodpovednú za kybernetickú bezpečnosť poskytovateľa.

6. Objednávateľ je oprávnený zaslať kontaktnej osobe poskytovateľa informácie ohľadom podozrení na bezpečnostne relevantné udalosti týkajúce sa poskytovateľa.

7. Objednávateľ je oprávnený na zisťovanie stavu kybernetickej bezpečnosti poskytovateľa použiť služby tretích strán.

8. Objednávateľ je oprávnený zbierať informácie o kybernetickej bezpečnosti IT prostredia poskytovateľa bez predchádzajúceho upozornenia a oznámenia rozsahu a spôsobu zisťovania.

9. Poskytovateľ poskytne objednávateľovi písomné vyjadrenie k odstráneniu príčin problémov v oblasti kybernetickej bezpečnosti.

10. V prípade kritických nedostatkov v kybernetickej bezpečnosti musí poskytovateľ zabezpečiť bezodkladnú nápravu nedostatkov. Každý takýto kritický nedostatok v kybernetickej bezpečnosti bude evidovaný, riadený, sledovaný a vyhodnocovaný ako závažný bezpečnostný incident.

11. Poskytovateľ sa zaväzuje informovať objednávateľa o každom svojom závažnom bezpečnostnom incidente.

12. Poskytovateľ sa zaväzuje vytvoriť, aplikovať a dodržiavať písomne vypracované pravidlá bezpečného vývoja počas celej doby trvania zmluvného vzťahu a na požiadanie ich bezodkladne poskytnúť NBS.

13. Poskytovateľ sa zaväzuje, že jeho zamestnanci a osoby ktoré sa podieľajú na tvorbe a úpravách zdrojových kódov sú preukázateľne regulárne vyškolení na bezpečný vývoj aplikácií.

14. Pravidlá bezpečného vývoja aplikácií obsahujú oblasti podľa "best practices", ako napr. komentáre, funkčné testovanie, predchádzanie typickým bezpečnostným chybám, pravidelné bezpečnostné testovanie kódu integrované do procesu vývoja.
15. Objednávateľ je oprávnený posúdiť pravidlá bezpečného vývoja aplikácií poskytovateľa prostredníctvom tretej strany.
16. Poskytovateľ sa zaväzuje dodržiavať štandardy stanovené objednávateľom a zakomponovať ich do svojich pravidiel bezpečného vývoja aplikácií pre dodaný informačný systém a zmeny dodaného informačného systému poskytované pre objednávateľa.
17. Ak odovzdávané dielo/zmena dodaného informačného systému obsahuje bezpečnostné nedostatky, ktoré sú klasifikované objednávateľom ako zásadný bezpečnostný incident, tak toto dielo/zmena nebude prevzaté do prevádzky objednávateľa, kým nebudú uvedené bezpečnostné nedostatky primerane odstránené, resp. ošetrené.
18. Objednávateľ je oprávnený vykonávať preverenie bezpečnosti diela, pričom poskytovateľ sa zaväzuje poskytnúť potrebnú súčinnosť (napr. dokumentáciu, vysvetlenia). Objednávateľ je oprávnený na preverenie bezpečnosti diela/zmeny použiť služby tretích strán.

Článok VII
Ochrana dôverných informácií

1. Dôverné informácie sú všetky informácie sprístupnené, poskytnuté objednávateľom poskytovateľovi počas trvania zmluvy, ktoré nie sú verejne prístupné, a to najmä technické, obchodné, finančné alebo všetky iné informácie, ktoré objednávateľ poskytne poskytovateľovi v akejkoľvek podobe či už zachytené hmotne alebo ústne poskytnuté, ako aj informácie prijaté od inej osoby ako je objednávateľ, pokiaľ je táto osoba zaviazaná s nimi nakladať ako s dôvernými (ďalej len „dôverné informácie").
2. Dôvernými informáciami nie sú informácie, ktoré sú, alebo sa následne stanú verejne dostupnými inak ako porušením povinností podľa tejto zmluvy poskytovateľom, verejne dostupnými sa stávajú dňom zverejnenia.
3. Poskytovateľ sa zaväzuje:
   - dodržiavať a prijať zodpovedajúce technické, organizačné a iné opatrenia potrebné na ochranu dôverných informácií v rozsahu ako je primerane obvyklé za účelom zabezpečenia neoprávneného pozmenenia, zničenia, straty, odcudzenia, zverejnenia, zneužitia alebo neoprávneným sprístupnením neoprávnenej osobe (ďalej ako „neoprávnená manipulácia s dôvernými informáciami"),
   - dôverné informácie viesť od iných dôverných informácií, ktorými disponuje, aby sa predišlo ich zmiešaniu alebo zámene,
   - bezodkladne oznámiť objednávateľovi každú neoprávnenú manipuláciu s dôvernými informáciami a zabezpečiť obnovu všetkých opatrení na ochranu dôverných informácií v zmysle tejto zmluvy.
4. Poskytovateľ je oprávnený využívať dôverné informácie iba pre účely plnenia zmluvy a po jej skončení nesmie bez akéhokoľvek časového obmedzenia použiť dôverné informácie na akýkoľvek účel. Likvidáciu dôverných informácií zabezpečí poskytovateľ v súlade s článkom IX bod 18 všeobecných podmienok.
5. Poskytovateľ nie je oprávnený dôverné informácie poskytnúť inej osobe, ako zamestnancom, oprávneným osobám poskytovateľa a subdodávateľom ustanovenými v súlade s ustanoveniami tejto zmluvy, ak ďalej nie je uvedené inak. Zároveň je povinný zaviazať všetky takéto osoby záväzkami mlčanlivosti a nakladania s dôvernými informáciami minimálne v rozsahu ako je zaviazaný sám touto zmluvou.
6. Poskytovateľ je oprávnený poskytnúť dôverné informácie v nevyhnutnom rozsahu:
   - príslušnému súdnemu, správnemu orgánu v súvislosti s akýmkoľvek súdnym, správnym, či iným úradným konaním vzniknutým a vedeným v súvislosti s obchodnými vzťahmi medzi zmluvnými stranami, alebo
   - ak je ich poskytnutie požadované na základe rozhodnutia vydaného príslušným súdnym orgánom alebo orgánom verejnej správy, ktoré nadobudlo právne účinky, pričom sa zaväzuje včas a vopred oznámiť takúto povinnosť poskytnúť dôverné informácie objednávateľovi.

7. Poskytovateľ môže poskytnúť dôverné informácie inej osobe ako je uvedená v bode 5. a 6. tohto článku iba po predchádzajúcom písomnom súhlase objednávateľa s takýmto poskytnutím a súčasne takáto osoba, ktorej sa majú poskytnúť dôverné informácie uzavrela dohodu o ochrane dôverných informácií s poskytovateľ v rozsahu stanovenom touto zmluvou.
8. V prípade, že bude u poskytovateľa inštalované vývojové prostredie dodaného informačného systému smie byť toto využívané len pre vykonanie činností pre zabezpečenie poskytovania Poskytovaných služieb pre objednávateľa. Poskytovateľ nie je oprávnený používať inštalované prostredia dodaného informačného systému pre prevádzku výpočtového strediska, teda za účelom spracovania dát tretích strán a/alebo osôb, napr. tým, že dovolí tretej strane a/alebo osobe užívanie dodaného informačného systému akýmkoľvek technickým spôsobom, alebo tým, že využije alebo umožní využitie dodaného informačného systému pre účely tretej strany a/alebo osoby.
9. Zmluvné strany písomne zaviažu svojich zamestnancov, iné strany a osoby, ktoré budú pracovať na základe zmluvy a týchto podmienok, na dodržiavanie povinností podľa tohto článku všeobecných podmienok.
10. Objednávateľ neposkytne poskytovateľovi informácie, ktoré patria do zoznamu utajovaných skutočností v zmysle všeobecne záväzného právneho predpisu, ak tieto informácie nie sú nutné na splnenie predmetu zmluvy. V prípade, že tieto informácie budú potrebné k splneniu predmetu zmluvy bude sa postupovať v zmysle všeobecne záväzných predpisov upravujúcich ochranu utajovaných skutočností.
11. Zmluvné strany sa dohodli, že v prípade porušenia akejkoľvek povinnosti poskytovateľa uvedenej v tomto článku všeobecných podmienok, má objednávateľ právo uplatniť voči poskytovateľovi zmluvnú pokutu vo výške 70.000,- eur bez DPH (slovom: sedemdesiat tisíc eur), a to za každé jednotlivé porušenie povinnosti poskytovateľa. Zmluvná pokuta je splatná do 3 dní odo dňa doručenia výzvy na zaplatenie zmluvnej pokuty. Povinnosť uhradiť zmluvnú pokutu vzniká bez ohľadu na skutočnosť, či objednávateľovi vznikla škoda v dôsledku porušenia povinnosti poskytovateľa. Tým nie je dotknuté právo poškodenej osoby (objednávateľa) na náhradu škody v zmysle § 373 a nasl. Obchodného zákonníka.

Článok VIII
Podmienky poskytovania Poskytovaných služieb

1. Poskytovateľ a objednávateľ sa dohodli, že pre účely poskytovania Poskytovaných služieb bude využívaný informačný systém na evidenciu a správu incidentov poskytnutý objednávateľom, pokiaľ sa zmluvné strany nedohodnú inak.
2. Objednávateľ sa v prípade opodstatnenej potreby môže s poskytovateľom dohodnúť aj na inej dobe odozvy na riešenie prevádzkových incidentov ako je zmluvne dohodnuté v špecifikácii Poskytovaných služieb.
3. Objednávateľ je oprávnený vykonávať zmeny a/alebo rozšírenia dodaného informačného systému v mieste objednávateľa a postupovať pri zaraďovaní zmien a/alebo rozšírení dodaného informačného systému v súlade so zmluvne dohodnutými postupmi v špecifikácii Poskytovaných služieb.
4. Objednávateľ je oprávnený bez predchádzajúceho súhlasu poskytovateľa vykonávať také zmeny a/alebo rozšírenia dodaného informačného systému, ktoré vykonáva v súlade a na základe poskytovateľom dodaných postupov. V tomto prípade sa neuplatňuje postup na odsúhlasenie zmien a/alebo rozšírení dodaného systému odovzdaných poskytovateľovi uvedený v špecifikácii Poskytovaných služieb.

Článok IX
Subdodávatelia, register partnerov verejného sektora a iné povinnosti poskytovateľa

1. Poskytovateľ je povinný riadne a načas plniť záväzky vyplývajúce zo zmluvy a týchto podmienok vo vlastnom mene, na vlastný účet, na svoje náklady a na svoje nebezpečenstvo. Pokiaľ poskytovateľ poverí plnením ktoréhokoľvek zo záväzkov podľa zmluvy a týchto podmienok tretiu stranu, má poskytovateľ voči objednávateľovi rovnakú zodpovednosť za poskytovanie

Poskytovaných služieb a za prípadné škody, náklady a únik dôverných informácií spôsobený treťou stranou, ako by plnil tieto záväzky sám.

2. Poskytovateľ je povinný požiadať objednávateľa o zriadenie/zrušenie prístupu do dodaného systému v súlade s postupmi pre zabezpečenie prístupu do dodaného informačného systému v rámci zmluvy.
3. Poskytovateľ podpisom tejto zmluvy potvrdzuje a zaväzuje sa, že na plnení zmluvy sa budú podieľať iba osoby legálne zamestnané poskytovateľom v súlade s právnym poriadkom Slovenskej republiky.
4. V prípade, ak poskytovateľ poruší svoju povinnosť podľa bodu 3 tohto článku všeobecných podmienok zmluvy a kontrolný orgán uloží objednávateľovi pokutu za porušenie zákazu prijať prácu alebo službu podľa § 7b ods. 5 zákona č. 82/2005 Z. z. o nelegálnej práci a nelegálnom zamestnávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, tak sa poskytovateľ zaväzuje uhradiť objednávateľovi zmluvnú pokutu v sume rovnajúcej sa pokute uplatnenej kontrolným orgánom u objednávateľa, a to do siedmich dní odo dňa jej uplatnenia u poskytovateľa objednávateľom.
5. Poskytovateľ je povinný na požiadanie objednávateľa bezodkladne poskytnúť v nevyhnutnom rozsahu doklady (pracovné zmluvy, dohody o prácach vykonávaných mimo pracovného pomeru v zmysle Zákonníka práce) a osobné údaje fyzických osôb, prostredníctvom ktorých plní zmluvu, a ktoré sú potrebné na to, aby objednávateľ mohol skontrolovať, či poskytovateľ neporušuje zákaz nelegálneho zamestnávania.
6. V prípade, ak pri poskytovaní Poskytovaných služieb poskytovateľom počas trvania zmluvy poskytovateľ zhotoví dielo, poskytovateľ sa týmto zaväzuje poskytnúť objednávateľovi záruku na vytvorené dielo v dĺžke trvania 24 mesiacov, ktorá začne plynúť odo dňa podpisu príslušného preberacieho protokolu objednávateľom.
7. Poskytovateľ sa zaväzuje, že zabezpečí, aby jeho zamestnanci a ostatné osoby poskytovateľa konajúce v mene poskytovateľa pri plnení zmluvy v objektoch objednávateľa dodržiavali všetky všeobecne záväzné právne predpisy vzťahujúce sa k vykonávaniu činností, hlavne predpisy súvisiace s bezpečnosťou práce a požiarnou bezpečnosťou, interné predpisy objednávateľa, najmä predpisy o vstupe do objektov objednávateľa a k bezpečnosti systémov a aby sa riadili organizačnými pokynmi oprávnených zamestnancov objednávateľa.
8. Objednávateľ na základe písomnej žiadosti poskytovateľa je povinný zabezpečiť vstupy do svojich priestorov povereným osobám poskytovateľa. Tento prístup poskytovateľa bude vykonaný vždy len pod priamym dozorom objednávateľa za účelom včasného plnenia záväzkov poskytovateľa dohodnutých v tejto zmluve a v súlade s internými predpismi objednávateľa upravujúcimi vstup zamestnancov cudzích organizácií a vykonávanie činnosti v priestoroch objednávateľa a bude platiť len na obdobie trvania tejto zmluvy.
9. Poskytovateľ sa zaväzuje, že viacerí používatelia poskytovateľa nebudú pristupovať do testovacieho a vývojového prostredia dodaného informačného systému pod jedným identifikačným názvom.
10. Poskytovateľ zodpovedá za plnenie zmluvy v súlade s § 41 ods. 8 zákona o verejnom obstarávaní a poskytovateľ je povinný odovzdávať objednávateľovi plnenia sám, na svoju zodpovednosť, v dohodnutom čase a v dohodnutej kvalite.
11. Poskytovateľ sa zaväzuje, počas celej doby trvania tejto zmluvy byť zapísaný v registri partnerov verejného sektora, a to v prípade, ak má túto povinnosť podľa zákona č. 315/2016 Z. z. o registri partnerov verejného sektora a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon č. 315/2016 Z. z.“). U subdodávateľa táto povinnosť platí, ak mu takáto povinnosť v zmysle zákon č. 315/2016 Z. z. vzniká, pričom za jej splnenie zodpovedá poskytovateľ.
12. Poskytovateľ potvrdzuje, že podľa § 41 ods. 3 zákona o verejnom obstarávaní uviedol v príslušnej prílohe tejto zmluvy údaje o všetkých známych subdodávateľoch, údaje o osobe oprávnenej konať za subdodávateľoch v rozsahu meno a priezvisko, adresa pobytu/sídlo, dátum narodenia/IČO. Poskytovateľ je povinný písomne oznámiť objednávateľovi akúkoľvek zmenu údajov o subdodávateľoch uvedených v príslušnej prílohe tejto do troch pracovných dní odo dňa uskutočnenia tejto zmeny.
13. V prípade zmeny subdodávateľa alebo doplnenia nového subdodávateľa, je poskytovateľ povinný písomne oznámiť objednávateľovi údaje o navrhovanom subdodávateľovi v rozsahu podľa bodu 9

tohto článku, najmenej štyri pracovné dni pred jeho plánovaným využitím. Počas trvania tejto zmluvy je poskytovateľ oprávnený zmeniť subdodávateľa uvedeného v príslušnej prílohe tejto zmluvy výlučne na základe predchádzajúceho písomného oznámenia a predchádzajúceho písomného odsúhlasenia objednávateľom, pričom objednávateľ si vyhradzuje právo odmietnuť subdodávateľa, a to najmä v prípade, ak existuje dôvodný predpoklad, že plnenie záväzkov subdodávateľa podľa tejto zmluvy je ohrozené a v prípade, ak subdodávateľ nespĺňa požiadavky na odborno-technickú spôsobilosť vo vzťahu k tej časti predmetu plnenia, ktorá má byť subdodávateľom plnená.

14. Za účelom preukázania splnenia povinnosti v zmysle bodu 8 tohto článku zmluvy je poskytovateľ povinný kedykoľvek na výzvu objednávateľa bezodkladne, najneskôr však do troch pracovných dní, predložiť objednávateľovi všetky zmluvy so subdodávateľmi identifikovanými v príslušnej prílohe tejto zmluvy, resp. následne doplnenými/ zmenenými postupom podľa bodu 10 tohto článku zmluvy a zároveň predložiť zoznam všetkých subdodávateľov v zmysle § 2 ods. 1 písm. a) bod 7 zákona č. 315/2016 Z. z., ktorí napĺňajú definičné znaky partnera verejného sektora v zmysle § 2 ods. 1 písm. a) bod 7 a § 2 ods. 2 zákona č. 315/2016 Z. z., v dôsledku ich participácie na plnení tejto zmluvy. Za úplnosť a pravdivosť poskytnutých údajov nesie plnú zodpovednosť poskytovateľ.

15. V prípade, ak poskytovateľ poruší povinnosť v zmysle bodu 11 tohto článku, a teda bude táto zmluva plnená (resp. budú na jej plnení participovať) subdodávateľmi, ktorí si riadne nesplnili svoju zákonnú povinnosť zápisu (resp. jeho udržiavania) do registra partnerov verejného sektora, má objednávateľ právo na zmluvnú pokutu od poskytovateľa vo výške 3 000,- eur bez DPH za každé jednotlivé porušenie stanovenej povinnosti. Zmluvná pokuta je splatná do 5 pracovných dní odo dňa doručenia výzvy na zaplatenie zmluvnej pokuty.

16. V prípade omeškania poskytovateľa so splnením záväzku (povinnosti) v zmysle bodu 12 tohto článku zmluvy, má objednávateľ právo na zmluvnú pokutu vo výške 1.000,- eur bez DPH, a to za každý aj začatý deň omeškania. Zmluvná pokuta je splatná do 5 pracovných dní odo dňa doručenia výzvy na zaplatenie zmluvnej pokuty.

17. Poskytovateľ sa môže odvolávať na objednávateľa vo svojich verejných materiáloch v tom zmysle, že ide o zákazníka poskytovateľa s písomným súhlasom objednávateľa a nesmie bez predchádzajúceho písomného súhlasu objednávateľa, publikovať prácu poskytovateľa podľa tejto zmluvy. Každá zo zmluvných strán sa zaväzuje, že nebude publikovať prácu vykonanú druhou zmluvnou stranou tak, že by použil názov druhej zmluvnej strany bez jej predchádzajúceho písomného súhlasu. V prípade odstúpenia od zmluvy sa poskytovateľ zaväzuje dňom odstúpenia od zmluvy zrušiť odvolávku vo svojich verejných materiáloch o tom, že ide o zákazníka poskytovateľa.

18. Poskytovateľ je povinný na požiadanie objednávateľa po ukončení zmluvy vydať objednávateľovi všetky hmotné nosiče, ich kópie a vymazať programy uložené do pamäti, ako aj vydať všetku Sprievodnú dokumentáciu a Ostatné náležitosti patriace k dodanému informačnému systému, ktoré boli poskytnuté od objednávateľa.

Článok X
Zmluvné pokuty

1. Zaplatením zmluvnej pokuty nebude dotknutý nárok objednávateľa na náhradu škody. Zmluvné pokuty sa nezapočítavajú na úhradu škôd, ktoré objednávateľovi vzniknú porušením zmluvných povinností poskytovateľa.

2. Objednávateľ nie je oprávnený uplatniť voči poskytovateľovi zmluvnú pokutu v prípade, že pri riešení prevádzkového incidentu poskytovateľom sa zistí, že prevádzkový incident vznikol v dôsledku toho, že objednávateľ preukázateľne nepoužíval dodaný informačný systém v súlade s poskytovateľovými dodanými inštalačnými a používateľskými príručkami dodaného informačného systému.

Článok XI
Preukazovanie schopnosti poskytovať Poskytované služby

1. Poskytovateľ sa zaväzuje do 15 dní po skončení každého ročného výročia účinnosti zmluvy objednávateľovi preukázateľne dokladovať, že pre tie časti dodaného informačného systému, pre

ktoré je poskytovanie Poskytovaných služieb viazané na poskytnutie Poskytovaných služieb treťou stranou, má zabezpečené poskytovanie Poskytovaných služieb od tretej strany za takých podmienok, aby bol schopný poskytovať Poskytované služby objednávateľovi v súlade s touto zmluvou. Zmluvné strany sa dohodli, že v prípade porušenia záväzku upraveného v tomto bode, má objednávateľ právo uplatniť voči poskytovateľovi zmluvnú pokutu vo výške 1.500,- eur bez DPH (slovom: tisícpäťsto eur), a to za každé jednotlivé porušenie záväzku poskytovateľom. Zmluvná pokuta je splatná do 5 pracovných dní odo dňa doručenia výzvy na zaplatenie zmluvnej pokuty.

2. Za preukázateľné dokladovanie objednávateľ bude môcť považovať napr. zmluvu poskytovateľa na poskytnutie Poskytovaných služieb treťou stranou, doklad o vykonaní úhrady za poskytnutie Poskytovaných služieb treťou stranou, a pod.

3. Objednávateľ bude oprávnený priebežne požadovať od poskytovateľa dokladovanie v zmysle bodu 1 a bodu 2 tohto článku všeobecných podmienok pre vybranú časť dodaného informačného systému a poskytovateľ je povinný takéto zdokladovanie dodať do 1 mesiaca od vznesenia požiadavky objednávateľom.

Článok XII
Ochrana osobných údajov

V prípade, ak bude objednávateľ poskytovať alebo sprístupňovať poskytovateľovi v súvislosti s plnením podľa tejto zmluvy informácie obsahujúce osobné údaje chránené v zmysle nariadenia Európskeho parlamentu a rady (EÚ) 2016/679 o ochrane fyzických osôb pri spracúvaní ich osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) a zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, je poskytovateľ povinný s objednávateľom **uzatvoriť zmluvu** v zmysle § 28 zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov.

Článok XIII
Zodpovednosť za škodu

1. Poskytovateľ zodpovedá objednávateľovi za škody spojené s predmetom zmluvy v zmysle § 373 - § 386 Obchodného zákonníka.

2. Pre vylúčenie pochybností a príkladom platí, že poskytovateľ zodpovedá objednávateľovi za škody spojené s predmetom zmluvy a jeho dodávkou, a to:

a) vzniknuté v dôsledku toho, že chod a funkčnosť dodaného systému alebo jeho jednotlivých modulov, komponentov, programov a funkcií, pokiaľ nebudú modifikované objednávateľom a ak objednávateľ neporuší svoje povinnosti, nebude zodpovedať chodu a funkčnosti dodaného systému uvedenému v sprievodnej dokumentácií dodaného systému, ktorú poskytovateľ odovzdal objednávateľovi a ktorá bola objednávateľom prijatá podľa tejto zmluvy,

b) takým spôsobom zapríčinené následné škody, ušlý zisk, straty dát alebo porušenia technických zariadení,

c) škody vzniknuté iným nedovoleným konaním, škody vzniknuté nedbanlivosťou, porušením zmluvy,

d) škody spôsobené na majetku objednávateľa zamestnancami a subdodávateľmi poskytovateľa pri plnení tejto zmluvy.

Článok XIV
Ukončenie zmluvy

1. Zmluva zaniká:

a) uplynutím doby, na ktorú bola uzavretá,

b) písomnou dohodou zmluvných strán,

c) odstúpením od zmluvy,

d) výpoveďou zo strany objednávateľa aj bez uvedenia dôvodu s trojmesačnou výpovednou lehotou a výpoveďou poskytovateľa aj bez uvedenia dôvodu so šesťmesačnou výpovednou lehotou, pričom výpovedná lehota začína plynúť prvým dňom

mesiaca nasledujúceho po mesiaci, v ktorom bola písomná výpoveď riadne doručená druhej zmluvnej strane. V tomto prípade je poskytovateľ povinný objednávateľovi po dobu plynutia výpovednej lehoty od doručenia písomnej výpovede plniť záväzky plynúce zo zmluvy. V prípade porušenia tejto povinnosti je poskytovateľ povinný nahradiť škody, ktoré by objednávateľovi vznikli neplnením povinností vyplývajúcich z tejto zmluvy.

2. Odstúpiť od zmluvy je možné z dôvodov podstatného porušenia zmluvných povinností druhou zmluvnou stranou alebo v prípade nepodstatného porušenia zmluvných povinností zmluvy druhou zmluvnou stranou v prípadoch, ak to upravuje všeobecne záväzný právny predpis alebo zmluva (napr. v zmysle § 19 ods. 3 zákona č. 343/2015 Z. z. alebo § 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). Odstúpenie od zmluvy musí byť v písomnej forme doručené na adresu druhej zmluvnej strany.
3. Za nepodstatné porušenie zmluvy sa považuje každé porušenie zmluvy, okrem porušení zmluvy upravených v zmluve a/alebo v všeobecných podmienkach ako podstatné porušenie zmluvy. V prípade, ak ktorákoľvek zo zmluvných strán poruší nepodstatným spôsobom niektorú zo svojich povinností dohodnutých v zmluve a nesplní svoju povinnosť ani v dodatočne určenej primeranej lehote stanovenej dotknutou zmluvnou stranou, môže táto zmluvná strana od zmluvy odstúpiť. Výzva na splnenie povinnosti s určením dodatočnej primeranej lehoty musí byť písomná a doručená druhej zmluvnej strane. Právne účinky odstúpenia od zmluvy nastanú dňom doručenia písomného oznámenia o odstúpení druhej zmluvnej strany.
4. Ukončením zmluvy nie je dotknutý nárok na náhradu škody vzniknutej porušením ustanovení zmluvy a tiež nie je dotknutý nárok na úhrady sumy zodpovedajúcej zmluvnej pokute, ktorý vznikol do účinnosti odstúpenia. Skončenie zmluvy nemá vplyv na ustanovenia, ktorých platnosť a účinnosť vzhľadom na ich povahu má trvať aj po skončení zmluvy.

Článok XV
Záverečné ustanovenia

1. Všetky dokumenty, oznámenia, žiadosti, správy, výzvy, požiadavky a ostatné písomnosti určené druhej zmluvnej strane (ďalej len „písomnosti“) musia byť doručené, ak zmluva neustanovuje inak v písomnej forme:

   a) v listinnej podobe prostredníctvom pošty doporučene s doručenkou; za deň doručenia sa považuje dátum prevzatia zásielky,

   b) osobne do sídla druhej zmluvnej strany alebo

   c) elektronicky formou e-mailu, a to pri objednávaní Poskytovaných služieb a pri bežnej komunikácii zaslaním spätného potvrdzujúceho e-mailu príjemcom, pričom za spätný potvrdzujúci e-mail príjemcu sa nepovažuje správa automaticky vygenerovaná systémom.
2. V prípade, ak je to účelné a potrebné, objednávateľ sprístupní poskytovateľovi v mieste poskytovania Poskytovaných služieb na dobu a pre účel poskytovania Poskytovaných služieb podľa tejto zmluvy a všeobecných podmienok nevyhnutný počet licencií na použitie softvéru, ktorý má objednávateľ v užívaní.
3. zmluva a tieto podmienky sa budú riadiť slovenským právnym poriadkom.
4. Všetky spory zo zmluvy a týchto podmienok alebo súvisiace s jej porušením, ukončením alebo neplatnosťou budú riešené s konečnou platnosťou vecne a miestne príslušným súdom Slovenskej republiky.
5. Práva a povinnosti zmluvných strán neupravené v zmluve a týchto podmienkach sa riadia príslušnými ustanoveniami Obchodného zákonníka a ďalšími všeobecne záväznými právnymi predpismi platnými na území Slovenskej republiky.
6. Komunikácia medzi objednávateľom a poskytovateľom vrátane zmluvnými stranami vytvorenej písomnej dokumentácie sa bude v priebehu trvania zmluvy uskutočňovať výhradne v slovenskom a/alebo českom jazyku.

Koniec dokumentu.

1. Ceny poskytovaných služieb

Cena predmetu plnenia		
Položka	**Popis**	**Cena v € bez DPH**
S1	Paušálna mesačná platba za službu „**SOC**" – režim 15/5	*9 314,00 €*
S2	Paušálna mesačná platba za službu „**MBIT**" – režim 15/5	*17 780,00 €*
S3	Paušálna mesačná platba za službu „**SOC**" – režim 24/7 - OPCIA	*10 316,00 €*
S4	Paušálna mesačná platba za službu „**MBIT**" – režim 24/7 - OPCIA	*18 923,00 €*
S5	Paušálna mesačná platba za službu „**Skenovanie zraniteľností**" – režim 8/5	*3 905,58 €*
S6	Paušálna mesačná platba za službu „**Sledovanie IT hrozieb a zraniteľností**" – režim 8/5	*1 543,00 €*
S7	Paušálna mesačná platba za službu „**BAS**" – režim 8/5	*4 375,80 €*
S8	Paušálna mesačná platba za službu „**Rozvoj a optimalizácia MBIT**" – režim 8/5	*10 757,00 €*
S9	Hodinová sadzba za osobohodinu služby **„Forenzná analýza"**	*50,00 €*
S10	Hodinová sadzba za osobohodinu služby **„Exit služba"**	*69,00 €*
S11	Hodinová sadzba za osobohodinu **konzultačné a implementačné služby**	*69,00 €*
Výpočet celkovej ceny		
CC	Celková cena vypočítaná ako CC = 24 x (S1 +S2) + 36 x (S3 + S4) + 60 x (S5 +S6 + S7 + S8) + 200 x S9 + 250 x S10 + 500 x S11	*2 999 492,80 €*

uchádzač vyplní žlté bunky

Cena za položku S3 (Paušálna mesačná platba za službu „SOC" – režim 24/7 – OPCIA) nemôže byť nižšia ako cena za položku S1 (Paušálna mesačná platba za službu „SOC" – režim 15/5)

Cena za položku S4 (Paušálna mesačná platba za službu „MBIT" – režim 24/7 – OPCIA) nemôže byť nižšia ako cena za položku S2 (Paušálna mesačná platba za službu „MBIT" – režim 15/5)

Cena za hodinovú sadzbu za osobohodinu položky S10 (Hodinová sadzba za osobohodinu služby „Exit služba") a S11 (Hodinová sadzba za osobohodinu konzultačné a implementačné služby) musia byť rovnaké

Príloha 4 k Zmluve na poskytovanie služieb IT monitoring bezpečnosti č. C-NBS1-000-106-915

Slovník pojmov k zmluve a použité skratky

I. Slovník pojmov

Pojem (y) / Výraz / Skratka	Vysvetlenie Pojmu / Výrazu / Skratky
Aktualizácie	zmluvné strany rozumejú zmeny, zdokonalenia alebo zlepšenia dodávaného systému (licencovaných programov), ktoré poskytovateľ bude podľa vlastného uváženia určovať a voliť na zabudovanie do dodávaného systému (licencovaných programov) a vytváranie ich častí, namiesto separátnych softvérových programov. Uvedené aktualizácie poskytuje poskytovateľ objednávateľovi podľa podmienok tejto zmluvy.
Aplikačné programové rozhranie (API)	zmluvné strany rozumejú komponenty, programy, procedúry, funkcie, dátové a iné objekty systému, ktoré ako celok a/alebo jednotlivo zabezpečujú obojsmerný, resp. jednosmerný prenos a spracovanie dát a/alebo správ pre dodaný informačný systém tak, aby bola dosiahnutá jeho funkcionalita podľa dokumentu stanovujúceho celkovú funkcionalitu dodaného informačného systému a podľa sprievodnej dokumentácie dodaného informačného systému
poskytovateľ	subjekt/organizácia/spoločnosť/firma, ktorá dodáva, zabezpečuje a zodpovedá za dodávky, práce a služby uvedené v popise predmetu tejto zmluvy a vo svojich záväzkoch v tejto zmluve pre objednávateľa.
Definovaný používateľ	osoba, ktorá má priamy alebo nepriamy prístup k Systému. Taktiež používatelia technických systémov umožňujúcich nepriamy prístup k Systému, ako aj technický systém sám, musia byť definovaní ako definovaní používatelia v zmysle tejto Zmluvy. Každá takáto osoba musí mať od objednávateľa pridelený identifikačný názov, pod ktorým je jeho prístup umožnený. Definovanými používateľmi môžu byť iba zamestnanci objednávateľa či zamestnanci právnych subjektov, s ktorými je objednávateľ v obchodnom styku.
Doba odozvy	rozumie sa časové obdobie, počas ktorého je zhotoviteľ povinný začať vykonávať príslušnú činnosť od nahlásenia požiadavky objednávateľa na jej vykonanie.
Dodať podľa tejto zmluvy, Odovzdať	zmluvné strany rozumejú dodanie dodávky, uvedenej v popise predmetu zmluvy a záväzkoch poskytovateľa v tejto zmluve poskytovateľom objednávateľovi podľa zmluvných podmienok, záväzkov, štandardov, postupov a oprávnení uvedených v tejto zmluve. Táto skutočnosť musí byť písomne potvrdená poskytovateľom a objednávateľom v príslušnom protokole.
Dodaný informačný systém	dodaný informačný systém znamená informačný systém objednávateľa, ktorý bol dodaný Národnej banke Slovenska (ďalej len „dodaný informačný systém) na základe zmluvy o dielo pred zákazkou s názvom Monitoring bezpečnosti IT. Môžu sa tým myslieť akékoľvek informačné systémy pre ktoré sa poskytujú služby podľa Zmluvy alebo služby podpora, Údržba, Konzultácie, Školenie, Implementácia a Služba sledovania aktuálnych IT hrozieb a zraniteľností.
Dostupnosť služby	čas, kedy je služba poskytovateľom poskytovaná objednávateľovi.
Dôverná informácia druhej strany	zmluvné strany rozumejú každý dokument, materiál, myšlienku, údaje alebo iné informácie vzťahujúce sa k výskumu a vývoju, obchodným tajomstvám, bankovým a služobným tajomstvám alebo obchodným záležitostiam poskytovateľa alebo objednávateľa alebo sú označené ako dôverné, a ktorejkoľvek zo strán dané druhou stranou iba pre účely tejto zmluvy.

Pojem (y) / Výraz / Skratka	Vysvetlenie Pojmu / Výrazu / Skratky
Chyba, nedostatok	chybu a/alebo nedostatok predstavuje akékoľvek nesplnenie požiadaviek na dodaný informačný systém, nesplnenie stanovených štandardov, neschválené odchýlky od stanovenej funkcionality dodaného informačného systému alebo úprav dodaného informačného systému, nedodržanie postupov stanovených pre analýzu, návrh, implementovanie, testovanie a spracovanie dokumentácie úprav dodaného informačného systému a používanie iných ako stanovených softvérových nástrojov. Nedostatok predstavuje aj nevykonávanie alebo iba čiastočné vykonávanie funkcií komponentov, modulov, objektov a programov špecifikovaných v sprievodnej dokumentácií dodaného informačného systému.
Incident	každá udalosť, ktorá nie je štandardnou funkčnosťou dodávaného systému, infraštruktúry dodávaného systému alebo prevádzky osobných počítačov používateľov dodávaného systému a môže spôsobiť alebo spôsobila výpadok alebo zníženie funkcionality a výkonnostných parametrov dodávaného systému, infraštruktúry dodávaného systému alebo prevádzky osobných počítačov používateľov dodávaného systému,
Inštalácia	zmluvné strany rozumejú inštaláciu všetkých komponentov, programov a dát dodaného informačného systému v databázovej a aplikačnej vrstve dodaného informačného systému. Táto inštalácia môže byť vykonaná na testovacom prostredí a/alebo v produkčnom prostredí u objednávateľa.
IT zariadenie	technologické zariadenie, ktoré je súčasťou IT infraštruktúry NBS a zabezpečuje aplikačné alebo komunikačné funkcie pre informačné systémy prevádzkované v NBS napr. zariadenia výpočtovej techniky ako servery, aktívne prvky sietí, elektronické komunikačné systémy, virtuálne systémy a podobne vrátane operačného systému alebo softvéru zabezpečujúceho funkčnosť IT zariadenia (napr. firmware).
IS, informačný systém	kompaktný programový produkt, pomocou ktorého sa na prostriedkoch výpočtovej techniky s nosičmi údajov spracúvajú údaje a informácie v elektronickej forme
Komponent IT infraštruktúry	IT zariadenie a/alebo Základný aplikačný softvér
Kritérium kvality	kritérium kvality predstavuje tie charakteristiky produktu, ktoré určujú, či produkt spĺňa požiadavky pre produkt stanovené.
Kritický IT systém NBS	– Explicitne určený zoznam IT služieb a ich komponentov (napr. SWIFT, SIPS, ...)
Kvalita	celkový súhrn znakov prvku, ktoré ovplyvňujú jeho schopnosť uspokojiť stanovené a predpokladané potreby.
Licencované materiály	zmluvné strany rozumejú dokumenty písané poskytovateľom na používanie v spojení s dodaným informačným systémom (licencovaným programom) v slovenskom jazyku vrátane používateľských smerníc a referenčných materiálov dodávaných poskytovateľom objednávateľovi podľa tejto zmluvy.
Nastavenia dodaného (informačného) systému	nastavenie dodaného informačného systému znamená zmenu parametrov (parametrizácia) vykonaných v používateľskom rozhraní systému. Nastavenie dodaného informačného systému musí byť vykonané v súlade s používateľskou dokumentáciou.
Nedostatok	nedostatok predstavuje akékoľvek nesplnenie požiadaviek na dodávaný systém, nesplnenie stanovených štandardov, neschválené odchýlky od stanovenej funkcionality dodaného informačného systému, nedodržanie postupov stanovených pre analýzu, návrh, implementovanie, testovanie a spracovanie dokumentácie dodávaného systému a používanie iných ako stanovených softvérových nástrojov. Nedostatok predstavuje aj nevykonávanie alebo iba čiastočné vykonávanie funkcií komponentov, modulov, objektov a programov špecifikovaných v sprievodnej dokumentácií dodávaného systému. Nedostatok predstavuje aj nesplnenie skúšobnej podmienky stanovenej na overenie požadovaných funkčných, technických, prevádzkových a

Pojem (y) / Výraz / Skratka	Vysvetlenie Pojmu / Výrazu / Skratky
	bezpečnostných vlastností dodávaného systému počas akceptačného testovania dodaného informačného systému
Osobodeň	zmluvné strany rozumejú práce a služby 1 osoby počas 8 hodín práce počas pracovnej doby (od 8:00 h do 16:00 h) počas pracovných dní, pričom sa počíta iba naplnených osem hodín.
Osobohodina	1 osobohodina = 60 minút pracovného času.
Poverená osoba	zástupca jednej zo strán tejto Zmluvy zaisťujúca spoluprácu a komunikáciu medzi stranami v rozsahu danom touto zmluvou a jeho oprávnením.
Podozrivé zistenie	– anomália, neštandardné správanie, podozrivá aktivita, identifikované narušenie bezpečnosti, opakované neúspešné/úspešné pokusy o komunikáciu s podozrivými IP adresami, využívanie neštandardných portov, použitie nepovolených služieb (vzdialený prístup, anonymizačné služby, ťažba kryptomien, a pod.), atď.
Požiadavka na zmenu	požiadavka na zmenu predstavuje prostriedok na modifikáciu dodaného informačného systému, t.j. akýkoľvek návrh a podnet, ktorého cieľom je zmeniť vlastnosti dodaného informačného systému voči požiadavkám na systém so zámerom zlepšiť vlastnosti dodaného informačného systému.
Pracovná doba	za pracovnú dobu sa pre účely tejto Servisnej zmluvy rozumie časové obdobie medzi 7.00 – 23.00 hod. v pracovných dňoch platobného systému TARGET2, ktorými sú všetky dni okrem soboty, nedele, Nového roku, Veľkého piatku a Veľkonočného pondelka (podľa kalendára platného v sídle ECB), 1. mája, prvého sviatku vianočného a druhého sviatku vianočného.
Prijatý, Prijatie, Prijať	pojmy „Prijatý“, ”Prijatie”, „Prijať“ tak, ako sú uvádzané v zmluve znamenajú pre obidve zmluvné strany, že: akákoľvek dodávka uvedená v popise predmetu tejto zmluvy a/alebo akýkoľvek záväzok poskytovateľa boli zo strany poskytovateľa splnené podľa podmienok, štandardov, procedúr a kritérií tejto zmluvy, a ktorých splnenie objednávateľ podľa podmienok tejto zmluvy písomne odsúhlasil (akceptoval), akákoľvek dodávka uvedená v popise predmetu tejto zmluvy a/alebo akýkoľvek záväzok poskytovateľa boli na základe predchádzajúceho objednávateľom odsúhlaseného splnenia (akceptácie) fyzicky dodané poskytovateľom objednávateľovi v mieste objednávateľa a ktoré objednávateľ fyzicky prijal, fyzické prijatie písomne odsúhlasenej (akceptovanej) dodávky a/alebo záväzku poskytovateľa potvrdia poskytovateľ a objednávateľ písomne v preberacom protokole.. Predmetný protokol je uvedený ako štandard v Prílohe 4 tejto zmluvy..
Prevzatý, Prevzatie, Prevziať	pojmy „Prevzatý“, ”Prevzatie”, Prevziať“ tak ako sú uvádzané v zmluve znamenajú pre obidve zmluvné strany, že: a) akákoľvek dodávka uvedená v popise predmetu tejto zmluvy a/alebo akýkoľvek záväzok poskytovateľa boli zo strany poskytovateľa fyzicky dodané objednávateľovi v mieste objednávateľa za účelom ich prevzatia napr. na informovanie objednávateľa, na vykonanie akceptačného testovania, na vykonanie pripomienkovania a akceptovania dokumentov, na zaistenie kvality riadenia projektu a na zaistenie kvality dodávaného systému a objednávateľ ich k uvedenému účelu fyzicky prevzal. b) fyzické prevzatie dodávky a/alebo záväzku poskytovateľa potvrdia poskytovateľ a objednávateľ písomne v preberacom protokole. Predmetný protokol bude uvedený ako štandard v tejto zmluve. c) účel a stav dodávky alebo záväzku poskytovateľa musí byť jednoznačne uvedený vo funkčnom prijímacom protokole.
Prevádzkový incident	akákoľvek udalosť ktorá je spôsobená správou a prevádzkou IT infraštruktúry a IS NBS.
Produkčné prostredie	zmluvné strany rozumejú technické zariadenia a programové vybavenie (softvér) a všetky údaje nachádzajúce sa u objednávateľa vrátane nastavenia

Pojem (y) / Výraz / Skratka	Vysvetlenie Pojmu / Výrazu / Skratky
	ich parametrov určené k produkčnej prevádzke dodaného informačného systému.
Produkt	produkt predstavuje akýkoľvek výstup projektu alebo servisnej služby, t.j. softvér, hardvér, dokumentácia a údaje. Popis produktu popisuje jeho účel, formát (podobu), prvky, z ktorých sa skladá, t.j. komponenty, a kvalitatívne kritéria, ktorým musia vyhovieť. Každý produkt má svoj popis. Čiastkové produkty komplexných produktov môžu mať svoje vlastné popisy a samotné sa môže skladať z ďalších produktov, podproduktov.
Produktová dokumentácia	technická dokumentácia, používateľská dokumentácia, inštalačná dokumentácia dodaného informačného systému.
Projektant, projektant prevádzky	odbor informačných technológií, ktorý je zodpovedný za technické a programové vybavenie pracovísk a zabezpečenie prevádzky IS v NBS.
Prostredie	zmluvné strany rozumejú testovacie a/alebo produkčné a/alebo archivačné prostredie objednávateľa, ktoré je inštalované v priestoroch objednávateľa na používanie s dodaným informačným systémom (licencovanými programami).
Riadenie	proces plánovania, zabezpečenia, kontrolovania a vyhodnocovania činností pri realizácii servisných služieb.
Riadenie incidentov	spočíva v: a) zaznamenaní incidentov v rámci prevádzky dodaného informačného systému a/alebo počas akceptačného testovania úpravy dodaného informačného systému alebo jeho časti b) vykonanie analýzy príčin incidentu, c) vyriešenie incidentov a otestovanie u poskytovateľa tak, aby bolo vylúčené zanesenie nových incidentov do dodaného informačného systému ako dôsledok riešenia daného incidentu, d) vykonanie overenia vyriešenia incidentu formou regresného testovania objednávateľom, e) vedenie dokumentácie o riadení incidentov.
Riadiaci výbor	predstavuje tú úroveň v rámci riadiacej organizačnej štruktúry projektu, ktorá má oprávnenia a zodpovednosť na rozhodovanie o vecnej oblasti riadenia poskytovania Servisných služieb, t.j. riadiaci orgán projektu predstavujú vedúci projektu poskytovateľa a objednávateľa v rámci oprávnení a zodpovedností delegovaných vedúcemu projektu objednávateľa riadiacou radou projektu, resp. riadiaca rada projektu, ak vedúci projektu poskytovateľa a objednávateľa nedokážu zaujať spoločné stanovisko k prerokovávanej vecnej oblasti projektu alebo vedúci projektu objednávateľa nemá postačujúce oprávnenia rozhodovať o vecnej oblasti projektu. V prípade, že ani riadiaca rada projektu nemá dostatočné oprávnenia rozhodovať, o vecnej oblasti projektu rozhoduje štatutárny orgán objednávateľa.
Rozšírený pracovný deň	sú všetky dni okrem soboty, nedele, Nového roku, Veľkého piatku a Veľkonočného pondelka (podľa kalendára platného v sídle ECB), 1. mája, prvého sviatku vianočného a druhého sviatku vianočného.
Sprievodná dokumentácia dodaného (informačného) systému	sprievodnú dokumentáciu dodaného informačného systému predstavuje: vývojová dokumentácia dodaného informačného systému, technická dokumentácia dodaného informačného systému, používateľská dokumentácia dodaného informačného systému, inštalačná dokumentácia dodaného informačného systému.
Softvér tretej strany	zmluvné strany rozumejú softvérové programy, ktoré sú zabudované v systéme (licencovanom programe), alebo sú vyžadované na jeho používanie a ich výrobcom alebo autorom nie je poskytovateľ alebo ide o softvérové programy vytvorené poskytovateľom, s ktorými poskytovateľ bežne obchoduje na trhu formou predaja licencií.

Pojem (y) / Výraz / Skratka	Vysvetlenie Pojmu / Výrazu / Skratky
Systém na zaznamenávanie prevádzkových incidentov	systém určený na evidovanie prevádzkových incidentov/vád/ chýb/nedostatkov zistených pri prevádzke dodaného informačného systému, alebo v súvislosti s prevádzkou dodaného informačného systému alebo incidentov zistených počas overovania funkčnosti dodaného informačného systému (akceptačného testovania).
SW	Softvér - programové vybavenie počítača; vybavenie počítača programovacím jazykom a programom, programové vybavenie počítača (na rozdiel od technického vybavenia, hardvéru)
Testovacie prostredie	zmluvné strany rozumejú technické zariadenia a programové vybavenie (softvér) a všetky údaje nachádzajúce sa u objednávateľa vrátane nastavenia ich parametrov určené k akceptačnému testovaniu dodaného informačného systému.
Účastník servisnej služby	účastníkmi servisnej služby sú výhradne zmluvné strany, t. j. objednávateľ a poskytovateľ.
Výkaz	zmluvné strany rozumejú tlačový výstup vyhotovený vo formáte a grafickej úprave, ktorý je predpísaný internými aktmi riadenia objednávateľa alebo všeobecne záväznými právnymi predpismi. Vzor každého výkazu je uvedený v tejto zmluve. Tlač môže byť vykonávaná na (čistý) papier formátu A4 a A3 podľa formátu požadovaného výkazu.
Vývojové prostredie	dodaný informačná systém, ktorý je inštalovaný a sprístupnený v mieste poskytovateľa a/alebo objednávateľa.
Zmluva, zmluva, táto Zmluva, tejto Zmluvy,	rozumie sa zmluva číslo č. C-NBS1-000-080-754.Uvedený pojem zahŕňa zmluvu vrátane všetkých príloh, ktoré tvoria jej neoddeliteľnú súčasť a každý iný dokument, ktorý sa dohodne medzi stranami a výslovne určí, aby tvoril súčasť tejto zmluvy a zahŕňa každú zmenu tejto zmluvy, ktorú zmluvné strany dohodli písomne.
Zmluvná strana	rozumie sa objednávateľ alebo poskytovateľ.
Lehota služby	rozumie sa časové obdobie, počas ktorého je poskytovateľ povinný dokončiť vykonávanie príslušnej činnosti od prevzatia požiadavky objednávateľa na jej vykonanie. V prípade zásadného, závažného incidentu môže poskytovateľ navrhnúť náhradné riešenie, čím však nie je zbavený povinností vyriešiť incident v náhradnom termíne dohodnutom objednávateľom. Pre účely zmluvných pokút za nedodržanie lehoty služby sa poskytnutie náhradného riešenia chápe ako vyriešenie incidentu.
Podozrivá udalosť	anomália, neštandardné správanie, podozrivá aktivita, identifikované narušenie bezpečnosti, opakované neúspešné/úspešné pokusy o komunikáciu s podozrivými IP adresami, využívanie neštandardných portov, použitie nepovolených služieb (vzdialený prístup, anonymizačné služby, ťažba kryptomien, a pod.), atď.
Bezpečnostná hrozba	zverejnená/nahlásená/detegovaná bezpečnostná zraniteľnosť alebo varovanie, ktoré sa týka služby IT alebo niektorého jej komponentu.
Bezpečnostný incident	akákoľvek udalosť narušenia bezpečnosti IT infraštruktúry a IS NBS ktorej následkom je 1. strata dôvernosti údajov, únik/zničenie údajov alebo narušenie integrity, 2. obmedzenie alebo odmietnutie dostupnosti IT služby NBS, poškodenie mena NBS
Prevádzkový incident	akákoľvek udalosť ktorá je spôsobená správou a prevádzkou IT infraštruktúry a IS NBS.
Rozšírený pracovný deň	sú všetky dni okrem soboty, nedele, Nového roku, Veľkého piatku a Veľkonočného pondelka (podľa kalendára platného v sídle ECB), 1. mája, prvého sviatku vianočného a druhého sviatku vianočného.

II. Použité skratky

Skratka	Vysvetlenie Skratky
HTP	Hlavné technologické pracovisko (ústredie NBS) – Imricha Karvaša 1, 813 25 Bratislava
ZTP	Záložné technologické pracovisko - Kopčianska ulica 92/D, Bratislava
AD	Active Directory
ADS	Anomaly Detection System
BAS	Breach and Attack Simulation
SIEM	Security Information and Event Management
MBIT	Monitoring bezpečnosti informačných technológií zahŕňa technológie SIEM a NDR
Flowmon OS	Flowmon Operating System
Flowmon ADS	Flowmon Anomaly Detection System
Flowmon FMC	Flowmon Monitoring Center
OS	operačný systém
AI	korelačná jednotka
DC	Data Collector
DI	Data Indexer
DP	Data Processor
DR	Disaster Recovery
FM	Flowmon
HW	Hardware
LS	Log Source
NBS	Národná banka Slovenska
NDR	Network Detection and Response
NM	Network Monitor
OS	operačný systém
PM	Platform Manager
SW	Software
UC	use-case NBS
WC	Web Console
XM	all-in-one appliance, ktorá obsahuje všetky moduly riešenia SIEM
IS	informačný systém
SAN	Storage Area Network
SOC	Security Operation Center
Barracuda WAF	Barracuda Web Application Firewall
Trellix ATD	Trellix Advanced Threat Defense
Trellix ePO	Trellix ePolicy Orchestrator
Trellix EDR	Trellix MVISION Endpoint Detection and Response
NGFW	Next-Generation Firewalls
IDS	Intrusion Detection Systems
IPS	Intrusion Prevention Systems
EDR	Endpoint Detection and Response
DLP	Data Leakage Prevention
DLP	Data Leakage Prevention
Interný SOC tím	**Interný SOC tím** – tvoria zamestnanci NBS
Externý SOC tím	**Externý SOC tím** - tvoria zamestnanci dodávateľa

Príloha 5 k zmluve č. C-NBS1-000-106-915

Zoznam subdodávateľov

Zoznam subdodávateľov

V súlade s ustanovením § 41 ods. 3 zákona o verejnom obstarávaní verejný obstarávateľ **požaduje od úspešného uchádzača (poskytovateľa), aby najneskôr v čase uzavretia Zmluvy uviedol**:

1. údaje všetkých známych subdodávateľoch v rozsahu obchodné meno, sídlo, IČO, zápis do príslušného obchodného registra
2. údaje o osobe oprávnenej konať za subdodávateľa v rozsahu meno a priezvisko, adresa pobytu, dátum narodenia.

Úspešný uchádzač môže pridať toľko riadkov v tabuľke koľko potrebuje.
V prípade, ak úspešný uchádzač nebude mať subdodávateľov uvedie túto skutočnosť v tabuľke.

p. č.	Subdodávateľ	Údaje o osobe oprávnenej konať za subdodávateľa
1.	ANECT a.s. Purkyňova 646/107, Medlánky, 612 00 Brno Česká republika	
2.	COMGUARD a.s. Sochorova 3209/38, Žabovřesky, 616 00 Brno Česká republika	
3.	Validato s.r.o. Dělnická 213/12, Holešovice, 170 00 Praha 7 Česká republika	

Príloha 7 k Zmluve č. C-NBS1-000-160-915

Zoznam pracovníkov poskytovateľa

1 ZOZNAM KĽÚČOVÝCH PRACOVNÍKOV POSKYTOVATEĽA A POŽIADAVKY NA ICH TECHNICKÚ A ODBORNÚ SPÔSOBILOSŤ

1.1 Objednávateľ požaduje, aby poskytovateľ uviedol v tomto zozname všetkých jeho pracovníkov, ktorí boli predmetom vyhodnocovania podmienok účasti a vyhodnocovania kritéria č. 2 a zároveň im boli pridelené body za toto kritérium v zákazke *Monitoring kybernetickej bezpečnosti*.

p. č.	Pracovník poskytovateľa (meno, priezvisko)	Kľúčový pracovník/expert (požiadavky z podmienok účasti v rámci verejného obstarávania)	Mobilné alebo telefónne číslo	E-mailová adresa	
1.	xxx	**Expert na architektúru systémov kybernetickej bezpečnosti má:** - **odbornú prax na pozícii experta na architektúru systémov kybernetickej bezpečnosti v trvaní minimálne 5 rokov**. Rola experta na architektúru systémov kybernetickej bezpečnosti predstavuje výkon činností a s tým spojenú zodpovednosť za plánovanie a návrh bezpečnostnej infraštruktúry a poskytovanie súčinnosti pri jej implementácii. Expert na architektúru systémov kybernetickej bezpečnosti sleduje nové verzie bezpečnostných systémov, záplat a vylepšení a navrhuje ich spôsob a čas implementácie a zároveň dohliada na ich správnu a včasnú implementáciu, *pričom túto podmienku účasti preukazuje uchádzač predložením odborného profesijného životopisu osoby určenej ako expert na architektúru systémov bezpečnosti;* - **minimálne jednu osobnú praktickú skúsenosť** na pozícii experta na architektúru systémov kybernetickej bezpečnosti v zákazke, ktorej predmetom bolo nasadzovanie alebo prevádzka alebo poskytovanie SOC (Security Operation Center) alebo SIEM (Security Information and Event Management) alebo NDR (Network Detection and Response) alebo ich vzájomná ľubovoľná kombinácia s minimálne 200 servermi a sieťovými zariadeniami alebo prevádzka SOC a NDR v prostredí s aspoň 200 servermi a sieťovými zariadeniami, a to za predchádzajúcich päť (5) rokov počítaných od vyhlásenia verejného obstarávania, pričom *túto podmienku účasti preukazuje uchádzač predložením odborného profesijného životopisu osoby určenej ako expert na architektúru systémov kybernetickej bezpečnosti a túto podmienku účasti môže uchádzač preukázať jednou alebo dvoma osobami;* - **minimálne jeden certifikát** so zameraním na architektúru systémov kybernetickej bezpečnosti, *túto podmienku účasti preukazuje uchádzač predložením kópie certifikátu;*	xxx	xxx	
2.	xxx	- **SOC Manager má:** - **minimálne jednu osobnú praktickú skúsenosť** na pozícii SOC Managera v zákazke, ktorej predmetom bolo nasadzovanie alebo prevádzka alebo poskytovanie SOC (Security Operation Center) alebo SIEM (Security Information and Event Management) alebo NDR (Network Detection and Response) alebo ich vzájomná ľubovoľná kombinácia s minimálne 200 servermi a sieťovými zariadeniami alebo prevádzka SOC a NDR v prostredí s aspoň 200 servermi a sieťovými zariadeniami, a to za predchádzajúcich päť (5) rokov počítaných od vyhlásenia verejného obstarávania, pričom *túto podmienku účasti preukazuje uchádzač predložením odborného profesijného životopisu osoby určenej ako SOC Manager a uchádzač môže túto podmienku účasti preukázať jednou alebo dvoma osobami;* - **minimálne jeden certifikát** so zameraním na kybernetickú bezpečnosť, *túto podmienku účasti preukazuje uchádzač predložením kópie certifikátu;*	xxx	xxx	
3.	xxx	SOC **Operátor/analytik má:** - **odbornú prax na pozícii SOC Operatéra/analytika v trvaní minimálne 2 roky.** Rola SOC Operátora/analytika predstavuje činnosti ako monitorovanie a kontrolu alarmov a hrozieb, potvrdením, určením alebo úpravou kritickosti výstrah a ich obohatením o relevantné údaje, identifikáciou opodstatnenosti, resp. falošnej pozitivity alarmov a hrozieb, identifikácia ďalších vysoko rizikových udalostí a potenciálnych incidentov, monitorovaním a vyhodnocovanie prevádzky bezpečnostných nástrojov, riadením a konfiguráciou monitorovacích nástrojov, pričom túto podmienku účasti preukazuje uchádzač predložením odborného profesijného životopisu osoby určenej ako SOC Operátor/analytik; **minimálne jednu osobnú praktickú skúsenosť** na pozícii SOC Operátor/analytik v zákazke, ktorej predmetom bolo nasadzovanie alebo prevádzka alebo poskytovanie SOC (Security Operation Center) alebo SIEM (Security Information and Event Management) alebo NDR (Network Detection and Response) alebo ich vzájomná ľubovoľná kombinácia s minimálne 200 servermi a sieťovými zariadeniami alebo prevádzka SOC a NDR v prostredí s aspoň 200 servermi a sieťovými zariadeniami, a to za predchádzajúcich päť (5) rokov počítaných od vyhlásenia verejného obstarávania, pričom *túto podmienku účasti preukazuje uchádzač predložením odborného profesijného životopisu osoby určenej ako SOC Operátor/analytik;* **minimálne jeden certifikát** so zameraním na kybernetickú bezpečnosť, *túto podmienku účasti preukazuje uchádzač predložením kópie certifikátu;*	xxx	xxx	

4.	xxx	SOC **Operátor/analytik má:** - **odbornú prax na pozícii SOC Operatéra/analytika v trvaní minimálne 2 roky.** Rola SOC Operátora/analytika predstavuje činnosti ako monitorovanie a kontrolu alarmov a hrozieb, potvrdením, určením alebo úpravou kritickosti výstrah a ich obohatením o relevantné údaje, identifikáciou opodstatnenosti, resp. falošnej pozitivity alarmov a hrozieb, identifikácia ďalších vysoko rizikových udalostí a potenciálnych incidentov, monitorovaním a vyhodnocovanie prevádzky bezpečnostných nástrojov, riadením a konfiguráciou monitorovacích nástrojov, pričom túto podmienku účasti preukazuje uchádzač predložením odborného profesijného životopisu osoby určenej ako SOC Operátor/analytik; **minimálne jednu osobnú praktickú skúsenosť** na pozícii SOC Operátor/analytik v zákazke, ktorej predmetom bolo nasadzovanie alebo prevádzka alebo poskytovanie SOC (Security Operation Center) alebo SIEM (Security Information and Event Management) alebo NDR (Network Detection and Response) alebo ich vzájomná ľubovoľná kombinácia s minimálne 200 servermi a sieťovými zariadeniami alebo prevádzka SOC a NDR v prostredí s aspoň 200 servermi a sieťovými zariadeniami, a to za predchádzajúcich päť (5) rokov počítaných od vyhlásenia verejného obstarávania, pričom *túto podmienku účasti preukazuje uchádzač predložením odborného profesijného životopisu osoby určenej ako SOC Operátor/analytik;* **minimálne jeden certifikát** so zameraním na kybernetickú bezpečnosť, *túto podmienku účasti preukazuje uchádzač predložením kópie certifikátu;*	xxx	xxx	
5.	xxx	SOC **Operátor/analytik má:** - **odbornú prax na pozícii SOC Operatéra/analytika v trvaní minimálne 2 roky.** Rola SOC Operátora/analytika predstavuje činnosti ako monitorovanie a kontrolu alarmov a hrozieb, potvrdením, určením alebo úpravou kritickosti výstrah a ich obohatením o relevantné údaje, identifikáciou opodstatnenosti, resp. falošnej pozitivity alarmov a hrozieb, identifikácia ďalších vysoko rizikových udalostí a potenciálnych incidentov, monitorovaním a vyhodnocovanie prevádzky bezpečnostných nástrojov, riadením a konfiguráciou monitorovacích nástrojov, pričom túto podmienku účasti preukazuje uchádzač predložením odborného profesijného životopisu osoby určenej ako SOC Operátor/analytik; **minimálne jednu osobnú praktickú skúsenosť** na pozícii SOC Operátor/analytik v zákazke, ktorej predmetom bolo nasadzovanie alebo prevádzka alebo poskytovanie SOC (Security Operation Center) alebo SIEM (Security Information and Event Management) alebo NDR (Network Detection and Response) alebo ich vzájomná ľubovoľná kombinácia s minimálne 200 servermi a sieťovými zariadeniami alebo prevádzka SOC a NDR v prostredí s aspoň 200 servermi a sieťovými zariadeniami, a to za predchádzajúcich päť (5) rokov počítaných od vyhlásenia verejného obstarávania, pričom *túto podmienku účasti preukazuje uchádzač predložením odborného profesijného životopisu osoby určenej ako SOC Operátor/analytik;* **minimálne jeden certifikát** so zameraním na kybernetickú bezpečnosť, *túto podmienku účasti preukazuje uchádzač predložením kópie certifikátu;*	xxx	xxx	
6.	xxx	SOC **Operátor/analytik má:** - **odbornú prax na pozícii SOC Operatéra/analytika v trvaní minimálne 2 roky.** Rola SOC Operátora/analytika predstavuje činnosti ako monitorovanie a kontrolu alarmov a hrozieb, potvrdením, určením alebo úpravou kritickosti výstrah a ich obohatením o relevantné údaje, identifikáciou opodstatnenosti, resp. falošnej pozitivity alarmov a hrozieb, identifikácia ďalších vysoko rizikových udalostí a potenciálnych incidentov, monitorovaním a vyhodnocovanie prevádzky bezpečnostných nástrojov, riadením a konfiguráciou monitorovacích nástrojov, pričom túto podmienku účasti preukazuje uchádzač predložením odborného profesijného životopisu osoby určenej ako SOC Operátor/analytik; **minimálne jednu osobnú praktickú skúsenosť** na pozícii SOC Operátor/analytik v zákazke, ktorej predmetom bolo nasadzovanie alebo prevádzka alebo poskytovanie SOC (Security Operation Center) alebo SIEM (Security Information and Event Management) alebo NDR (Network Detection and Response) alebo ich vzájomná ľubovoľná kombinácia s minimálne 200 servermi a sieťovými zariadeniami alebo prevádzka SOC a NDR v prostredí s aspoň 200 servermi a sieťovými zariadeniami, a to za predchádzajúcich päť (5) rokov počítaných od vyhlásenia verejného obstarávania, pričom *túto podmienku účasti preukazuje uchádzač predložením odborného profesijného životopisu osoby určenej ako SOC Operátor/analytik;* **minimálne jeden certifikát** so zameraním na kybernetickú bezpečnosť, *túto podmienku účasti preukazuje uchádzač predložením kópie certifikátu;*	xxx	xxx	
7.	xxx	SOC **Operátor/analytik má:** - **odbornú prax na pozícii SOC Operatéra/analytika v trvaní minimálne 2 roky.** Rola SOC Operátora/analytika predstavuje činnosti ako monitorovanie a kontrolu alarmov a hrozieb, potvrdením, určením alebo úpravou kritickosti výstrah a ich obohatením o relevantné údaje, identifikáciou opodstatnenosti, resp. falošnej pozitivity alarmov a hrozieb, identifikácia ďalších vysoko rizikových udalostí a potenciálnych incidentov, monitorovaním a vyhodnocovanie prevádzky bezpečnostných nástrojov, riadením a konfiguráciou monitorovacích nástrojov, pričom túto podmienku účasti preukazuje uchádzač predložením odborného profesijného životopisu osoby určenej ako SOC Operátor/analytik; **minimálne jednu osobnú praktickú skúsenosť** na pozícii SOC Operátor/analytik v zákazke, ktorej predmetom bolo nasadzovanie alebo prevádzka alebo poskytovanie SOC (Security Operation Center) alebo SIEM (Security Information and Event Management) alebo NDR (Network Detection and Response) alebo ich vzájomná ľubovoľná kombinácia s minimálne 200 servermi a sieťovými zariadeniami alebo prevádzka SOC a NDR v prostredí s aspoň 200 servermi a sieťovými zariadeniami, a to za predchádzajúcich päť (5) rokov počítaných od vyhlásenia verejného obstarávania, pričom *túto podmienku účasti preukazuje uchádzač predložením odborného profesijného životopisu osoby určenej ako SOC Operátor/analytik;* **minimálne jeden certifikát** so zameraním na kybernetickú bezpečnosť, *túto podmienku účasti preukazuje uchádzač predložením kópie certifikátu;*	xxx	xxx	

8.	xxx	SOC **Operátor/analytik má:** - **odbornú prax na pozícii SOC Operatéra/analytika v trvaní minimálne 2 roky.** Rola SOC Operátora/analytika predstavuje činnosti ako monitorovanie a kontrolu alarmov a hrozieb, potvrdením, určením alebo úpravou kritickosti výstrah a ich obohatením o relevantné údaje, identifikáciou opodstatnenosti, resp. falošnej pozitivity alarmov a hrozieb, identifikácia ďalších vysoko rizikových udalostí a potenciálnych incidentov, monitorovaním a vyhodnocovanie prevádzky bezpečnostných nástrojov, riadením a konfiguráciou monitorovacích nástrojov, pričom túto podmienku účasti preukazuje uchádzač predložením odborného profesijného životopisu osoby určenej ako SOC Operátor/analytik; **minimálne jednu osobnú praktickú skúsenosť** na pozícii SOC Operátor/analytik v zákazke, ktorej predmetom bolo nasadzovanie alebo prevádzka alebo poskytovanie SOC (Security Operation Center) alebo SIEM (Security Information and Event Management) alebo NDR (Network Detection and Response) alebo ich vzájomná ľubovoľná kombinácia s minimálne 200 servermi a sieťovými zariadeniami alebo prevádzka SOC a NDR v prostredí s aspoň 200 servermi a sieťovými zariadeniami, a to za predchádzajúcich päť (5) rokov počítaných od vyhlásenia verejného obstarávania, pričom *túto podmienku účasti preukazuje uchádzač predložením odborného profesijného životopisu osoby určenej ako SOC Operátor/analytik;* **minimálne jeden certifikát** so zameraním na kybernetickú bezpečnosť, *túto podmienku účasti preukazuje uchádzač predložením kópie certifikátu;*	xxx	xxx	
9.	xxx	**SOC Senior analytik** má**:** - **odbornú prax na pozícii SOC Senior analytika v trvaní minimálne 5 rokov;** Rola SOC Senior analytika predstavuje činnosti a zodpovednosť za spracovanie detailnej analýzy bezpečnostných incidentov eskalovaných SOC operátormi, návrhom a implementáciou stratégií na zvládnutie incidentov a zotavenie sa z nich, pričom túto podmienku účasti preukazuje uchádzač predložením odborného profesijného životopisu osoby určenej ako SOC Senior/analytik; **- minimálne jednu osobnú praktickú skúsenosť na pozícii SOC Senior analytik** v zákazke, ktorej predmetom bolo nasadzovanie alebo prevádzka alebo poskytovanie SOC (Security Operation Center) alebo SIEM (Security Information and Event Management) alebo NDR (Network Detection and Response) alebo ich vzájomná ľubovoľná kombinácia s minimálne 200 servermi a sieťovými zariadeniami alebo prevádzka SOC a NDR v prostredí s aspoň 200 servermi a sieťovými zariadeniami, a to za predchádzajúcich päť (5) rokov počítaných od vyhlásenia verejného obstarávania, pričom *túto podmienku účasti preukazuje uchádzač predložením odborného profesijného životopisu osoby určenej ako SOC Senior analytik;* - **minimálne jeden medzinárodný certifikát** so zameraním na minimálne jeden certifikát so zameraním na analýzu a riešenie kybernetických incidentov, *túto podmienku účasti preukazuje uchádzač predložením kópie certifikátu;* **uchádzač môže splniť požiadavky pre Senior analytika a Threat Huntera rovnakou osobou*	xxx	xxx	
10.	xxx	**SOC Senior analytik** má**:** - **odbornú prax na pozícii SOC Senior analytika v trvaní minimálne 5 rokov;** Rola SOC Senior analytika predstavuje činnosti a zodpovednosť za spracovanie detailnej analýzy bezpečnostných incidentov eskalovaných SOC operátormi, návrhom a implementáciou stratégií na zvládnutie incidentov a zotavenie sa z nich, pričom túto podmienku účasti preukazuje uchádzač predložením odborného profesijného životopisu osoby určenej ako SOC Senior/analytik; **- minimálne jednu osobnú praktickú skúsenosť na pozícii SOC Senior analytik** v zákazke, ktorej predmetom bolo nasadzovanie alebo prevádzka alebo poskytovanie SOC (Security Operation Center) alebo SIEM (Security Information and Event Management) alebo NDR (Network Detection and Response) alebo ich vzájomná ľubovoľná kombinácia s minimálne 200 servermi a sieťovými zariadeniami alebo prevádzka SOC a NDR v prostredí s aspoň 200 servermi a sieťovými zariadeniami, a to za predchádzajúcich päť (5) rokov počítaných od vyhlásenia verejného obstarávania, pričom *túto podmienku účasti preukazuje uchádzač predložením odborného profesijného životopisu osoby určenej ako SOC Senior analytik;* - **minimálne jeden medzinárodný certifikát** so zameraním na minimálne jeden certifikát so zameraním na analýzu a riešenie kybernetických incidentov, *túto podmienku účasti preukazuje uchádzač predložením kópie certifikátu;* **uchádzač môže splniť požiadavky pre Senior analytika a Threat Huntera rovnakou osobou*	xxx	xxx	
11.	xxx	**SOC Senior analytik** má**:** - **odbornú prax na pozícii SOC Senior analytika v trvaní minimálne 5 rokov;** Rola SOC Senior analytika predstavuje činnosti a zodpovednosť za spracovanie detailnej analýzy bezpečnostných incidentov eskalovaných SOC operátormi, návrhom a implementáciou stratégií na zvládnutie incidentov a zotavenie sa z nich, pričom túto podmienku účasti preukazuje uchádzač predložením odborného profesijného životopisu osoby určenej ako SOC Senior/analytik; **- minimálne jednu osobnú praktickú skúsenosť na pozícii SOC Senior analytik** v zákazke, ktorej predmetom bolo nasadzovanie alebo prevádzka alebo poskytovanie SOC (Security Operation Center) alebo SIEM (Security Information and Event Management) alebo NDR (Network Detection and Response) alebo ich vzájomná ľubovoľná kombinácia s minimálne 200 servermi a sieťovými zariadeniami alebo prevádzka SOC a NDR v prostredí s aspoň 200 servermi a sieťovými zariadeniami, a to za predchádzajúcich päť (5) rokov počítaných od vyhlásenia verejného obstarávania, pričom *túto podmienku účasti preukazuje uchádzač predložením odborného profesijného životopisu osoby určenej ako SOC Senior analytik;* - **minimálne jeden medzinárodný certifikát** so zameraním na minimálne jeden certifikát so zameraním na analýzu a riešenie kybernetických incidentov, *túto podmienku účasti preukazuje uchádzač predložením kópie certifikátu;* **uchádzač môže splniť požiadavky pre Senior analytika a Threat Huntera rovnakou osobou*	xxx	xxx	

12.	xxx	**Threat Hunter** má**:** - **odbornú prax na pozícii Threat Hunterov (analytikov historických záznamov) v trvaní minimálne 5 rokov;** Rola Threat Huntera predstavuje činnosti a zodpovednosť za prešetrovanie podozrivých udalostí, alarmov a hrozieb v dlhšom časovom úseku so zameraním na identifikáciu podozrivých vzorov správania a anomálií, identifikáciou možných vektorov útokov, bezpečnostných hrozieb a bezpečnostných slabín a návrhom optimalizácie nasadených bezpečnostných nástrojov, pričom t*úto podmienku účasti preukazuje uchádzač predložením odborného profesijného životopisu osoby určenej ako Threat Hunter;* - **minimálne jednu osobnú praktickú skúsenosť na pozícii Threat Hunter** v zákazke, ktorej predmetom bolo nasadzovanie alebo prevádzka alebo poskytovanie SOC (Security Operation Center) alebo SIEM (Security Information and Event Management) alebo NDR (Network Detection and Response) alebo ich vzájomná ľubovoľná kombinácia s minimálne 200 servermi a sieťovými zariadeniami alebo prevádzka SOC a NDR v prostredí s aspoň 200 servermi a sieťovými zariadeniami, a to za predchádzajúcich päť (5) rokov počítaných od vyhlásenia verejného obstarávania, pričom *túto podmienku účasti preukazuje uchádzač predložením odborného profesijného životopisu osoby určenej ako Threat Hunter;* **- minimálne jeden certifikát so zameraním na analýzu a riešenie kybernetických incidentov**, *túto podmienku účasti preukazuje uchádzač predložením kópie certifikátu;* **uchádzač môže splniť podmienky účasti pre SOC Senior analytika a Threat Huntera rovnakou osobou.*	xxx	xxx	
13.	xxx	**Threat Hunter** má**:** - **odbornú prax na pozícii Threat Hunterov (analytikov historických záznamov) v trvaní minimálne 5 rokov;** Rola Threat Huntera predstavuje činnosti a zodpovednosť za prešetrovanie podozrivých udalostí, alarmov a hrozieb v dlhšom časovom úseku so zameraním na identifikáciu podozrivých vzorov správania a anomálií, identifikáciou možných vektorov útokov, bezpečnostných hrozieb a bezpečnostných slabín a návrhom optimalizácie nasadených bezpečnostných nástrojov, pričom t*úto podmienku účasti preukazuje uchádzač predložením odborného profesijného životopisu osoby určenej ako Threat Hunter;* - **minimálne jednu osobnú praktickú skúsenosť na pozícii Threat Hunter** v zákazke, ktorej predmetom bolo nasadzovanie alebo prevádzka alebo poskytovanie SOC (Security Operation Center) alebo SIEM (Security Information and Event Management) alebo NDR (Network Detection and Response) alebo ich vzájomná ľubovoľná kombinácia s minimálne 200 servermi a sieťovými zariadeniami alebo prevádzka SOC a NDR v prostredí s aspoň 200 servermi a sieťovými zariadeniami, a to za predchádzajúcich päť (5) rokov počítaných od vyhlásenia verejného obstarávania, pričom *túto podmienku účasti preukazuje uchádzač predložením odborného profesijného životopisu osoby určenej ako Threat Hunter;* **- minimálne jeden certifikát so zameraním na analýzu a riešenie kybernetických incidentov**, *túto podmienku účasti preukazuje uchádzač predložením kópie certifikátu;* **uchádzač môže splniť podmienky účasti pre SOC Senior analytika a Threat Huntera rovnakou osobou.*	xxx	xxx	

Príloha č. 8 k Zmluve č. C-NBS1-000-160-915

Vzor výkazu

Ukončené služby

Por. č.	Typ služby	Krátky popis	ID Service Desk NBS	Dátum začiatku	Dátum ukončenia	Realizátor	Reklamácia	Plnenie služby	Poznámka
	požiadavka / incident / činnosť					meno a priezvisko - môže byť uvedených aj viac realizátorov	áno/ nie	Podľa časti: Monitorovanie a vyhodnocovanie poskytovaných služieb	

Neukončené služby

Por. č.	Typ služby	Krátky popis	ID Service Desk NBS	Dátum začiatku	Predpokladaný dátum ukončenia	Realizátor		Stav rozpracovanosti	Poznámka
	požiadavka/ incident/ činnosť					meno a priezvisko - môže byť uvedených aj viac realizátorov	prázdny stĺpec na zjednotenie formátu tabuliek	Slovný popis	

Služby dodané na hodinovú sadzbu

Por. č.	Krátky popis činnosti	ID Service Desk NBS	Dátum začiatku	Dátum ukončenia	Realizátor	Reklamácia	Odpracované hodiny	Hodinová sadzba bez DPH	Spolu bez DPH		Poznámka
					meno a priezvisko - max. jeden realizátor na jednom riadku	áno/ nie				prázdny stĺpec na zjednotenie formátu tabuliek	

Služby rozpracované na hodinovú sadzbu

Por. č.	Krátky popis činnosti	ID Service Desk NBS	Dátum začiatku	Predpokladaný dátum ukončenia	Realizátor		Doteraz odpracované hodiny	Hodinová sadzba bez DPH	Spolu bez DPH	Stav rozpracovanosti	Poznámka
					meno a priezvisko - max. jeden realizátor na jednom riadku	prázdny stĺpec na zjednotenie formátu tabuliek					

Mesačná štatistika služieb (bez služieb realizovaných na hodinovú sadzbu)

Mesiac	Celkový počet ukončených služieb v danom mesiaci	Počet ukončených služieb do stanoveného času v danom mesiaci	Percento ukončených služieb do stanoveného času v danom mesiaci	Počet ukončených služieb do dvojnásobku stanoveného času v danom mesiaci	Percento ukončených služieb do dvojnásobku stanoveného času v danom mesiaci	Počet ukončených služieb nad dvojnásobok stanoveného času v danom mesiaci	Percento ukončených služieb nad dvojnásobok stanoveného času v danom mesiaci	Počet nevykonaných služieb v danom mesiaci

Upozornenie:

Poskytovateľ v rámci ponuky predloží príslušné produktové certifikáty pre technológie SIEM, NDR, Skener zraniteľností a BAS preukazujúce kompetenciu implementovať, resp. používať tieto technológie vystavené minimálne na jednu osobu určenú na plnenie zmluvy (certifikáty a doklady v predložené cudzom jazyku inom ako v českom a anglickom jazyku, musia byť doplnené prekladom do slovenského jazyka. Originály predložených dokladov postačuje predložiť na požiadanie verejným obstarávateľom).

p.č.	názov položky	biele pole - slovný popis spôsobu naplnenia požiadavky, resp. deklarácia splnenia prožiadavky textom "spĺňa" alebo "nespĺňa", žlté pole - odkaz na dokumentáciu (názov, číslo strany, kapitola atď.), ktorá je súčasťou ponuky, kde sa dá overiť splnenie požiadavky <vyplní uchádzač>
	Všeobecné požiadavky na služby	
2.1	Všetky požadované služby sú poskytované na obdobie 5 rokov.	Spĺňa
2.2	Uchádzač v ponuke uvedie komunikačný jazyk (SK, CZ) v ktorom budú poskytované služby.	Spĺňa
2.3	Služby musia spĺňať požiadavky na architektúru uvedené v prílohách (Príloha č. 1 - Architektonické princípy NBS, Príloha č. 2 - Referenčná architektúra IS NBS a Príloha č.3 - Technologické štandardy NBS).	Spĺňa
2.4	Služby musia spĺňať požiadavky na bezpečnosť uvedené v prílohe (Príloha č.4 - Bezpečnostné požiadavky).	Spĺňa
2.5	Služby sú poskytované na technológiách umiestnených v cloude a/alebo on-site. (Pozn.: NBS počíta s tým, že potrebná infraštruktúra napr. MBIT bude umiestnená v prostredí NBS.)	Spĺňa
2.6	Potrebný SW a HW bude súčasťou dodávky služieb. NBS poskytne v obidvoch lokalitách montážne racky, pripojenie do dátovej a elektrickej siete, fyzický a vzdialený prístup, prístupy do NBS systémov, súčinnosť a pod.	Spĺňa
2.7	Všetky potrebné licencie a oprávnenia sú súčasťou dodávky služieb. Posledné 2 roky sú počty monitorovaných zariadení stabilné. Na základe skúseností NBS odhaduje možné medziročné navyšovanie objemov (počtu zariadení, udalostí, network flows a pod.) na úrovni 5 %. Je nepravdepodobné, že by došlo k výraznému poklesu.	Spĺňa
2.8	Súčasťou služieb je aj starostlivosť o technológie (prevádzka, inštalácia aktualizácií SW a bezpečnostných záplat a pod.).	Spĺňa
2.9	Služby sú poskytované primárne zabezpečeným vzdialeným prístupom. V prípade potreby a po vzájomnej dohode, služby je možné poskytovať v priestoroch NBS na vopred stanovenú dobu.	Spĺňa
2.10	SOC tím bude mať prístup do SD (riešenie žiadostí a incidentov) a podporných technológií NBS (Trellix ePO, Trellix ATD, Trellix EDR, Barracuda, WAF, Infoblox DNS, Fortinet a pod.) pre potreby prešetrovania bezpečnostných zistení v IT NBS.	Spĺňa
2.11	Služby sú poskytované minimálne v rozsahu súčasného monitoringu kybernetickej bezpečnosti vrátane integrácií s bezpečnostnými systémami (Trellix ATD, EPO, EDR, WebWasher, F5 DDoS a GenieATM DDoS, Barracuda WAF NBS, Excalibur a pod.) technickými (sieťové zariadenia, OS, DB, VMware, OpenShift a pod.) a aplikačnými systémami (SAP, SWIFT a pod.). Detailnejší popis je v kapitolách k jednotlivým technológiám.	Spĺňa
2.12	Migrácia custom use casov zo starého na nové prostredie.	Spĺňa
2.13	Súčasťou služieb sú aj reporty o ich stave a kvalite vrátane komponentov. Uchádzač na požiadanie odprezentuje stav poskytovaných služieb vrátane ich komponentov.	Spĺňa
2.14	Súčasťou dodávky sú všetky podporné nástroje (reportovací nástroj, denník bezpečnostných a prevádzkových zistení a pod.)	Spĺňa
2.15	Dodané riešenie, resp. poskytované služby a technológie sú v súlade, resp. podporujú medzinárodné štandardy, legislatívu, príp. organizáciu minimálne: NIST, NIS2, CIS, ISO/IEC 27001, GDPR a MITRE ATT&CK.	Spĺňa
2.16	NBS má zavedené procesy Disaster Recovery a Incident Response. Monitoring kybernetickej bezpečnosti je ich súčasťou. Od poskytovateľa služieb monitoringu kybernetickej bezpečnosti sa vyžaduje súčinnosť pri vzájomnom vyladení procesov ako aj participácia v daných procesoch.	Spĺňa
2.17	Pravidelné stretnutie členov tímu k optimalizácii a rozvoju služieb minimálne 1 x 14 dní.	Spĺňa
	Všeobecné požiadavky na technológie	
2.18	Architektúra bezpečnostných nástrojov a technológií vychádzajúca z princípov Cybersecurity Mesh Architecture (CSMA)	Spĺňa
2.19	Podpora autentifikácie v súlade referenčnou architektúrou IS NBS (Príloha č. 2 - Referenčná architektúra IS NBS).	Spĺňa
2.20	Zber bezpečnostných udalostí z celého IT prostredia a bezpečnostných technológií v reálnom čase do jedného úložiska.	Spĺňa
2.21	Centrálny dashboard pre potreby investigácie a analýzy bezpečnostných zistení.	Spĺňa
2.22	Centrálny dashboard aktuálneho stavu jednotlivých komponentov bezpečnostných technológií.	Spĺňa
2.23	Personalizované prístupy pre zamestnancov NBS do dashboardov jednotlivých technológií minimálne s read only prístupovými právami s možnosťou vytvárať custom pohľady a reporty.	Spĺňa
2.24	Centrálne nastavenie metód na automatické vyhodnotenie bezpečnostných udalostí.	Spĺňa
2.25	Metódy na automatické vyhodnotenie bezpečnostných udalostí využívajúce ML/AI.	Spĺňa
2.26	Centrálne nastavenie rizikového skóre pre systémy a vyhodnocovacie metódy a výpočet celkového rizikového skóre.	Spĺňa
2.27	Centrálny alertovací systém na základe celkového rizikového skóre.	Spĺňa
2.28	Centrálny notifikačný systém (mail, sms).	Spĺňa
2.29	Centrálny reportovací systém (vyhodnotenie dostupnosti komponentov, štatistické údaje o počtoch a dobe riešenia riešených bezpečnostných udalostí, detailné informácie o riešení bezpečnostných udalostí, type a počte alertov, štatistické údaje o počtoch zbieraných udalostí, ich spracovaní, počte monitorovaných systémov, databáz, ...).	Spĺňa
2.30	Centralizované playbook-y a automatizácia pri reakcii na bezpečnostné udalosti formou semiautomatických reakcií (napr. pred vykonaním nápravnej akcie bude potrebné manuálne potvrdenie)	Spĺňa
	Všeobecné požiadavky na on-site technológie, každé on-site dodané zariadenie musí:	
2.31	obsahovať min. 2 redundantné napájacie zdroje	Spĺňa - https://d117h1jjiq768j.cloudfront.net/docs/default-source/flowmon-resources/2024-12-flowmon_collector_specification.pdf?sfvrsn=90711628_92, str.7 Gen6 Appliance Environmental Specs.pdf
2.32	byť montovateľné do štandardného 19'' technologického stojana (montážna sada súčasťou dodávky)	Spĺňa - https://d117h1jjiq768j.cloudfront.net/docs/default-source/flowmon-resources/2024-12-flowmon_collector_specification.pdf?sfvrsn=90711628_92, spĺňa str.7 Gen6 Appliance Environmental Specs.pdf
2.33	mať pripojenie ku dvom samostatným zdrojom napájania 230V dĺžka káblov min. 3m ukončenými IEC 60 884-1 a IEC320 C14 (oba typy napájacích káblov sú súčasťou dodávky)	Spĺňa - https://d117h1jjiq768j.cloudfront.net/docs/default-source/flowmon-resources/2024-12-flowmon_collector_specification.pdf?sfvrsn=90711628_92, spĺňa Kabel sieťový IEC320 C14 - C19, 3x 1,5mm2, 3m.pdf a Kabel sieťový predlžovací IEC320 C14 - IEC320 C13, 3m.pdf
2.34	musí spĺňať požiadavky na kabeláž (Príloha č. 5 - PARAMATRE OPTICKÝCH KOMPONENTOV a Príloha č. 6 - PARAMATRE PRE METALICKÚ ŠTRUKTÚROVANÚ KABELÁŽ). Každé technologické zariadenie zapájané do sieťovej infraštruktúry NBS musí pripojené minimálne 10 Gbps optikou v multimode, pričom z dôvodu vysokej dostupnosti bude pripojené do dvoch nezávislých switchov. Výnimku na pripojenie má vzdialený LAN manažment, ktorý môže byť pripojený cez metalické pripojenie minimálne 1 Gbps.	Spĺňa
2.35	obsahovať všetky potrebné HW a SW komponenty vrátane všetkých licencií umožňujúce ich používať a spravovať v prostredí NBS od prvého dňa nasadenia	Spĺňa
2.36	mať synchronizovaný čas z NTP	Spĺňa
2.37	byť navrhnuté minimálne s výhľadom na 5 rokov od podpisu zmluvy, dodávateľ bude počas tejto doby poskytovať na dodané zariadenia zmluvný servis ako aj priebežné aktualizácie, vrátane bezpečnostných	Spĺňa
2.38	byť postavené na štandardných HW a SW produktoch výrobcov	Spĺňa
2.39	spĺňať podmienku, že v čase predloženia ponuky nie je na zozname výrobcu oznamujúcom koniec predaja (End of Sale) alebo koniec životnosti (End of Life)	Spĺňa
2.40	byť komponentovo nezávislé od prvkov sieťovej infraštruktúry, tak aby po výmene sieťových komponentov tej istej kategórie od rovnakého výrobcu nedošlo k obmedzeniu alebo znefunkčneniu upgradovaného riešenia	Spĺňa
2.41	obsahovať firmvér alebo operačný systém v poslednej výrobcom doporučenej verzii v čase predloženia ponuky pre daný typ zariadenia a takisto rovnaké typy zariadení musia obsahovať rovnaký firmvér alebo operačný systém	Spĺňa
2.42	musia umožniť ich vzdialený manažment cez dedikovaný LAN manažment port.	Spĺňa - https://d117h1jjiq768j.cloudfront.net/docs/default-source/flowmon-resources/2024-12-flowmon_collector_specification.pdf?sfvrsn=90711628_92, spĺňa str.7 Gen6 Appliance Environmental Specs.pdf https://d117h1jjiq768j.cloudfront.net/docs/default-source/flowmon-resources/2024-12-flowmon_probe_specificationd3f59d3395354fb78859a6757e4e9506.pdf?sfvrsn=b7d1fab4_102

Ciele služby SOC:
Cieľom služby je vyhľadávanie a prešetrenie podozrivých log záznamov, udalostí a alarmov a spolupodieľanie na riešení bezpečnostných incidentov.

Časový harmonogram poskytovania služby SOC:
Režim 24/7 alebo 15/5 (počas rozšírených pracovných dní v čase od 6.00h do 21.00h) okrem činností uvedených v bodoch 2.51, 2.52 a 2.53.

Monitorovanie a vyhodnocovanie poskytovaných služieb SOC:
Služba sa považuje za riadne poskytnutú, ak sú splnené všetky nasledovné minimálne podmienky:
a) Všetky prešetrenia bezpečnostných zistení sú evidované.
b) Riešenie podozrivej udalosti, bezpečnostnej hrozby alebo prevádzkového incidentu začne najneskôr do 8 hodín od rozhodnutia v úvodnom prešetrení a kategorizácii, že sa jedná o podozrivú udalosť, bezpečnostnú hrozbu alebo prevádzkový incident.
c) Detailné prešetrenie bezpečnostného incidentu začne najneskôr do 2 hodín od rozhodnutia, že sa jedná o bezpečnostný incident.
d) Poskytovanie súčinnosti internému SOC tímu pri riešení bezpečnostných incidentov až do ich vyriešenia.
e) Reporty o stave riešenia bezpečnostných zistení (Počet nových/vyriešených zistení, priemerná doba riešenia zistení za obdobie 7 dní/mesiac/štvrťrok, filtrovanie zistení podľa kategórií, detailné informácie o priebehu riešenia zistení a pod.) formou dashboardu.

p.č.	názov položky	biele pole - slovný popis spôsobu naplnenia požiadavky, resp. deklarácia splnenia prožiadavky textom "spĺňa" alebo "nespĺňa", žlté pole - odkaz na dokumentáciu (názov, číslo strany, kapitola atď.), ktorá je súčasťou ponuky, kde sa dá overiť splnenie požiadavky <vyplní uchádzač>
	Požiadavky na službu SOC	
2.43	Priebežné monitorovanie bezpečnostných udalostí v IT NBS pomocou nástrojov SIEMu.	Spĺňa. Priebežné monitorovanie bezpečnostných udalostí je zabezpečené tímom SOC z režimového pracoviska s obmedzeným prístupom s využitím nástroja SIEM – Logrythm, ktorého architektúra je opísaná v príslušnej časti tohto dokumentu.
2.44	Detekcia bezpečnostných zistení v nazbieraných dátach.	Spĺňa. Detekcia bezpečnostných udalostí prebieha v rámci dohodnutých SLA na základe detekčných pravidiel nastavených v nástroji SIEM.
2.45	Evidencia, kategorizácia a prioritizácia prešetrovaných bezpečnostných zistení.	Spĺňa
2.46	Úvodné prešetrenie bezpečnostných zistení a rozhodnutie či sa jedná o podozrivú udalosť, bezpečnostnú hrozbu, bezpečnostný incident alebo prevádzkový incident.	Spĺňa. Úvodné prešetrenie bezpečnostných udalostí vykonáva certifikovaný SOC operátor na úrovni L1 podľa vopred definovaných postupov a best practices. V prípade akejkoľvek nejasnosti alebo podozrenia na bezpečnostnú udalosť alebo incident eskaluje bezpečnostné zistenie na úroveň Senior SOC analytika.
2.47	Detailné prešetrenie bezpečnostných incidentov, t.j. zistenie príčiny a súvislostí vzniku bezpečnostného incidentu, vykonanie analýzy rozsahu a dopadu na IT NBS.	Spĺňa
2.48	Nahlásenie prevádzkových incidentov správcom dotknutých systémov do Service Desku NBS.	Spĺňa. Zistené prevádzkové udalosti sú podľa stanovených SLA hlásené do ServiceDesku NBS.
2.49	Nahlásenie bezpečnostných incidentov do Service Desku NBS. Bezpečnostné incidenty s vysokou prioritou (ktoré neznesú odklad) nahlásiť aj telefonicky na dedikované telefónne číslo.	Spĺňa
2.50	Poskytovať súčinnosť pri riešení bezpečnostných incidentov až do ich úplného vyriešenia a odstránenia dôsledkov. Aktívny zásah je v kompetencii zamestnancov NBS.	Spĺňa. Súčinnosť je poskytovaná naprieč všetkými rolami podieľajúcimi sa na službe SOC podľa vopred dohodnutých postupov a best practices.
2.51	Poskytovať súčinnosť pri riešení ostatných bezpečnostných zistení až do ich úplného vyriešenia a odstránenia dôsledkov v režime 8/5. Aktívny zásah je v kompetencii zamestnancov NBS.	Spĺňa.Súčinnosť je poskytovaná naprieč všetkými rolami podieľajúcimi sa na službe SOC podľa vopred dohodnutých postupov a best practices.
2.52	V rámci prešetrovania bezpečnostných zistení, ak je to možné, navrhovať opatrenia na zamedzenie ich opakovania, alebo vypracovať návrh na zabezpečenie včasnej identifikácie v prípade opakovania. V prípade identifikácie falošného poplachu navrhnúť opatrenia na zamedzenie jeho opakovania.	Spĺňa
2.53	Analýza historických dát, t.j. minimálne 1x za týždeň prehľadanie a prešetrenie podozrivých log záznamov, udalostí a alarmov so zameraním na identifikáciu podozrivých vzorov správania a anomálií v dlhšom časovom úseku.	Spĺňa
	Požiadavky na technológiu SOC	
2.54	Denník bezpečnostných zistení určený na evidenciu riešenia bezpečnostných zistení.	Spĺňa
2.55	Komunikačný systém na medzi SOC tímom a NBS správcami prepojený s denníkom bezpečnostných zistení (v súčasnosti sa na komunikáciu medzi SOC tímom a NBS správcami využívajú TEAMS kanály).	Spĺňa
2.56	Integrácia denníka bezpečnostných zistení so Service Deskom NBS (CA Service Desk).	Spĺňa
2.57	Zabezpečenie komunikácie SOC tímu s CSIRT, CERT a inými bezpečnostnými platformami (v súčasnosti na prijímanie emailových upozornení).	Spĺňa

Ciele služby MBIT (SIEM a NDR):
Cieľom služby je monitorovanie a zabezpečenie dostupnosti, výkonu a funkčnosti komponentov MBIT, nepretržitého zberu a spracovania logov a sieťových tokov, vykonávanie bežných prevádzkových činností MBIT za účelom zabezpečenia funkčnosti a aktuálnosti jednotlivých komponentov MBIT a zabezpečenia nepretržitého zberu a spracovania logov z monitorovaných zariadení. Aktivity sú rozdelené do 2 služieb: Monitoring a prevádzka MBIT a Rozvoj a optimalizácia MBIT.

Ciele služby monitoring a prevádzka MBIT:
Cieľom služby je najmä monitorovanie a zabezpečenie dostupnosti, výkonu a funkčnosti komponentov MBIT a nepretržitého zberu a spracovania logov z existujúcich zdrojov logov. Na monitorovanie dostupnosti MBIT komponentov sa okrem MBIT nástrojov môže využiť aj v NBS používaná technológia Zabbix.

Časový harmonogram poskytovania služieb monitoringu a prevádzky MBIT:
Režim 24/7 alebo 15/5 (počas rozšírených pracovných dní v čase od 6.00h do 21.00h)

Monitorovanie a vyhodnocovanie poskytovaných monitoringu a prevádzky MBIT:
Služba sa považuje za riadne poskytnutú, ak sú splnené všetky nasledovné minimálne podmienky:
a) Všetky identifikované prevádzkové incidenty sú evidované.
b) Vyriešenie prevádzkového incidentu v stanovenom čase.
c) Poskytovanie súčinnosti pri riešení prevádzkových incidentov až do ich vyriešenia.
d) Dostupnosť komponentov MBIT vyhodnocovaná na dennej báze formou dashboardu.

Ciele služby rozvoja a optimalizácie MBIT:
Cieľom služby je najmä tvorba a úprava konfigurácie komponentov MBIT, vytváranie nových a údržba existujúcich use casov. Takisto cieľom služby je pravidelné vyhľadávanie anomálií v nazbieraných dátach, stavu parsovania udalostí a posudzovanie kvality fungovania vyhodnocovania bezpečnostných udalostí komponentmi MBIT za dlhšie časové obdobie, vypracovávanie odporúčaní a návrhov na zlepšenie kvality fungovania zberu a vyhodnocovania bezpečnostných udalostí. Obsahom služby je aj pravidelná účasť na stretnutiach členov tímu spravujúceho MBIT, analýza zistených nedostatkov a návrh obsahovej náplne a ďalšieho rozvoja celého systému na zber a vyhodnocovanie bezpečnostných udalostí. Teda napr. čo, prečo a ako má byť logované a monitorované, aké reporty a alarmy je odporúčané v prostredí NBS vytvoriť, analýza falošných poplachov (false positive) a návrh riešení za účelom ich eliminácie a pod.

Časový harmonogram poskytovania služieb rozvoja a optimalizácie MBIT:
Počas pracovných dní v čase od 8.00h do 16.30h (režim 8/5).

Monitorovanie a vyhodnocovanie poskytovaných služieb rozvoja a optimalizácie MBIT:
Služba sa považuje za riadne poskytnutú, ak sú splnené všetky nasledovné minimálne podmienky:
a) Požadovaná úprava je vykonaná podľa požiadaviek NBS a v stanovenom čase.
b) Use case je zrealizovaný podľa požiadaviek NBS a v stanovenom čase.
c) Všetky zmeny v konfigurácii MBIT sú zaznamenané v prevádzkovom denníku MBIT.
d) Reporty o anomáliách (napr. výrazne zvýšený/znížený počet udalostí, nové typy alebo udalosti ktoré prestali chodiť a pod.) – minimálne 1 x za týždeň.
e) Report o stave zberu udalostí (napr. počet monitorovaných zdrojov, priemerný počet zbieraných udalostí, úspešnosť parsovania udalostí a pod.) a posúdenie zmysluplnosti zbieraných údajov - minimálne 1 x za mesiac.
f) Analýza zistených nedostatkov a vypracovanie návrhu ďalšieho rozvoja MBIT.

p.č.	názov položky	<u>biele pole</u> - slovný popis spôsobu naplnenia požiadavky, resp. deklarácia splnenia prožiadavky textom "spĺňa" alebo "nespĺňa", <u>žlté pole</u> - odkaz na dokumentáciu (názov, číslo strany, kapitola atď.), ktorá je súčasťou ponuky, kde sa dá overiť splnenie požiadavky <vyplní uchádzač>
	Požiadavky na monitoring a prevádzku MBIT	
2.58	Monitorovanie dostupnosti, výkonu a funkčnosti MBIT komponentov	Spĺňa
2.59	Monitorovanie nepretržitého zberu udalostí z monitorovaných zariadení a ich následného spracovania a vyhodnotenia	Spĺňa
2.60	Monitorovanie zberu a vyhodnocovania sieťových tokov v LAN NBS a na perimetri NBS	Spĺňa
2.61	Správa MBIT komponentov (zaraďovanie, vyraďovanie a konfigurácia)	Spĺňa
2.62	Správa a konfigurácia MBIT infraštruktúry (používateľov, dashboardov, detekčných metód, korelačných a parsovacích pravidiel a pod.)	Spĺňa
2.63	Zaevidovanie vzniknutého prevádzkového incidentu do prevádzkového denníka MBIT, v prípade potreby súčinnosti správcov zaevidovať do Service Desku NBS	Spĺňa
2.64	Vyriešenie vzniknutého incidentu odhaleného pri monitorovaní MBIT do 24 hodín. V prípade, že incident nie je možné odstrániť do 24 hodín, navrhnúť riešenie. V prípade odsúhlasenia predloženého návrhu riešenia, zrealizovať riešenie do 3 pracovných dní. V prípade nemožnosti vyriešenia zisteného incidentu, zaevidovanie prevádzkového problému	Spĺňa
2.65	Prístup do technológií MBIT (SIEM a NDR) pre minimálne 5 zamestnancov NBS s možnosťou nastaviť vlastné dashboardy	Spĺňa
	Požiadavky na rozvoj a optimalizáciu MBIT	
2.66	Integrácia nových typov zdrojov logov do MBIT a úprava existujúcich zdrojov logov. Jedná sa najmä o analýzu logov a tvorbu nových resp. úpravu existujúcich parsovacích pravidiel na základe požiadaviek NBS. Súčasťou služby je aj návrh a realizácia spôsobu integrácie nového zdroja logov do MBIT a návrh a úprava spracovania logov existujúceho zdroja logov t.j. ide aj o návrh, tvorbu a úpravu politík spracovania logov.	Spĺňa
2.67	Tvorba a úprava investigácií a reportov	Spĺňa
2.68	Tvorba a úprava korelačných pravidiel a pravidiel generovania alarmov	Spĺňa
2.69	Tvorba a úprava detekčných metód	Spĺňa
2.70	Návrh nových use case-ov, t.j. vyjasnenie zadania use case-u (cieľ, zameranie, rozsah, popis, výstupy), analýzu riešenia a vypracovanie zadania use casu	Spĺňa
2.71	Vytvorenie nových use case-ov, t.j. zabezpečenie logovania a parsovania relevantných udalostí, vytvorenie korelačných pravidiel, reportov a notifikácií, vyladenie a otestovanie use casu	Spĺňa
2.72	Údržba existujúcich use case-ov (napr. po zmenách v IT infraštruktúre NBS), kontrola všetkých komponentov use case-ov vrátane správneho parsovania udalostí, aktuálnosti zoznamov a pod.	Spĺňa
2.73	Dokumentácia nových use case-ov a vykonaných zmien v existujúcich use case-och	Spĺňa
2.74	Evidencia vykonaných zmien.	Spĺňa
2.75	Vyhodnocovanie anomálií v nazbieraných dátach. Pod anomáliami v nazbieraných dátach sa rozumie napr. výrazne zvýšená/znížená početnosť udalostí určitého typu oproti bežnému výskytu, prípadne prestali chodiť alebo výskyt udalostí, ktoré sa bežne nevyskytujú a pod.	Spĺňa
2.76	Vyhodnocovanie stavu parsovania udalostí, t.j. posudzovanie správneho parsovania a normalizácie udalostí	Spĺňa
2.77	Posudzovanie zmysluplnosti zbieraných údajov a ich ďalšie spracovanie a archivácia	Spĺňa
2.78	Vypracovávanie odporúčaní a návrhov na zlepšenie kvality fungovania zberu a vyhodnocovania bezpečnostných udalostí. Súčasťou služby sú aj konzultácie k vypracovaným odporúčaniam a návrhom	Spĺňa
2.79	Nešpecifikované konfiguračné úpravy podľa požiadaviek NBS	Spĺňa
	Požiadavky na NDR technológiu. (NDR dodané zariadenia musia byť nakonfigurované tak, aby boli splnené nasledovné požiadavky):	
2.80	monitorovanie celej sieťovej komunikácie v LAN, DMZ na HTP a ZTP	Spĺňa
2.81	monitorovanie sieťovej komunikácie na perimetroch HTP a ZTP (detekciu správania používateľov, použitých aplikácií pri komunikácii smerom do internetu a pod.)	Spĺňa
2.82	všetky monitorované zariadenia z HTP logujú NetFlow informácie na jeden kolektor umiestnený na HTP	Spĺňa
2.83	všetky monitorované zariadenia zo ZTP logujú NetFlow informácie na jeden kolektor umiestnený na ZTP	Spĺňa
2.84	výpadok NetFlow kolektora v jednej lokalite nesmie znemožniť analýzu a spracovanie NetFlow dát (NetFlow analyzátor) kolektora v druhej lokalite	Spĺňa
2.85	konfigurácia NetFlow kolektorov, analýza a vyhodnocovanie NetFlow z kolektorov (NetFlow analyzátor) musí byť riadené z jedného centrálneho miesta (on-site alebo cloud) s prepojením (integráciou) na SIEM pre centrálne vyhodnocovanie bezpečnostných udalostí	Spĺňa
	NDR musí poskytovať nasledovnú funkcionalitu:	
2.86	NetFlow analyzátor musí umožniť spracovať v každej lokalite LAN minimálne 5000 flows/s	Spĺňa - https://d117h1jjiq768j.cloudfront.net/docs/default-source/flowmon-resources/2024-12-flowmon_collector_specification.pdf?sfvrsn=90711628_92
2.87	NDR infraštruktúra musí na každej lokalite umožniť uložiť udalosti po dobu min. 1 roka	Spĺňa - https://d117h1jjiq768j.cloudfront.net/docs/default-source/flowmon-resources/2024-12-flowmon_collector_specification.pdf?sfvrsn=90711628_92
2.88	zber, zobrazenie, analýzu a dlhodobé uloženie sieťových štatistík (NetFlow v5/v9, IPFIX, sFlow, príp. ďalšie kompatibilné s technológiou NetFlow)	Spĺňa - https://d117h1jjiq768j.cloudfront.net/docs/default-source/flowmon-resources/2024-12-flowmon_collector_specification.pdf?sfvrsn=90711628_92
2.89	ADS - Real-time detekciu anomálií dátovej prevádzky (DNS, DHCP, atď.), anomálií v správaní zariadení pripojených do siete, detekciu nových/neznámych zariadení, sieťových útokov (skenovanie portov, slovníkové útoky, DDoS), detekciu nežiadúcich aplikácií, vírusov, botnetov, atď.	Spĺňa - https://d117h1jjiq768j.cloudfront.net/docs/default-source/flowmon-resources/2024-12-flowmon_collector_specification.pdf?sfvrsn=90711628_92
2.90	IDS - monitorovanie sieťovej prevádzky alebo aktivít systémov na známe hrozby, škodlivé správanie, narušenie politík a pod.	Spĺňa - https://d117h1jjiq768j.cloudfront.net/docs/default-source/flowmon-resources/2024-12-flowmon_collector_specification.pdf?sfvrsn=90711628_92 https://d117h1jjiq768j.cloudfront.net/docs/default-source/flowmon-resources/2024-12- flowmon_probe_specificationd3f59d3395354fb78859a6757e4e9506.pdf?sfvrsn=b7d1fab4_102
2.91	automatický záchyt a analýzu packetov pre vybrané typy anomálií pre účely neskoršej detailnej analýzy	Spĺňa - https://d117h1jjiq768j.cloudfront.net/docs/default-source/flowmon-resources/2024-12-flowmon_collector_specification.pdf?sfvrsn=90711628_92
2.92	NetFlow analyzátor musí umožniť v každej lokalite vyhodnotiť dáta na perimetri s priepustnosťou dátovej linky 10 Gb/s.	Spĺňa - https://d117h1jjiq768j.cloudfront.net/docs/default-source/flowmon-resources/2024-12-flowmon_collector_specification.pdf?sfvrsn=90711628_92 https://d117h1jjiq768j.cloudfront.net/docs/default-source/flowmon-resources/2024-12- flowmon_probe_specificationd3f59d3395354fb78859a6757e4e9506.pdf?sfvrsn=b7d1fab4_102
2.93	customizáciu detekčných metód a vytváranie vlastných metód	Spĺňa - https://d117h1jjiq768j.cloudfront.net/docs/default-source/flowmon-resources/2024-12-flowmon_collector_specification.pdf?sfvrsn=90711628_92
2.94	vytváranie automatických a custom reportov	Spĺňa - https://d117h1jjiq768j.cloudfront.net/docs/default-source/flowmon-resources/2024-12-flowmon_collector_specification.pdf?sfvrsn=90711628_92
	Požiadavky na SIEM technológiu (Technológia SIEM musí minimálne umožniť):	
2.95	centrálne ukladanie logov v pôvodnom tvare (raw logov)	spĺňa, Exabeam-LogRhythm-SIEM-Help-7.19-RevB str. 1026 Data Indexer
2.96	spracovať minimálne 5000 (priemer za 24 hodín) záznamov za sekundu (EPS)	spĺňa, dokument Exabeam-LogRhythm-Standard-Installation-Upgrade-Guide-7.19-RevA.pdf str. 24 (max processing rate model LR-XM6600)
2.97	uchovávať raw logy ako aj spracované udalosti minimálne po dobu 90 dní	spĺňa, externí storage SAA86120 str. 20/23 dokument Gen6 Appliance Environmental Specs.pdf
2.98	zber dát z monitorovaných zdrojov pomocou agentov a/alebo bez agentov	spĺňa, LogRhythm-System-Monitor-Documentation-7.16.0-RevA.pdf str. 5
2.99	zber dát minimálne pomocou syslog, SNMP v2/v3, ODBC/OLE (logy v DB tabuľkách), XML, JSON	spĺňa, LogRhythm-System-Monitor-Documentation-7.16.0-RevA.pdf str. 112 System Monitor Functionality by Operating System Exabeam-Open-Collector-Installation-User-Guide-2025.04-RevA.pdf str. 5
2.100	spracovanie jedno a viacriadkových textových záznamov	spĺňa, Exabeam-LogRhythm-SIEM-Help-7.19-RevB.pdf str. 504
2.101	normalizáciu záznamov do jednotného formátu udalosti (parsing)	spĺňa, Exabeam-LogRhythm-SIEM-Help-7.19-RevB.pdf str. 1009 - Log Processing
2.102	parsovanie a spracovanie záznamov na základe preddefinovaných pravidiel od výrobcu, ktoré sú automaticky aktualizované	spĺňa, Exabeam-LogRhythm-SIEM-Help-7.19-RevB.pdf str. 443, 664, 868, 1065 - Knowledge Base, Knowledge Base Modules, MPE Policies, MPE Rules str. 1151 - Automatic Download
2.103	definovanie/pridávanie vlastných normalizačných pravidiel a log parserov	spĺňa, Exabeam-LogRhythm-SIEM-Help-7.19-RevB.pdf str. 868 a dál - Message Processing Engine Rule Builder, MPE Policies, Custom MPE rules can be edited celý LogRhythm-MPE-Rule-Builder-Parsing-Guide-7.x-RevA.pdf
2.104	automatické korelácie udalostí	spĺňa, Exabeam-LogRhythm-SIEM-Help-7.19-RevB.pdf str. 26 a dále - Advanced Intelligence Engine
2.105	generovanie alarmov, napr. po vyhodnotení korelácie, príp. výskyte špecifickej udalosti	spĺňa, Exabeam-LogRhythm-SIEM-Help-7.19-RevB.pdf str. 30 a dále - Advanced Intelligence Engine ... alarm properties ... Alarm Status
2.106	nastavenie rizikového skóre pre alarmy, monitorované systémy a pod.	spĺňa, Exabeam-LogRhythm-SIEM-Help-7.19-RevB.pdf str. 387 Risk-Based Priority (RBP) - The Message Processing Engine (MPE) uses Network and Host records to set the Risk-Based Priority (RBP) str. 406 a dále - Host Risk Level (required), Network Risk Level str. 641 a dále - Global Risk Based Priority, AIE RBP Calculation, Source Threat Level (STL) Calculation (AIE or MPE), MPE RBP Calculation str. 653 a dále - Risk Based Priority Calculator
2.107	automatický výpočet výsledného rizikového skóre	spĺňa, Exabeam-LogRhythm-SIEM-Help-7.19-RevB.pdf str. 642 - AIE RBP Calculation
2.108	vytvárať z monitorovaných systémov logické skupiny	spĺňa, Exabeam-LogRhythm-SIEM-Help-7.19-RevB.pdf str. 24, 387 - Entities str. 847 - Lists in the Client Console, List type = (Hosts, IP Address, Log Source)
2.109	využívanie ML/AI pri spracovaní udalostí	spĺňa, Exabeam-LogRhythm-SIEM-Help-7.19-RevB.pdf str. 31 - Součástí modelování AI jsou bloky pravidel typu Statistical, resp. Trend, které jsou typu Machine Learning. Dynamicky se upravuje statistický model normálního chování na základě historických dat a porovnává se s aktuálním stavem, resp. rozpoznává se změna v časových řadách nebo detekce odchylek od dlouhodobého vzorce
2.110	out-of-the-box konektory do systémov, databáz a pod.	spĺňa, celý dokument LogRhythm-Device-Configuration-Guides-7.12.0-API-Log-Sources-RevA.pdf podporovná je veká řada konektorů do dalších systémů
2.111	out-of-the-box vyhodnocovacie pravidlá, metódy, playbook-y a pod.	spĺňa, Exabeam-LogRhythm-SIEM-Help-7.19-RevB.pdf str. 443, 664, 868, 1065 - Knowledge Base, Knowledge Base Modules, MPE Policies, MPE Rules
2.112	integráciu udalostí z bezpečnostných systémov: Trellix (ePO, EDR, EDS, ATD, Webwasher), F5 DDoS, GenieATM DDoS, Barracuda WAF, ESET Mail Security	spĺňa, seznam v dokumentu Logrhythm-Supported-DS.docx GenieATM DDOs - tam se provede custom integrace Exabeam-LogRhythm-SIEM-Help-7.19-RevB.pdf str. 868 a dál - Message Processing Engine Rule Builder, MPE Policies, Custom MPE rules can be edited
2.113	investigáciu a vyhľadávanie anomálií v udalostiach	spĺňa, Exabeam-LogRhythm-Web-Console-User-Guide-7.19-RevA.pdf str. 25 Drill into Log Data Associated with an Alarm str. 179 Search
2.114	automatické vytváranie tiketov do Service Desku NBS	spĺňa, Exabeam-LogRhythm-SIEM-Help-7.19-RevB.pdf str. 696 SmartResponse - intergace se systémy třetích stran
2.115	dlhodobú archiváciu záznamov a spracovaných udalostí - min. 1 rok	spĺňa, Exabeam-LogRhythm-SIEM-Help-7.19-RevB.pdf str. 95 Data Archives and Restoration
2.116	analytické nástroje napr. reportovanie, forenznú analýzu, nástroje na určovanie trendov, analýzu zmien, štatistickú analýzu, štatistické reporty nad aktuálnymi aj historickými dátami	spĺňa, Exabeam-LogRhythm-SIEM-Web-Console-User-Guide-7.20-RevA.pdf Součástí je analytický nástroj Web Console s těmito funkcemi mimo jiné: Reportování a Vizualizace - dashboardy str. 243 Určování trendů pomocí TopX widgetů - widgets str. 279 a také pomocí podpůrných funkcí Custom Time Range str. 301 Forensní analýza pomocí - Analyze Page str. 25 a také pomocí funkce Searches pomocí kritérií str. 146 a například také pomocí Perform Pivot Searches str. 166
2.117	personalizovaný dashboard	spĺňa, Exabeam-LogRhythm-SIEM-Web-Console-User-Guide-7.20-RevA.pdf Součástí je analytický nástroj Web Console s funkcí vytváření dashboardů str. 246. V nich se dají používate různé visualizační nástroje Widgets str. 277. Tyto dashboardy mají svého vlastníka a ten je může používat sám nebo je i sdílet
2.118	out-of-the-box reporty a vytvárať vlastné reporty	spĺňa, Exabeam-LogRhythm-SIEM-Help-7.19-RevB.pdf Out-of-the-box reporty obsahují moduly z - Knowledge Base str. 430. str. 443 - Knowledge Base Modules are prepackaged, customizable content applicable to a specific regulation or need, such as reports, investigations, alerts, AI Engine rules, or other applicable product areas Vlastní reporty lze realizovat pomocí záložky Report Center v clientské konzoli, např. str. 988 Create Reports
2.119	automatické spúšťanie definovaných reportov (mesačne, týždenne, denne, alebo v definovanom čase) a ich zasielanie e-mailom priamo zo systému	spĺňa, Exabeam-LogRhythm-SIEM-Help-7.19-RevB.pdf Scheduled Report Job Manager - str. 625, 1075, A Report tool used to schedule report packages to run for a specified period on a specified date and time. The job can be set to email an existing person and/or export to a UNC path
	Dodané riešenie SIEM musí umožniť monitorovať a zbierať udalosti z minimálne nasledovných IT technológií (spolu cca 4700 zdrojov IT infraštruktúry):	
2.120	Servery (470 ks): Microsoft Windows (300), Oracle Linux a Red Hat Linux (170) z toho je 450 VM a 20 fyzických serverov	spĺňa, podpora těchto datových zdrojů je uvedena v seznamu datových zdrojů v dokument Logrhythm-Supported-DS.docx Řešení není licenčně omezené na počet zdrojů.
2.121	Sieťové prvky (FW, switch, router) 450 ks : Fortigate , HP, Cisco, Forcepoint	spĺňa, podpora těchto datových zdrojů je uvedena v seznamu datových zdrojů v dokument Logrhythm-Supported-DS.docx Řešení není licenčně omezené na počet zdrojů.
2.122	Databázové platformy: MS SQL, Oracle, MySQL	spĺňa, MS SQL a Oracle jsou v listu nativně podporovaných datových zdrojů - dokument Logrhythm-Supported-DS.docx MySQL podpora bude realizována pomocí custom wrapperu. Řešení není licenčně omezené na počet zdrojů.
2.123	Virtualizačné platformy: VMware, OpenShift	spĺňa, podpora datových zdrojů je uvedena v seznamu datových zdrojů v dokument Logrhythm-Supported-DS.docx OpenShift není explicitně uveden, ale jeho podpora je zajištěna integrací pomocí protokolu syslog se sdružením záznamů, které půjdou na SIEM z jedné IP. Řešení není licenčně omezené na počet zdrojů.
2.124	Hlasové služby: Mitel	provede se custom integrace Exabeam-LogRhythm-SIEM-Help-7.19-RevB.pdf str. 868 a dál - Message Processing Engine Rule Builder, MPE Policies, Custom MPE rules can be edited
2.125	MDM: Ivanti	provede se custom integrace Exabeam-LogRhythm-SIEM-Help-7.19-RevB.pdf str. 868 a dál - Message Processing Engine Rule Builder, MPE Policies, Custom MPE rules can be edited
2.126	Cloud: Microsoft 365, Entra ID, SharePoint online, Teams online	spĺňa, využije se integrace přes Beats jednou z možností - Integrace Microsoft 365 bude realizovaná pomocí API - dokument seznamu podporovaných DS Logrhythm-Supported-DS.docx API - Office 365 Management Activity API - Office 365 Message Tracking Integrace Microsoft EntraID pomocí jedné z variant využití Open Collectoru: * Exabeam-MSGraph-API-Beat-6.0.9-RevA.pdf Pomocí registrace aplikace v EntraID * LogRhythm-Azure-Event-Hubs-Beat-6.0.10-RevA.pdf Využije se export dat z Azure Monitor do Azure Event Hubs Microsoft Teams samotný neposkytuje přímo nativní API pro export dat, ale data související s Teams jsou dostupná prostřednictvím Microsoft 365 a Entra ID (dříve Azure AD)
2.127	VPN: Fortinet	spĺňa, podpora těchto datových zdrojů je uvedena v seznamu datových zdrojů v dokument Logrhythm-Supported-DS.docx Řešení není licenčně omezené na počet zdrojů.
2.128	LDAP: Microsoft AD	spĺňa, Exabeam-LogRhythm-SIEM-Help-7.19-RevB.pdf str.677 - Active Directory Domain Manager, Active Directory Synchronization, vyčítaní přes LDAP Active Directory Kontroléry standarně dále monitorujeme sběrem Security, System, Application event logu. Viz. podporované datové zdroje dokument Logrhythm-Supported-DS.docx MS Windows Event Logging XML
2.129	Elektronická pošta: MS Exchange on premise (správa mailových objektov a smerovanie mailov) a MS Exchange online (mailové schránky)	spĺňa, Podporované datové zdroje dokument Logrhythm-Supported-DS.docx jsou typu Flat File - MS Exchange Message Tracking Log, MS Windows Event Logging - MSExchange Management, MS Windows Event Logging - Exchange Mailbox DB Failures Exchange Online aktivita je součástí auditovaných protokolů Microsoft 365 viz. podpora Office 365 Message Tracking API - Logrhythm-Supported-DS.docx
	SIEM zariadenia dodávané on-site musia byť nakonfigurované tak, aby boli splnené nasledovné požiadavky:	
2.130	monitorované zariadenia a aplikácie logujú na logserver umiestnený v ich lokalite, t.j. HTP alebo ZTP. Logserver môže byť tvorený aj viacerými zariadeniami, pričom výpadok jedného zo zariadení zabezpečujúceho funkcionalitu logservera v danej lokalite nesmie znemožniť funkcionalitu samotného logservera	Spĺňa
2.131	v prípade úplného výpadku logservera v jednej lokalite, musí logserver v druhej lokalite prevziať funkcionalitu vypadnutého logservera a to tak, aby nebola potrebná rekonfigurácia agentov/zariadení zasielajúcich dáta do systému SIEM.	Spĺňa

Ciele služby Skenovanie zraniteľnosti:

Cieľom služby je zabezpečiť výkon činností procesu riadenia zraniteľností v IT infraštruktúre spravovanej NBS.

Časový harmonogram poskytovania služby Skenovanie zraniteľností:

Počas pracovných dní v čase od 8.00h do 16.30h (režim 8/5).

Monitorovanie a vyhodnocovanie poskytovaných služieb Skenovanie zraniteľností:

Služba sa považuje za riadne poskytnutú, ak sú splnené všetky nasledovné minimálne podmienky:

a) Prístup do portálu služby – nepretržite, s nedostupnosťou max. 3 x mesačne v celkovej úhrnnej dobe najviac 3 hodiny mesačne.

b) Skenovanie: Discovery sken – min. 1 x mesačne, pravidelné skenovanie IT infraštruktúry NBS – min. 1 x týždenne.

c) Kontroly konfigurácie – min. 1 x mesačne.

d) Poskytnutá súčinnosť pri riešení prevádzkových problémov týkajúcich sa skenovaní a kontrol konfigurácie až do vyriešenia.

e) Údržba komponentov systému, vrátane ich aktualizácie a prípadných úprav konfigurácie – min. 1 x mesačne.

p.č.	názov položky	**biele pole** - slovný popis spôsobu napĺnenia požiadavky, resp. deklarácia splnenia prožiadavky textom "spĺňa" alebo "nespĺňa", **žlté pole** - odkaz na dokumentáciu (názov, číslo strany, kapitola atď.), ktorá je súčastou ponuky, kde sa dá overiť splnenie požiadavky <vyplní uchádzač>
	Požiadavky na službu Skenovanie zraniteľností	
2.132	Cieľové aktíva (skenované systémy): všetky servery, sieťové zariadenia, appliances, pripojené do LAN NBS, vrátane virtualizačných platforiem, databázových platforiem, virtuálnych serverov a kontajnerov prevádzkovaných na virtualizačných platformách ako aj serverov a zariadení spravovaných NBS v cloude. Predmetom služby nie sú koncové zariadenia používateľov (NTB, PC, mobilné zariadenia a pod.).	Spĺňuje QualysCloud Agent - https://success.qualys.com/customersupport/s/cloud-agent-pam Qualys Virtuální Appliance - https://docs.qualys.com/en/scanner/supported-platform/get_started/supported_virtualization_platforms.htm Qualys autentizace - podpora autentizačních skenů na OS/HW - https://success.qualys.com/support/s/article/000006761
2.133	Discovery sken infraštruktúry a identifikácia cieľových aktív, ktoré nie sú zahrnuté do pravidelného skenovania zraniteľností (min. 1x mesačne).	Spĺňuje Počet Discovery/Map skenů není omezeno. Pro jednotlivé sítě se definují virtuální skenovací appliance (licence umožňuje deployment až 999 skenovacích appliancí) Počet cílových aktiv není limitován licencí. Dokumentace k Discovery/MAP skenům - https://docs.qualys.com/en/vm/latest/maps/mapping_basics.htm
2.134	Zaradovanie a vyradovanie cieľových aktív do pravidelných skenov zraniteľností na základe požiadaviek NBS a výsledkov discovery skenu. Riešenie problémov pri zaradovaní so správcami cieľových aktív.	Spĺňuje
2.135	Pravidelné skenovanie. Naplánovanie, konfigurácia a realizácia pravidelných skenov známych zraniteľností pre cieľové aktíva (každé cieľové aktívum musí byť skenované min. 1x týždenne).	Spĺňuje Doporučení na Servery využít agenty - u agentů lze definovat jejich aktivní okno a dochází ke sběru dat kontinuálně vychází z dokumentace QualysCloud Agenta - https://docs.qualys.com/en/ca/getting-started-guide/get_started/get_started.htm Síťové prvky a nepodporované zařízení pro deployment agenta využít autentizované skeny pomocí virtuálních appliancí a autentizovaných skenů. Qualys Virtuální Appliance - https://docs.qualys.com/en/scanner/supported-platform/get_started/supported_virtualization_platforms.htm Qualys autentizace - podpora autentizačních skenů na OS/HW - https://success.qualys.com/support/s/article/000006761 Licenčně není omezen počet skenů zranitelností pomocí Virtuálních skenovacích appliancí
2.136	Zohľadnenie prevádzkových obmedzení – cieľové aktíva sú skenované v časoch určených NBS.	Spĺňuje není problém definovat na QAgentovi tzv. blackwindow to slouží k tomu kdy konkrétní agent spí a nekolektuje data, U virtuálních skenovacích appliancí se definuje čas startu a lze různě rozřazovat jednotlivé části sítě na konkrétní časové bloky. · QualysAgent blackwindow - https://docs.qualys.com/en/ca/portal/latest/profiles/manage_profiles.htm · Qualys Virtuální skenovací appliance scheduler - https://docs.qualys.com/en/vm/latest/schedules/schedules_basics.htm
2.137	Možnosť definovať a realizovať skenovanie vybraných cieľových aktív alebo ich skupín, podľa potreby NBS, či už na preverenie odstránenia zraniteľností alebo špecializované skenovania vybraných zraniteľností.	Spĺňuje jak je již zmíněno je možnost definovat jednorázové skeny, přeskenování konkrétních částí sítě, aktiv aj.
2.138	Hodnotenie a stanovanie priorít. Automatické hodnotenie závažnosti identifikovaných zraniteľností. Stanovenie priorít riešenia zraniteľností umožňuje zohľadniť okrem CVSS skóre aj existenciu exploitu, zneužívanie zraniteľnosti v praxi, výskyt v CISA katalógu známych zneužívaných zraniteľností a pod.	Spĺňuje Qualys využívá nejen úroveň jednotlivých zranitelností a tím určuje i QDS (Qualys Detection Score), je možnost úroveň kritičnosti ovlivnit at už štítkama a nebo prioritizaci aktiva. Dále Qualys využívá Prioritizační modul pro definici jaké zranitelnosti opraví nejkritičtější části systémů a lze to ovlivnit různými RTI (Real-Time threat indicators) - https://success.qualys.com/support/s/article/000006852 ty udávají existenci veřejného exploitu aj. K využití CISA je popis v článku - https://blog.qualys.com/product-tech/2022/02/22/managing-cisa-known-exploited-vulnerabilities-with-qualys-vmdr
2.139	Pre každú identifikovanú zraniteľnosť je v systéme k dispozícii informácia o odporúčanej nápravnej akcii alebo opatrení.	Spĺňuje Qualys zobrazuje tzv. Solution pro jednotlivé zranitelnosti viz. článek https://docs.qualys.com/en/pm/latest/patches/viewing_patch_details.htm
2.140	Možnosť akceptovať identifikovanú zraniteľnosť pre vybrané skupiny cieľových aktív do definovaného dátumu, resp. neobmedzene. Možnosť upraviť hodnotenie závažnosti identifikovanej zraniteľnosti pre vybrané skupiny cieľových aktív.	Spĺňuje lze vytvořit vyjímku pro konkrétní zranitelnost dle dokumentace - https://docs.qualys.com/en/cs/latest/exceptions/define_vulnerability_exceptions.htm
2.141	Kontrola konfigurácie cieľových aktív . Naplánovanie, konfigurácia a realizácia pravidelných previerok konfigurácie cieľových systémov (každé cieľové aktívum je kontrolované min. 1x mesačne). V tomto prípade sú navyše ako cieľové aktíva brané aj samostatné inštancie databáz. (Kontrola benchmarkov môže byť súčasťou aj technológie inej poskytovanej služby, nemusí byť nevyhnutne technicky zviazaná s technológiou skenovania zraniteľností. Optimálne kritérium je, aby na koncových zariadeniach bolo nainštalovaných minimum príslušných agentov.)	Spĺňuje Qualys je schopen řešit kontrolu konfiguračních standardů dle CIS a to s modulem SCA a nebo pokud je potřeba více typů standardů tak s plnohodnotným Policy Compliance. Kontrola se provádí buď pomocí již nainstalovaného QAgenta a nebo pomocí skenu virtuální skenovací appliancí. Stejnou které se využívá na skenování zranitelností nebo na discovery/map skeny. SCA - https://www.qualys.com/apps/secunty-configuration-assessment/ PC - https://www.qualys.com/apps/policy-compliance/
2.142	Príprava kontrolných šablón pre jednotlivé typy cieľových aktív formou prispôsobenia štandardných benchmarkov (CIS, definovaných výrobcami, resp. definovaných internými politikami NBS) podľa požiadaviek NBS. Údržba a aktualizácia kontrolných šablón.	Spĺňuje Připravené CIS benchmarky je možné upravit dle preferencí NBS
2.143	Riešenie problémov. Riešenie prevádzkových problémov pri skenovaní a kontrole konfigurácie so správcami cieľových aktív (nemožnosť vykonať sken/kontrolu, neúplné výsledky, neúmerná záťaž cieľového aktíva, neúmerná dĺžka skenovania/kontroly, diagnostika). Riešenie problémov s výsledkami skenovania a kontroly konfigurácie: false-positive nálezov (teda nesprávne detegované zraniteľnosti, resp. odchýlky od definovaného benchmaku) a false-negatives nálezov (chýbajúce detekcie).	Spĺňuje QAgent zanechává log soubor na každé stanici který se využívá k případnému troubleshootingu U virtuálních appliancí lze zapnout se supportem debug mod a řešit jednotlivé problémy a nebo lze spousta věcí zkontrolovat přímo z tenantu
2.144	Údržba, konfigurácia, aktualizácia a kontrola komponentov riešenia pre skenovanie zraniteľností (bez ohľadu na ich umiestnenie on-prem alebo off-prem).	Spĺňuje
2.145	Reporting. Príprava, definícia a naplánovanie automaticky generovaných reportov o zraniteľnostiach jednotlivých tried cieľových aktív •Reporty určené pre správcov jednotlivých tried cieľových aktív (podľa technológií). •Reporty určené pre koordinátorov IT služieb a pre analýzy rizík IT služieb (podľa IT služieb). •Ad-hoc reporty podľa špecifických potrieb.	Spĺňuje je možné definovat jednotlivé reporty dle konkrétních typů aktiv. Dále je možné připravit realtime pohledy, které je možné zaslat cílovým administrátorům pro kontrolu a pro jednoduchou identifikaci stavu. Takto vytvořené pohledy lze upravovat/připravovat dle preferencí. Velká výhoda je již vyobrazení požadovaných informací bez potřeby analyzovat data z reportů. Reporting - https://docs.qualys.com/en/vm/latest/#t=module_pc%2Fsetup%2Fpc_reports_setup.htm&hsearch=reporting&rhhlterm=reports%20reporting%20report Dashboardy - https://docs.qualys.com/en/ud/latest/get_started/getting_started_with_unified_dashboard.htm
2.146	Možnosť automatizovane zadávať tickety do Service Desk systému NBS.	Možnost integrace s Jira, CA ServiceDesk aj. Jira - https://docs.qualys.com/en/integration/jira_connector/#t=get_started%2Fget_started.htm CA Service Desk - https://success.qualys.com/discussions/s/question/0D52L00004TnuNESAZ/qualys-vm-and-ca-service-desk-integration-anyone-interested
	Požiadavky na technológiu Skenovanie zraniteľností	
2.147	Prístup do portálu služby pre minimálne 10 zamestnancov NBS s možnosťou nastaviť vlastné dashboardy a filtre.	Spĺňuje je možnost i definovat rozsah aktiv které jednotlivý administrátoři vidí. Není omezen počet administrátorů. https://docs.qualys.com/en/vm/latest/tbus/tag_based_user_scoping.htm
2.148	Riadenie rolí a oprávnení min. v rozsahu, ktorý umožní oddeliť používateľov s read-only prístupom a prístupom umožňujúcich definovať a plánovať skenovanie, obmedziť prístup na vybrané skupiny cieľových aktív.	Spĺňuje Scope se define dle přidělených štítků https://docs.qualys.com/en/vm/latest/tbus/tag_based_user_scoping.htm Definování rolí je možné dle typu - https://docs.qualys.com/en/vm/latest/user_accounts/user_roles_comparison_vm.htm
2.149	Architektúra riešenia umožní skenovať oddelene tzv. Secure zónu s požiadavkou, že credentials pre prístup k systémom v zóne nemôžu byť uložené mimo tejto zóny a agenti sú spravovaní oddelene od ostatných agentov.	Spĺňuje QAgenti mohou být spravování pomocí konkrétního klíče a mohouo mít definovaný rozdílná politiky pro oddělené prostředí Dále je možnost offline virtuální skenovací appliance pro autentizované skeny https://cdn2.qualys.com/docs/qualys-offline-scanner-user-guide.pdf
2.150	Skenovanie aj kontroly konfigurácie sú možné voliteľne prostredníctvom agentov, resp. prostredníctvom prihlasovania účtom.	Spĺňuje Data dokáže kolektovat jak QAgent tak virtuální skenovací appliance pomocí SCA/PC skenů https://cdn2.qualys.com/docs/qualys-policy-compliance-guide.pdf
2.151	Predpripravené šablóny konfigurácií CIS, DISA a pod., ktoré je možné upravovať (rozsah, očakávané parametre a atribúty).	Spĺňuje Qualys obsahuje šablony konfigurací CIS. Lze sledovat updaty jednotlivých standardů na https://notifications.qualys.com/category/policy-library
2.152	Bezpečné uloženie hesiel, súkromných kľúčov, API kľúčov a iných citlivých údajov použitých na autentizáciu na cieľové systémy. Citlivé parametre zadáva NBS, poskytovateľ služby ich vie použiť výlučne referenciou na definovanie skenov a kontrol konfigurácie.	Spĺňuje Qualys využívá vlastní datová centra a v tenantu zákazník vyplňuje potřebné autentizační profily. Heslo lze pouze zadat následně ho nelze přečíst, vyexportovat aj. Lze využít i napojení na PAM. https://success.qualys.com/discussions/s/question/0D52L00004TnuRSSAZ/storage-of-authentication-scan-password
2.153	Podpora pre integráciu s Password Vault riešeniami – napr. HashiCorp Vault a pod.	Spĺňuje Virtuální appliance si vždy vyžádá při skenu konkrétní heslo k cílovému aktivu. Integrace s HashiCorp - https://docs.qualys.com/en/vm/latest/authentication/vaults/win_hashicorp_vault.htm
2.154	Bezpečný komunikačný kanál medzi komponentami riešenia (obojstranne autentizovaný, so zabezpečenou dôvernosťou prenášaných údajov).	Spĺňuje https://docs.qualys.com/en/scanner/faq/scanner_appliance_security/index.htm
2.155	Možnosť filtrovať identifikované nálezy (zraniteľnosti, odchýlky od stanovenej konfigurácie) podľa závažnosti, času prvej detekcie, času ostatnej detekcie, triedy cieľových aktív, triedy zraniteľnosti, atď.	Spĺňuje Qualys většinu informací indexuje pro jednodušší vyhledávání ať už se jedná o čas/datum nálezu, typ zranitelnosti, třídy konkrétních aktiv, třídy zranitelnosti aj.
2.156	Možnosť exportovať filtrované údaje do čitateľného formátu (pdf), aj do strojovo spracovateľného formátu (csv).	Spĺňuje Reporty, exporty z výpisu zranitelností, seznamu serverů aj. lze exportovat nejen do CSV, PDF, XML a HTML https://docs.qualys.com/en/certview/latest/search/export.htm
2.157	Zdokumentované API pre pripojenie iných systémov a aplikácií	Spĺňuje Dokumentace API https://docs.qualys.com/en/vm/api/index.htm
2.158	Portál riešenia poskytuje dashboard pre používateľov, umožňujúci personalizáciu jednotlivých prvkov dashboardu, následné drill-down pohľady a možnosť analýzy identifikovaných zraniteľností. Dashboard umožňuje využiť predpripravené ako aj definovať vlastné štatistické pohľady na stav zraniteľností v prostredí NBS.	Spĺňuje Qualys má seznam předpřipravených pohledů (Dashboardů), ty lze upravovat/vytvářet vlastní. Každá dlaždici je možnost prokliknout a dostat se ne výstup konkrétního filtru. Dále je možnost přímo z filtru pod VMDR vytvářet dlaždici a tu přidat do pohledu. https://docs.qualys.com/en/ud/latest/get_started/getting_started_with_unified_dashboard.htm
2.159	Databáza zraniteľností aktualizovaná minimálne 1 x denne. Databáza musí pokrývať zraniteľnosti štandardných softvérových komponentov používaných v NBS (min. v rozsahu operačné systémy serverov, virtualizačné platformy, databázové systémy, webové a aplikačné servery, sieťové komponenty).	Spĺňuje vychází z FAQ https://www.qualys.com/support/faq/general/
2.160	Výrobca aktualizuje databázu zraniteľností tak, aby bolo možné skenovať závažné zraniteľnosti publikované výrobcami v ich bezpečnostných odporúčaniach, ako sú napr. RHSA, VMSA, ELSA, špecifických KB (Microsoft), alebo zverejnené v CISA katalógu, zvyčajne do 24 hodín po ich publikovaní.	Spĺňuje vychází z FAQ https://www.qualys.com/support/faq/general/
2.161	Integrácia s ostatnými bezpečnostnými nástrojmi (minimálne SIEM).	Spĺňuje https://blog.qualys.com/misc/2012/04/23/logrhythm-partners-with-qualys

Ciele služby Sledovanie IT hrozieb a zraniteľnosti:
Cieľom služby je sledovanie aktuálnych zraniteľností publikovaných na overených externých zdrojoch s cieľom identifikovať potenciálne bezpečnostné hrozby pre IT NBS.

Časový harmonogram poskytovania služby Sledovanie IT hrozieb a zraniteľnosti:
Počas pracovných dní v čase od 8.00h do 16.30h (režim 8/5).

Monitorovanie a vyhodnocovanie poskytovaných služieb Sledovanie IT hrozieb a zraniteľnosti:
Služba sa považuje za riadne poskytnutú, ak sú splnené všetky nasledovné minimálne podmienky:
a)Vyhodnotenie aktuálnych zraniteľností a ich relevantnosti - 1 x za deň.

p.č.	názov položky	biele pole - slovný popis spôsobu naplnenia požiadavky, resp. deklarácia splnenia prožiadavky textom "spĺňa" alebo "nespĺňa", žlté pole - odkaz na dokumentáciu (názov, číslo strany, kapitola atď.), ktorá je súčasťou ponuky, kde sa dá overiť splnenie požiadavky <vyplní uchádzač>
	Požiadavky na službu Sledovanie IT hrozieb a zraniteľnosti	
2.162	Denné vyhodnocovanie aktuálnych IT hrozieb a zraniteľností z overených externých zdrojov.	spĺňa
2.163	Vyhodnotenie relevantnosti IT hrozieb a zraniteľností s identifikáciou IT NBS ktorých sa týka zraniteľnosť.	spĺňa
2.164	Ohodnotenie závažnosti, resp. rizikovosti relevantných IT hrozieb a zraniteľností.	spĺňa
2.165	Popis jednotlivých relevantných IT hrozieb a zraniteľností s odporúčaniami ako sa brániť, resp. aké opatrenia, postupy a zmeny konfigurácií je potrebné vykonať na ochranu proti hrozbám, resp. pre odstránenie zraniteľnosti.	spĺňa
2.166	Upozornenie správcov dotknutých IT s návrhom vykonania odporúčaných nápravných opatrení.	spĺňa
	Požiadavky na technológiu Sledovanie IT hrozieb a zraniteľností	
2.167	Prístup do portálu služby pre minimálne 3 zamestnancov NBS s možnosťou nastaviť filter pre zobrazované zraniteľnosti podľa technológií využitých v IT NBS.	spĺňa

Ciele služby BAS:
Cieľom služby je zabezpečiť pravidelnú, systematickú a konzistentnú kontrolu stavu bezpečnosti IT infraštruktúry formou simulácie prienikov a útokov na IT infraštruktúru NBS metodikou MITRE ATT&CK (nie skutočný malvér na skutočnú infraštruktúru). Odhaliť slabé miesta ochrany bezpečnosti IT, resp. uskutočniteľnosť potenciálneho útoku. Účinnosť jestvujúcich ochranných prvkov, resp. námety na zlepšenie ich konfigurácie. Efektívnosť detekčných nástrojov, t.j. relevantnosť logovaných informácií do SIEMu. Spôsob vyhodnotenia v SIEMe. Reakcia SOC tímu a odozva na incident. Opakovaná automatická kontrola účinnosti jestvujúcich ochranných prvkov, najmä po zmenách v IT infraštruktúre a po zmenách nastaveniach ochranných prvkov.

Časový harmonogram poskytovania služby BAS:
Počas pracovných dní v čase od 8.00h do 16.30h (režim 8/5).

Monitorovanie a vyhodnocovanie poskytovaných služieb BAS:
Služba sa považuje za riadne poskytnutú, ak sú splnené všetky nasledovné minimálne podmienky:
a) Pravidelné automatické testovanie bezpečnosti IT infraštruktúry - minimálne 1 x mesiac.
b) Poskytnutá súčinnosť pri riešení prevádzkových problémov až do vyriešenia.

p.č.	názov položky	**biele pole** - slovný popis spôsobu naplnenia požiadavky, resp. deklarácia splnenia prožiadavky textom "spĺňa" alebo "nespĺňa", **žlté pole** - odkaz na dokumentáciu (názov, číslo strany, kapitola atd.), ktorá je súčasťou ponuky, kde sa dá overiť splnenie požiadavky <vyplní uchádzač>
	Požiadavky na službu BAS	Spĺňa
2.168	Pravidelné automatické testovanie bezpečnosti IT infraštruktúry formou simulácie techník prienikov a útokov s automatickým vyhodnotením vykonaných testov - minimálne 1 x mesačne.	Spĺňa
2.169	Automatické vyhodnotenie (report) identifikovaných zraniteľností s popis závažnosti, resp. rizikovosti prípadne aj s odporúčaním nápravných opatrení.	Spĺňa
2.170	Poskytovanie súčinnosti pri riešení prevádzkových problémov spojených s nasadením a prevádzkou BAS.	Spĺňa
2.171	Prístup do portálu služby pre minimálne 3 zamestnancov NBS s možnostou nastaviť vlastné dashboardy a filtre.	Spĺňa
	Požiadavky na technológiu BAS, BAS musí minimálne umožniť:	Spĺňa
2.172	bezpečné a kontrolované prostredie na testovanie kybernetickej bezpečnosti	Spĺňa - "_BAS_Validato_dokumentace_požadavky.docx", str. 1 High level architektura
2.173	kontrolu bezpečnosti za pomoci agentov a/alebo bez agentov z toho minimálne 50 zariadení za pomoci nainštalovaného agenta s možnosfou zmeny lokácie agentov na iné zariadenia	Spĺňa - "_BAS_Validato_dokumentace_požadavky.docx", str. 1 - obrázek 1. Jak Validato funguje? sekce 1
2.174	simulácie širokej škály scenárov útokov, ktoré pokrývajú rôzne taktiky, techniky a postupy používané útočníkmi podľa MITER ATT&CK framework napr. simuláciu e-mailovej infiltrácie odosielaním škodlivých e-mailov, simuláciu správania rôznych malvérových a ransomvérových infekcií, simuláciu získavania autentifikačných údajov a obídenie typických bezpečnostných kontrol, simuláciu zneužívania známych zraniteľností, simuláciu viacstupňových útokov, simuláciu útoku laterálneho pohybu v rámci LAN, simuláciu techník exfiltrácie dát napr. použitie skrytých kanálov a techník obfuskácie sieťovej komunikácie a pod.	Spĺňa - "_BAS_Validato_dokumentace_požadavky.docx", str. 4 - kapitola 2 Scénáře
2.175	monitorovať o.i. aj bezpečnostné systémy NGFW, IDS, IPS, EDR , Anti-virus and Anti-malware SW, DLP, SIEM, Email GW a pod.	Spĺňa - "_BAS_Validato_dokumentace_požadavky.docx", str. 5 kapitola 4 SIEM integrace
2.176	prispôsobiť scenáre testovania napr. proti hrozbám zameraným na systémy SWIFT	Spĺňa - "_BAS_Validato_dokumentace_požadavky.docx", Obrázek 6 SWIFT scénáře + modifikace Obrázek 7 Kopie existujícího scénáře
2.177	zbierať údaje o priebehu simulácie útokov a poskytovať prehľad o možných rizikách a nedostatkoch v bezpečnostných nastaveniach zariadení	Spĺňa - "_BAS_Validato_dokumentace_požadavky.docx", Obrázek 5 Simulace scénářů
2.178	po skončení simulácie vygenerovať komplexnú správu o bezpečnostnej situácii s podrobnými informáciami o zisteniach vrátane zistených zraniteľností, nesprávnych konfiguráciách a pod.	Spĺňa - "_BAS_Validato_dokumentace_požadavky.docx", Obrázek 8 Výstupy ze skenů
2.179	na základe výsledkov poskytnúť praktické návrhy na zmiernenie/odstránenie zistených nedostatkov	Spĺňa - "_BAS_Validato_dokumentace_požadavky.docx", Obrázek 8 Výstupy ze skenů
2.180	posúdiť bezpečnostnú ochranu proti špecifickým hrozbám z reálneho sveta	Spĺňa - "_BAS_Validato_dokumentace_požadavky.docx", str. 2
2.181	nedeštruktívnu simuláciu útokov, t.j. aby simulácia útoku nevytvorila bezpečnostnú dieru	Spĺňa - "_BAS_Validato_dokumentace_požadavky.docx", str. 2
2.182	plánovať simulácie v režime 24/7	Spĺňa - spouští v definovaný čas partner
2.183	integráciu s existujúcimi bezpečnostnými nástrojmi ako sú systémy SIEM, EDR a skener zraniteľnosti	Spĺňa - "_BAS_Validato_dokumentace_požadavky.docx",Kapitola 4. SIEM Integrace

Ciele služby Forenzná analýza:
Cieľom služby je vyšetrenie bezpečnostných incidentov tak, aby získané fakty a dôkazy boli použiteľné v právnych sporoch, poskytla pred súdom nespochybniteľné znalecké posudky alebo materiál na ďalšie vyšetrovanie počítačovej kriminality. Cieľom služby nie je analýza softvérového kódu. Služba je na objednávku.

Časový harmonogram poskytovania služby Forenzná analýza:
Aktivity spojené s forenznou analýzou môže externý SOC tím vykonávať bez časového obmedzenia, t.j. v ľubovoľný deň a hodinu.

Monitorovanie a vyhodnocovanie poskytovaných služieb Forenzná analýza:
Služba sa považuje za riadne poskytnutú, ak sú splnené všetky nasledovné minimálne podmienky:
a)Zaistené digitálne dôkazy.
b)Správa o výsledku základného (úvodného prešetrenia) forenznej analýzy do 24 hodín od podania žiadosti. Správa musí obsahovať minimálne informáciu či sa jedná o kompromitáciu systému (dôkazy, stopy a pod.), príčinu alebo zdroj kompromitácie, rozsah kompromitácie a návrh ďalšieho postupu vyšetrovania.

p.č.	názov položky	biele pole - slovný popis spôsobu naplnenia požiadavky, resp. deklarácia splnenia prožiadavky textom "spĺňa" alebo "nespĺňa", žlté pole - odkaz na dokumentáciu (názov, číslo strany, kapitola atď.), ktorá je súčasťou ponuky, kde sa dá overiť splnenie požiadavky <vyplní uchádzač>
	Požiadavky na službu Forenzná analýza	
2.184	Zozbierať dôkazy spôsobom, ktorý zabezpečí ich použitie v právnych sporoch, na súde alebo v ďalšom vyšetrovaní, t.j. pôvod, autentickosť a integritu zozbieraných dát.	Spĺňa
2.185	Uchovať získané dôkazy bezpečným spôsobom.	Spĺňa
2.186	Analyzovať získané dôkazy.	Spĺňa
2.187	Vypracovať správu o výsledkoch forenznej analýzy.	Spĺňa

Ciele Exit služby:
Cieľom služby je zabezpečiť plynulý prechod v poskytovaní služieb medzi pôvodným poskytovateľom a novým poskytovateľom služieb tak, aby nebola narušená kontinuita monitorovania IT bezpečnosti NBS. Služba je na objednávku.

Časový harmonogram poskytovania Exit služby:
Exit služba sa poskytuje po dobu 6 mesiacov.

Monitorovanie a vyhodnocovanie poskytovaných Exit služieb:
Služba sa považuje za riadne poskytnutú, ak sú splnené všetky nasledovné minimálne podmienky:
a)Požadovaná súčinnosť bola dodaná podľa požiadaviek NBS v stanovenom čase.

p.č.	názov položky	**biele pole** - slovný popis spôsobu naplnenia požiadavky, resp. deklarácia splnenia prožiadavky textom "spĺňa" alebo "nespĺňa", **žlté pole** - odkaz na dokumentáciu (názov, číslo strany, kapitola atď.), ktorá je súčasťou ponuky, kde sa dá overiť splnenie požiadavky <vyplní uchádzač>
	Požiadavky na Exit službu	
2.188	Poskytnutie súčinnosti novému poskytovateľovi na základe písomnej objednávky NBS: •pri prevzatí všetkých služieb ktoré sú predmetom zmluvy s novým poskytovateľom napr. formou workshopov, •pri riešení prevádzkových incidentov, v opodstatnených prípadoch aj priame riešenie incidentov, •pri implementácii novej funkčnosti, v opodstatnených prípadoch aj priama implementácia novej funkčnosti, •pri vykonaní migrácie case-ov (prípadov), •výmaz informácií z cloudu pôvodného poskytovateľa.	Spĺňa
2.189	Poskytnutie konzultácií novému poskytovateľovi o funkčnosti požadovanej časti systému a takisto k zdrojovému kódu, ktorý uvedenú funkčnosť zabezpečuje.	Spĺňa

POŽIADAVKY NA IMPLEMENTAČNÉ PRÁCE A SLUŽBY
NBS požaduje aby objednávateľ v rámci realizácie predmetu zmluvy dodal v obidvoch lokalitách NBS implementačné práce a služby v zmysle požiadaviek stanovených v bodoch s p.č. 2.1 až 2.189.

p.č.	názov položky	biele pole - slovný popis spôsobu napĺnenia požiadavky, resp. deklarácia splnenia prožiadavky textom "spĺňa" alebo "nespĺňa", žlté pole - príloha ktorá je súčasťou ponuky <vyplní uchádzač>
	Všeobecné požiadavky	
3.1	Uchádzač vypracuje funkčnú špecifikáciu – detailný technický popis cieľového stavu aj postup prechodu na cieľový stav v súlade so zmluvou a požiadavkami NBS. Funkčná a technická špecifikácia systému musí obsahovať minimálne: •schému a popis zapojenia jednotlivých komponentov •konfiguračné parametre komponentov (protokoly, porty, sieťovú vizibilitu a pod.) •konfiguračné nastavenia služieb (politiky, role, používatelia a pod.) •definície menných konvencií pre vytvorené objekty •popis integračných a komunikačných rozhraní •popis nastavení zberu dát •popis spracovania udalostí •popis nastavení pravidelnej automatickej archivácie dát •popis migrácie nastavení z pôvodného prostredia do nového prostredia •popis migrácie use casov, custom reportov a nastavení z pôvodného prostredia do nového prostredia •popis konfigurácie automatického zálohovania systémov •popis postupov pre diaster recovery	Spĺňa
3.2	Uchádzač zrealizuje implementáciu dodaného systému tak, aby bolo počas celej implementácie zachované monitorovanie IT bezpečnosti NBS, resp. v nevyhnutných prípadoch prerušené len na nevyhnutný čas.	Spĺňa
3.3	Uchádzač predloží architektúru služieb, procesov a produktov ktorými budú tieto služby poskytované (formou prílohy k ponuke).	Spĺňa - viď dokument 3.3 - Návrh architektúry služieb, procesov a produktov
3.4	Uchádzač predloží formou prílohy k ponuke a príp. na požiadanie odprezentuje rámcový časový plán implementácie a plán migrácie z pôvodného na dodaný systém v prostredí NBS s odhadom nutnej súčinnosti zamestnancov NBS.	Spĺňa - viď dokument 3.4 - Rámcový časový plán implementácie
	Požiadavky na dodávku, montáž a inštaláciu dodaného systému	
3.5	Uchádzač dodá a zabezpečí montáž a inštaláciu všetkých dodaných komponentov do technologických stojanov podľa požiadaviek NBS na HTP a ZTP, vrátane označenia káblov.	Spĺňa
3.6	V prípade potreby uvoľnenia potrebného priestoru v technologických stojanoch uchádzač presunie existujúce zariadenia v technologických stojanoch.	Spĺňa
3.7	Uchádzač zabezpečí demontáž zariadení, ktoré budú nahradené novými zariadeniami. Náklady spojené s demontážou a odvozom zariadení bude znášať uchádzač.	Spĺňa
3.8	Uchádzač zabezpečí bezpečné vymazanie konfigurácie demontovaných zariadení a vymazanie dát na nich uložených.	Spĺňa
3.9	Uchádzač zabezpečí vzájomne prepojenie dodaných zariadení, ako i prepojenie dodaných zariadení so zariadeniami NBS a zariadeniami ktoré nebudú nahradené, kde to bude potrebné, kabelážou priamo, resp. cez existujúce patch panelové prepojenia.	Spĺňa
3.10	Uchádzač zabezpečí inštaláciu a konfiguráciu dodaných komponentov podľa funkčnej špecifikácie.	Spĺňa
3.11	Uchádzač zabezpečí migráciu use casov, custom reportov a pod. z pôvodného prostredia do dodaného prostredia podľa funkčnej špecifikácie.	Spĺňa
3.12	Uchádzač zabezpečí konfiguráciu pravidelnej automatickej archivácie dát podľa funkčnej špecifikácie.	Spĺňa
3.13	Uchádzač zabezpečí konfiguráciu automatického zálohovania systémov.	Spĺňa
3.14	Uchádzač zabezpečí dodávku a inštaláciu aktuálneho softvérového vybavenia vrátane firmvéru na všetky dodávané zariadenia.	Spĺňa
	Požiadavky na testovanie dodaného systému	
3.15	Uchádzač vypracuje testovacie scenáre pokrývajúce testovanie všetkých funkčných čŕt implementovaného systému, vrátane testovania vybraných výkonových parametrov a výpadkov jednotlivých komponentov.	Spĺňa
3.16	Uchádzač vykoná testovanie dodaného systému v spolupráci s NBS.	Spĺňa
	Požiadavky na dokumentáciu	
3.17	Uchádzač dodá dokumentáciu k dodanému systému v elektronickej verzii vo formátoch MS Word, Excel a Visio.	Spĺňa
3.18	Uchádzač vypracuje podrobnú technickú dokumentáciu dodaného systému, ktorá nad rámec funkčnej špecifikácie bude zahŕňať minimálne: •detailný popis a schému funkčného prepojenia komponentov •detailný popis a schému fyzického zapojenia dodaných zariadení (el. kabeláž, LAN a pod.) •detailný popis konfigurácie jednotlivých zariadení (hostname, IP adresy, HW, OS, SW, komunikujúce porty a pod.) •detailný popis bezpečnostných čŕt a ich konfigurácie •detailný popis vykonaných natívnych aj custom integrácií so systémami NBS, ich nastavení a konfigurácií •detailný popis zálohovania, archivácie dát •detailný popis integrácie s centrálnym monitorovacím systémom dostupnosti NBS (Zabbix).	Spĺňa
3.19	Uchádzač vypracuje podrobnú prevádzkovú dokumentáciu dodaného systému a príslušných zariadení, ktorá nad rámec funkčnej špecifikácie bude zahŕňať minimálne: •detailné postupy pravidelnej údržby a profylaktiky •detailné postupy diagnostiky a monitorovania prevádzky •detailné postupy riešenia havarijných stavov •detailné postupy zálohovania, archivácie a obnovy konfigurácií zariadení, systémov a dát •detailné postupy pre failover primárneho systému (súbor postupov, ktoré umožnia obnovu služby na záložnom, sekundárnom zariadení).	Spĺňa
	Požiadavky na školenia	
3.20	Uchádzač zabezpečí realizáciu školení používateľov NBS pre dodávané zariadenia a systémy pre minimálne 10 používateľov	Spĺňa