#### OPIS PREDMETU ZMLUVY

#### POŽIADAVKY NA POSKYTOVANÉ SLUŽBY

NBS požaduje, aby Poskytované služby spĺňali minimálne nasledujúce požiadavky na služby:

#### Služba „Monitoring bezpečnosti IT“

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

* + 1. Priebežné monitorovanie bezpečnostných udalostí v IT NBS pomocou nástrojov SIEMu.
    2. Analýza a vyhodnotenie detegovaných podozrivých zistení v log záznamoch a udalostiach. A takisto analýza a vyhodnotenie alarmov detekčných metód a anomálií v nazbieraných dátach.
    3. Evidencia a kategorizácia prešetrovaných podozrivých zistení v denníku bezpečnostných zistení SIEM. V denníku bezpečnostných zistení SIEM je potrebné evidovať minimálne nasledovné informácie: jednoznačný identifikátor záznamu, dátum a čas zistenia, identifikátor riešiteľa, krátky popis zistenia, typ zistenia (týka sa bezpečnosti IT, prevádzky IT a pod.), kategória podozrenia (napr. závadný cieľ, prihlásenie používateľa, anomália v sieti a pod.), stav riešenia, postup riešenia, názov dotknutého systému, link na externú informáciu.
    4. Informácie evidované v denníku bezpečnostných zistení SIEM musia byť zdieľané medzi interným a externým SOC tímom. Denník bezpečnostných zistení SIEM je pomenovanie aplikácie/systému na evidenciu aktivít SOC tímov pri prešetrovaní podozrivých zistení a bezpečnostných incidentov. Pre účely denníka bezpečnostných zistení SIEM môže byť využitá existujúca NBS aplikácia alebo dodávateľom odporúčaná. Integrácia SIEM NBS a Denníka bezpečnostných zistení SIEM sa nevylučuje. Denník bezpečnostných zistení SIEM môže byť prevádzkovaný aj u dodávateľa. NBS nedisponuje automatizačnou platformou (SOAR) na orchestráciu a automatizáciu bezpečnostných operácií, incident response a threat hunting workflow.
    5. Úvodné prešetrenie podozrivých zistení, ktoré zahrňuje minimálne: popis zistenia, identifikátor riešiteľa, analýzu príčiny a rozsahu zistenia a návrh opatrení. Úvodné prešetrenie sa vykonáva pre každé podozrivé zistenie a informácia o priebehu prešetrenia, zistených skutočnostiach a výsledku prešetrenia je zaznamenaná v denníku bezpečnostných zistení SIEM. Výsledkom úvodného prešetrenia je rozhodnutie, či prešetrované zistenie je bezpečnostný alebo prevádzkový incident, prípadne odporúčanie alebo informácia..
    6. Nahlásenie prevádzkových incidentov správcom dotknutých systémov.
    7. Nahlásenie bezpečnostných incidentov správcom dotknutých systémov do Service Desku NBS. Bezpečnostné incidenty s vysokou prioritou (ktoré neznesú odklad) nahlásiť aj telefonicky správcovi dotknutého systému podľa rozpisu pohotovostí. V prípade že príslušný správca nezareaguje do 30 minút, kontaktovať osobu uvedenú v eskalačnom kontakte.
    8. Detailné prešetrenie bezpečnostných incidentov, t.j. zistenie príčiny a súvislostí vzniku bezpečnostného incidentu, vykonanie analýzy rozsahu a dopadu na IT NBS. Priebeh riešenia bezpečnostného incidentu, zistené skutočnosti a výsledok sa zaznamenáva do denníka bezpečnostných zistení SIEM. Detailné prešetrenie sa vykonáva iba pre identifikovaný bezpečnostný incident.
    9. V rámci riešenia podozrivých zistení a bezpečnostných incidentov, 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.
    10. Poskytovať súčinnosť internému SOC tímu pri riešení bezpečnostných incidentov týkajúcich sa kritických IT systémov až do ich úplného vyriešenia a odstránenia dôsledkov. Aktívny zásah je v kompetencii zamestnancov NBS.
    11. Poskytovať súčinnosť internému SOC tímu pri riešení ostatných bezpečnostných incidentov až do ich úplného vyriešenia a odstránenia dôsledkov v režime 8/5. Aktívny zásah je v kompetencii zamestnancov NBS.
    12. Aktívny Threat Hunting, 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.

**Časový harmonogram poskytovania služby:**

Režim 24/7 alebo 15/5 (počas rozšírených pracovných dní v čase od 6.00h do 21.00h s výnimkou poskytovania súčinnosti podľa bodu 2.10.)

**Monitorovanie a vyhodnocovanie poskytovaných služieb:**

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

1. Všetky prešetrenia podozrivých zistení sú zaznamenané v denníku bezpečnostných zistení SIEM do 24 hodín od ich prvej detekcie.
2. Detailné prešetrenie bezpečnostného incidentu kritického IT systému začne najneskôr do 2 hodín od rozhodnutia, že sa jedná o bezpečnostný incident.
3. Poskytovanie súčinnosti internému SOC tímu pri riešení bezpečnostných incidentov až do ich vyriešenia.

**Služba „Monitoring SIEMu“**

Cieľom služby je najmä monitorovanie a zabezpečenie dostupnosti, výkonu a funkčnosti SIEMu (LogRhythm, Netmon a Flowmon) a nepretržitého zberu a spracovania logov z existujúcich zdrojov logov. Na monitorovanie dostupnosti SIEM komponentov sa okrem SIEM nástrojov používa aj technológia Zabbix, do ktorej bude mať externý SOC tím prístup.

* + 1. Monitorovanie dostupnosti, výkonu a funkčnosti SIEMu (LogRhythm, Flowmon a Netmon), t.j. či jednotlivé komponenty SIEMu (servery, databázy, agenti, web konzola) správne fungujú (zaplnenie diskov, využitie CPU a RAM, spracovanie logov, archivácie a indexácie logov, objemu spracovávaných dát, aktualizácie Knowledge Base) a navzájom komunikujú (fungovanie LogRhythm clusteru, synchronizácie DB, atď).
    2. Monitorovanie nepretržitého zberu udalostí (LogRhythm) z jednotlivých agentov a zdrojov logov.
    3. Monitorovanie spracovávania sieťových tokov (Flowmon) a vyhodnocovania metód vo Flowmon ADS.
    4. Monitorovanie spracovávania sieťových tokov (Netmon).
    5. V prípade zistenia poruchy zberu udalostí/sieťových tokov, nahlásenie nefunkčného agenta/zdroja správcovi dotknutého systému a poskytovanie súčinnosti pri odstraňovaní problému so zberom udalostí.
    6. Zaevidovanie a kategorizovanie vzniknutého problému do prevádzkového denníka SIEM. V prevádzkovom denníku SIEM je potrebné evidovať minimálne nasledovné informácie: jednoznačný identifikátor záznamu, dátum a čas záznamu, názov dotknutého systému, popis problému a návrh jeho riešenia, stav riešenia.
    7. Informácie evidované v prevádzkovom denníku SIEM musia byť zdieľané medzi interným a externým SOC tímom. Prevádzkový denník SIEM je pomenovanie aplikácie/systému na evidenciu aktivít SOC tímov pri prevádzke SIEMu. Pre účely prevádzkového denníka SIEM môže byť využitá existujúca NBS aplikácia alebo dodávateľom odporúčaná.
    8. Problém týkajúci sa konfigurácie SIEMu odhaleného pri monitorovaní SIEMu vyriešiť do 24 hodín. V prípade, že problém 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 problému, zaevidovanie prevádzkového incidentu do prevádzkového denníka SIEM.

**Časový harmonogram poskytovania služby:**

Režim 24/7 alebo 15/5 (počas rozšírených pracovných dní v čase od 6.00h do 21.00h)

**Monitorovanie a vyhodnocovanie poskytovaných služieb:**

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

1. Všetky identifikované prevádzkové problémy sú zaznamenané v prevádzkovom denníku SIEM do 24 hodín od ich prvého výskytu.
2. Nahlásenie nefunkčného agenta/zdroja správcovi dotknutého systému do 24 hodín.
3. Poskytovanie súčinnosti pri riešení prevádzkových incidentov až do ich vyriešenia.
4. Technický report o stave SIEM – 1 x za týždeň
5. Manažérsky report o stave SIEM – 1 x za mesiac

**Služba „Prevádzka SIEMu“**

Cieľom služby je najmä vykonávanie bežných prevádzkových činností SIEMu (LogRhythm, Netmon a Flowmon) za účelom zabezpečenia funkčnosti a aktuálnosti jednotlivých komponentov SIEMu a zabezpečenia nepretržitého zberu a spracovania nazbieraných dát.

* + 1. Správa LogRhythm agentov
       1. Monitorovanie čakajúcich (Pending) LogRhythm agentov a zdrojov logov na zaradenie do systému LogRhythm.
       2. Zaradenie čakajúcich (Pending) LogRhythm agentov a zdrojov logov pre ktoré už existujú pravidlá na ich parsovanie do LogRhytm do 3 pracovných dní.
       3. Vyradenie LogRhythm agentov a zdrojov logov udalostí na základe požiadaviek NBS do 3 pracovných dní od zadania požiadavky.
    2. Správa LogRhythm zdrojov logov (logsources)
       1. Monitorovanie čakajúcich (Pending) zdrojov logov na zaradenie do systému LogRhythm počas pracovných dní.
       2. Zaradenie čakajúcich (Pending) zdrojov logov pre ktoré už existujú pravidlá na ich parsovanie do LogRhytm do 3 pracovných dní.
       3. Vyradenie zdrojov logov udalostí na základe požiadaviek NBS do 3 pracovných dní od zadania požiadavky.
    3. Správa LogRhythm entít, t.j. zaraďovanie, vyraďovanie a konfigurácia entít súvisiacich so správou agentov a zdrojov logov.
    4. Správa LogRhythm listov, t.j. vytváranie, deaktivácia a aktualizácia LogRhytm custom listov.
    5. Správa LogRhythm Log processing politík, t.j. vytváranie, deaktivácia a aktualizácia Log processing politík.
    6. Správa LogRhythm používateľov a ich profilov, t.j. pridávanie nových používateľov, nastavenie ich profilov a deaktivácia.
    7. Správa LogRhythm reportov, t.j. aktualizácia šablón reportov, reportov a balíkov reportov.
    8. Správa LogRhythm AI korelačných pravidiel, t.j. aktualizácia a deaktivácia LogRhythm AI korelačných pravidiel.
    9. Správa LogRhythm Web Console, t.j. konfigurácia a riešenie problémov LogRhythm Web Console používateľov.
    10. Správa LogRhythm Netmon dashboardov a pravidiel, t.j. konfigurácia a riešenie problémov s dashboardami a pravidlami pre alerty.
    11. Správa Flowmon Configuration Center, konfigurácia a riešenie problémov.
    12. Správa Flowmon Monitoring Center, t.j. aktualizácia a deaktivácia zdrojov, profilov, alertov a reportov.
    13. Správa Flowmon Anomaly Detection System, t.j. aktualizácia a deaktivácia detekčných metód, filtrov, reportov, blacklistov a false positive listov.
    14. Správa Flowmon Dasboard and Reports, t.j. konfigurácia a riešenie problémov s dashboardami, reportami, kapitolami a rozvrhmi používateľov.
    15. Aktualizácia SIEM serverov, t.j. pravidelná mesačná aktualizácia SIEM serverov (Windows OS a nainštalovaného SW, Flowmon OS, Flowmon ADS, Netmon appliance a iDRAC).
    16. Súčinnosť pri inštalácii, aktualizácii a upgrade LogRhythm komponentov.
    17. Súčinnosť pri inštalácii, aktualizácii a upgrade LogRhythm agentov na koncových systémoch.
    18. Evidencia vykonaných zmien v prevádzkovom denníku SIEM.

**Časový harmonogram poskytovania služby:**

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

**Monitorovanie a vyhodnocovanie poskytovaných služieb:**

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

1. Všetky zmeny v konfigurácii SIEMu sú zaznamenané v prevádzkovom denníku SIEM do 24 hodín od ich vykonania.
2. Aktualizácia SIEM serverov - 1x za mesiac

**Služba „Rozvoj SIEMu“**

Cieľom služby je najmä tvorba a úprava konfigurácie systémov LogRhythm, Netmon, FlowMon a vytváranie nových a údržba existujúcich use casov. Táto Poskytovaná služba je **na objednávku**.

* + 1. Integrácia nových typov zdrojov logov do systému LogRhythm 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 systému LogRhythm a návrh a úprava spracovania logov existujúceho zdroja logov t.j. ide aj o návrh, tvorbu a úpravu politík spracovania logov (Log Processing Policies, MPE Rule Builder).
    2. Tvorba a úprava investigácií a reportov v systéme LogRhythm a Flowmon na základe požiadaviek NBS.
    3. Tvorba a úprava AI korelačných pravidiel a pravidiel generovania alarmov v systéme LogRhythm na základe požiadaviek NBS.
    4. Tvorba a úprava detekčných metód v systéme Flowmon a Netmon
    5. Nešpecifikované konfiguračné úpravy systémov LogRhythm, Netmon a Flowmon podľa požiadaviek NBS.
    6. Návrh nového use casu, t.j. vyjasnenie zadania use casu (cieľ, zameranie, rozsah, popis, výstupy), analýzu riešenia a vypracovanie zadania use casu.
    7. Vytvorenie nového use casu, t.j. zabezpečenie logovania a parsovania relevantných udalostí, vytvorenie korelačných pravidiel, reportov a notifikácií, vyladenie a otestovanie use casu.
    8. Údržba existujúcich use casov, t.j. po zmenách v IT NBS, ktoré majú dopad na use casy, kontrola všetkých komponentov use casu vrátane správneho parsovania udalostí, aktuálnosti listov a pod.
    9. Dokumentácia nových use casov a vykonaných zmien v existujúcich use casoch.
    10. Evidencia vykonaných zmien v prevádzkovom denníku SIEM.

**Časový harmonogram poskytovania služby:**

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

**Monitorovanie a vyhodnocovanie poskytovaných služieb:**

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

1. Požadovaná úprava je vykonaná podľa požiadaviek NBS a v stanovenom čase.
2. Use case je zrealizovaný podľa požiadaviek NBS a v stanovenom čase.
3. Všetky zmeny v konfigurácii SIEMu sú zaznamenané v prevádzkovom denníku SIEM do 24 hodín od ich vykonania.

**Služba „Optimalizácia SIEMu“**

Cieľom služby je najmä pravidelné vyhľadávanie anomálií v nazbieraných dátach, stavu parsovania udalostí a posudzovanie kvality fungovania vyhodnocovania bezpečnostných udalostí v systémoch LogRhythm, Netmon a Flowmon 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 systém LogRhythm, Netmon a Flowmon, 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. Táto Poskytovaná služba je **na objednávku**.

* + 1. 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.
    2. Vyhodnocovanie stavu parsovania udalostí, t.j. posudzovanie správneho parsovania a normalizácie udalostí.
    3. Posudzovanie zmysluplnosti zbieraných údajov a ich ďalšie spracovanie a archivácia.
    4. Vypracovávanie odporúčaní a návrhov na zlepšenie kvality fungovania zberu a vyhodnocovania bezpečnostných udalostí. Súčasťou služby sú aj konzultácie k vypracovaným odporúčaniam a návrhom.
    5. Stretnutie členov tímu k optimalizácii a rozvoju SIEMu, t.j. pravidelná štvrťročná účasť na stretnutiach členov tímu spravujúceho systém LogRhythm, Netmon a Flowmon. Pravidelná štvrťročná analýza prerokovaných a zistených nedostatkov a vypracovanie návrhu ďalšieho rozvoja SIEMu.

**Časový harmonogram poskytovania služby:**

1x za týždeň, 1x za mesiac a 1 x štvrťrok.

**Monitorovanie a vyhodnocovanie poskytovaných služieb**:

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

1. Report o anomáliách v počtoch udalostí (výrazne zvýšený/znížený počet, nové typy alebo udalosti ktoré prestali chodiť a pod.) – 1 x za týždeň.
2. Report o stave parsovania udalostí a posúdenie zmysluplnosti zbieraných údajov - 1 x za mesiac.
3. Analýza zistených nedostatkov a vypracovanie návrhu ďalšieho rozvoja SIEMu - stretnutie 1 x za štvrťrok.

**Služba „Sledovanie IT hrozieb a zraniteľností“**

Cieľom služby je sledovanie aktuálnych zraniteľností publikovaných na overených externých zdrojoch s cieľom identifikovať potenciálne hrozby pre IT NBS. Ako jeden zo zdrojov môže poslúžiť aj technológia Tenable do ktorej bude mať externý SOC tím prístup.

* + 1. Denné vyhodnocovanie aktuálnych IT hrozieb a zraniteľností z overených externých zdrojov.
    2. Vyhodnotenie relevantnosti IT hrozieb a zraniteľností s identifikáciou IT NBS ktorých sa týka zraniteľnosť.
    3. Ohodnotenie závažnosti, resp. rizikovosti relevantných IT hrozieb a zraniteľností.
    4. 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 zraniteľností.
    5. Upozornenie správcov dotknutých IT s návrhom vykonania odporúčaných nápravných opatrení.
    6. Prístup do portálu služby pre minimálne 3 zamestnancov NBS s možnosťou nastaviť filter pre zobrazované zraniteľnosti podľa technológií využitých v IT NBS.

**Časový harmonogram poskytovania služby:**

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

**Monitorovanie a vyhodnocovanie poskytovaných služieb:**

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

1. Vyhodnotenie aktuálnych zraniteľností a ich relevantnosti - 1 x za deň.

**Služba „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. Táto Poskytovaná služba je na objednávku.

* + 1. Zozbierať dôkazy spôsobom, ktorý zabezpečí ich použitie v právnych sporoch, na súde alebo v ďalšom vyšetrovaní, t.j. pôvod, autentickosť a integritu zozbieraných dát.
    2. Uchovať získané dôkazy bezpečným spôsobom.
    3. Analyzovať získané dôkazy.
    4. Vypracovať správu o výsledkoch forenznej analýzy.

**Časový harmonogram poskytovania služby:**

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:**

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

1. Zaistené digitálne dôkazy.
2. 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

**Exit služba:**

* + 1. Poskytnutie súčinnosti novému poskytovateľovi na základe písomnej objednávky objednávateľa:
    2. pri prevzatí všetkých služieb ktoré sú predmetom tejto Zmluvy napr. formou workshopov,
    3. pri riešení prevádzkových incidentov, v opodstatnených prípadoch aj priame riešenie incidentov,
    4. pri implementácii novej funkčnosti, v opodstatnených prípadoch aj priama implementácia novej funkčnosti.
    5. Poskytnutie konzultácií novému poskytovateľovi o funkčnosti požadovanej časti systému a takisto k zdrojovému kódu, ktorý uvedenú funkčnosť zabezpečuje.

Exit služba sa poskytuje po dobu 3 mesiacov, maximálne 150 osobohodín.

**Spôsob poskytovania služieb:**

* + 1. Všetky Poskytované služby sú poskytované primárne zabezpečeným vzdialeným prístupom. V prípade potreby a po vzájomnej dohode objednávateľa a poskytovateľa službu je možné poskytovať v priestoroch objednávateľa na vopred stanovenú dobu.
    2. Maximálny reakčný čas dodávateľa na dotaz alebo žiadosť NBS formou e-mailu alebo telefonicky je 30 minút. Reakčný čas sa uplatňuje na všetky služby.
    3. Externý SOC tím bude mať prístup do všetkých SIEM NBS technológií.
    4. Externý SOC tím bude ma mať prístup (read only) aj do podporných technológií (Trellix ePO, Trellix ATD, Trellix EDR, Barracuda WAF NBS a pod.) pre potreby prešetrovania bezpečnostných udalostí v IT NBS. V prípade potreby môže NBS vytvoriť prístupy pre externý SOC tím aj do iných systémov NBS.

**Komunikácia**

Zmluvné strany si po uzatvorení Zmluvy vo fáze prípravy nábehu poskytovania Poskytovaných služieb vzájomne písomne oznámia preferované komunikačné kanály.