## SIEM SOC – špecifikácia služieb a aktivít (návrh)

**Prehľadová tabuľka služieb**

|  |  |  |  |
| --- | --- | --- | --- |
| Služba | Aktivity | Externý SOC team | Interný SOC team |
| Monitoring bezpečnosti IT | * Monitoring bezpečnosti IT NBS
* Detekcia podozrivých zistení v log záznamov, udalostí a alarmov
* Zaevidovanie a kategorizovanie prešetrovaných podozrivých zistení
* Úvodné prešetrenie podozrivých zistení a rozhodnutie či sa jedná o bezpečnostný alebo prevádzkový incident
* Detailné prešetrenie bezpečnostných incidentov
* Reportovanie bezpečnostných a prevádzkových incidentov internému SOC teamu
* Podieľať sa na riešení bezpečnostných incidentov týkajúcich sa kritických IT systémov NBS
* Podieľať sa na riešení ostatných bezpečnostných incidentov
 | 24/7 |  |
| 8/5 |
| 8/5 | 8/5 |
| Monitoring SIEMu | * Monitorovanie dostupnosti, výkonu a funkčnosti SIEMu
* Monitorovanie nepretržitého zberu udalostí (LogRhythm a Flowmon)
* Monitorovanie spracovávania sieťových tokov (Flowmon) a vyhodnocovania metód vo Flowmon ADS
* Monitorovanie spracovávania sieťových tokov (Netmon)
* Zaevidovanie a kategorizovanie vzniknutého problému
* Vyriešenie vzniknutých problémov odhalených pri monitorovaní SIEMu
 | 24/7 |  |
| Prevádzka SIEMu | * Správa LogRhythm agentov
* Správa LogRhythm zdrojov logov (logsources)
* Správa LogRhythm entít
* Správa LogRhythm listov
* Správa LogRhythm Log processing politík
* Správa LogRhythm používateľov a ich profilov
* Správa LogRhythm reportov
* Správa LogRhythm AI korelačných pravidiel
* Správa LogRhythm Web Console
* Správa LogRhythm Netmon dashboardov a pravidiel
* Správa Flowmon Configuration Center
* Správa Flowmon Monitoring Center
* Správa Flowmon Anomaly Detection System
* Správa Flowmon Dasboard and Reports
* Aktualizácia SIEM serverov
* Aktualizácia LogRhythm na vyššiu verziu
* Súčinnosť pri inštalácii, aktualizácii a upgrade LogRhythm agentov
* Evidencia vykonaných zmien
 | 8/5 |  |
| Rozvoj SIEMu | * Integrácia nových typov zdrojov (LogRhythm a Flowmon)
* Tvorba a úprava investigácií a reportov v systéme LogRhythm a Flowmon
* Tvorba a úprava AI korelačných pravidiel a pravidiel generovania alarmov
* Tvorba a úprava detekčných metód Flowmon a Netmon
* Nešpecifikované konfiguračné úpravy systémov LogRhythm, Netmon a Flowmon
* Evidencia vykonaných zmien
 | 8/5 | 8/5 |
| Optimalizácia SIEMu | * Vyhodnocovanie anomálií v nazbieraných dátach
* Vyhodnocovanie stavu parsovania udalostí
* Posudzovanie zmysluplnosti zbieraných údajov a ich ďalšie ukladanie a spracovanie
* Vypracovávanie odporúčaní a návrhov na zlepšenie kvality fungovania zberu a vyhodnocovania bezpečnostných udalostí
* Konzultácie k návrhom riešenia anomálií
* Stretnutie členov tímu k optimalizácii a rozvoju SIEMu
 | 1x mesačne |  |
| 4x rok | 4x rok |
| Sledovanie IT hrozieb a zraniteľností | * Denné vyhodnocovanie aktuálnych IT hrozieb a zraniteľností
* Vyhodnotenie relevantnosti IT hrozieb a zraniteľností pre IT NBS
* Identifikácia IT NBS ktorých sa týka zraniteľnosť
* Upozornenie správcov dotknutých IT
 |  | 8/5 |
| Rozvoj use casov | * Návrh nového use casu
* Vytvorenie nového use casu
* Údržba existujúcich use casov
* Dokumentácia nových use casov a vykonaných zmien
 | 8/5 | 8/5 |

## Definície:

**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.

**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,

 3. poškodenie mena NBS

**Prevádzkový incident**: akákoľvek udalosť ktorá je spôsobená správou a prevádzkou IT infraštruktúry a IS NBS.

**Kritický IT systém NBS**: Explicitne určený zoznam IT služieb a ich komponentov (napr. SWIFT, SIPS, ...)

## Špecifikácia služieb

##### **Špecifikácia služby „Monitoring bezpečnosti IT“**

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

1. Monitoring bezpečnosti IT NBS, t.j. priebežné monitorovanie bezpečnostných udalostí v systémoch SIEMu.
2. Detekcia podozrivých zistení v log záznamov, udalostí a alarmov, t.j. detekcia podozrivých zistení na základe alarmov z detekčných metód udalostí a anomálií v nazbieraných dátach.
3. Zaevidovanie a kategorizovanie prešetrovaných podozrivých zistení v denníku bezpečnostných zistení SIEM (teraz Analýza zachytených udalostí)
4. Úvodné prešetrenie podozrivých zistení a rozhodnutie či sa jedná o bezpečnostný alebo prevádzkový incident. Po vykonaní úvodného prešetrenia je správa o priebehu prešetrenia, zistených skutočnostiach a výsledku prešetrenia zaznamenaná do denníka bezpečnostných zistení SIEM.
5. Detailné prešetrenie bezpečnostných incidentov, t.j. vykonanie analýzy súvislostí a zistenie rozsahu a príčiny vzniku bezpečnostného incidentu. Ak je možné, navrhnúť opatrenia na zamedzenie jeho opakovania, alebo vypracovať návrh na zabezpečenie včasnej identifikácie v prípade opakovania. V prípade identifikácie falošného poplachu navrhnúť opatrenia na zamedzenie jeho opakovania. Priebeh riešenia bezpečnostného incidentu, zistené skutočnosti a výsledok zaznamenať do denníka bezpečnostných zistení SIEM.
6. Podieľať sa na riešení
	1. bezpečnostných incidentov týkajúcich sa kritických IT systémov v režime 24/7
	2. ostatných bezpečnostných incidentov v režime 8/5
7. Reportovanie bezpečnostných a prevádzkových incidentov internému SOC teamu

**Časový harmonogram poskytovania služby:**

Nepretržite počas kalendárnych dní (režim 24/7).

 **Spôsob poskytovania služby:**

* 1. Služba je poskytovaná zabezpečeným vzdialeným prístupom. Po vzájomnej dohode objednávateľa a poskytovateľa, je možné ju poskytovať v priestoroch objednávateľa.
	2. Dostupnosť služby nesmie v rámci 1 dňa (0:00-24:00) klesnúť pod 0,95.

**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 identifikácie bezpečnostného incidentu,
	3. podieľanie na riešení bezpečnostných incidentov až do ich vyriešenia.

##### **Špecifikácia služby „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.

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 a Flowmon) z jednotlivých agentov a zdrojov logov a riešenie tých zdrojov logov:
	1. ktoré nekomunikujú viac ako 1 pracovný deň (logy z kritických systémov NBS a logy use casov)
	2. ktoré nekomunikujú viac ako 3 pracovné dni (ostatné logy).
3. Monitorovanie spracovávania sieťových tokov (Flowmon) a vyhodnocovania metód vo Flowmon ADS.
4. Monitorovanie spracovávania sieťových tokov (Netmon).
5. Zaevidovanie a kategorizovanie vzniknutého problému do prevádzkového denníka SIEM.
6. Vyriešenie vzniknutého problému odhaleného pri monitorovaní SIEMu 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:**

Nepretržite počas kalendárnych dní (režim 24/7).

**Spôsob poskytovania služby:**

* 1. Služba je poskytovaná zabezpečeným vzdialeným prístupom. Po vzájomnej dohode objednávateľa a poskytovateľa, je možné ju poskytovať v priestoroch objednávateľa.
	2. Dostupnosť služby nesmie v rámci 1 dňa (0:00-24:00) klesnúť pod 0,95.

**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. podieľanie na riešení prevádzkových incidentov až do ich vyriešenia.

##### **Špecifikácia služby „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 logov z existujúcich zdrojov logov.

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. Aktualizácia LogRhythm na vyššiu verziu podľa potreby (min. 2 x ročne).
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).

**Spôsob poskytovania služby:**

* 1. Služba je poskytovaná zabezpečeným vzdialeným prístupom. Po vzájomnej dohode objednávateľa a poskytovateľa, je možné ju poskytovať v priestoroch objednávateľa.
	2. Dostupnosť služby nesmie v priebehu 8 pracovných hodín klesnúť pod 0,95.

**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. 1x mesačne - aktualizácia SIEM serverov
	3. 1x polrok - aktualizácia LogRhythm na vyššiu verziu

##### **Špecifikácia služby „Rozvoj SIEMu“**

Cieľom služby je najmä tvorba a úprava konfigurácie systémov LogRhythm, Netmon a FlowMon. Služba bude 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. 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).

**Spôsob poskytovania služby:**

* 1. Služba je poskytovaná zabezpečeným vzdialeným prístupom. Po vzájomnej dohode objednávateľa a poskytovateľa, je možné ju poskytovať v priestoroch objednávateľa.

**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. všetky zmeny v konfigurácii SIEMu sú zaznamenané v prevádzkovom denníku SIEM do 24 hodín od ich vykonania.

##### **Špecifikácia služby „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.

1. Vyhodnocovanie anomálií v nazbieraných dátach. Pod anomáliami v nazbieraných dátach sa rozumie napr. výrazne zvýšená alebo znížená početnosť udalostí určitého typu oproti bežnému výskytu, výskyt udalostí, ktoré sa bežne nevyskytujú a pod.
2. Vyhodnocovanie stavu parsovania udalostí, t.j. posudzovanie správneho parsovania a normalizácie udalostí z rôznych zdrojov.
3. Posudzovanie zmysluplnosti zbieraných údajov a ich ďalšie ukladanie a spracovanie.
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 mesačne a 1 x štvrťročne

**Spôsob poskytovania služby:**

* 1. Služba je poskytovaná zabezpečeným vzdialeným prístupom. Po vzájomnej dohode objednávateľa a poskytovateľa, je možné ju poskytovať v priestoroch objednávateľa.

**Monitorovanie a vyhodnocovanie poskytovaných služieb:**

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

* 1. 1 x mesačne report - vyhodnotenie anomálií v nazbieraných dátach, stavu parsovania udalostí a posúdenie zmysluplnosti zbieraných údajov,
	2. 1 x štvrťročne stretnutie - analýza zistených nedostatkov a vypracovanie návrhu ďalšieho rozvoja SIEMu.

##### **Špecifikácia služby „Sledovanie IT hrozieb a zraniteľností“**

Cieľom služby je sledovanie aktuálnych zraniteľností publikovaných na overených externých zdrojoch s cieľom identifikovať potenciálne hrozby pre IT NBS.

1. Denné vyhodnocovanie aktuálnych IT hrozieb a zraniteľností z overených externých zdrojov.
2. Vyhodnotenie relevantnosti IT hrozieb a zraniteľností pre IT NBS.
3. Identifikácia IT NBS ktorých sa týka zraniteľnosť.
4. Upozornenie správcov dotknutých IT s odporúčaním vykonania odporúčaných nápravných opatrení.

**Časový harmonogram poskytovania služby:**

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

**Spôsob poskytovania služby:**

* 1. Služba je poskytovaná zabezpečeným vzdialeným prístupom. Po vzájomnej dohode objednávateľa a poskytovateľa, je možné ju poskytovať v priestoroch objednávateľa.
	2. Dostupnosť služby nesme v priebehu mesiaca (pracovné dni) klesnúť pod 95 %.

**Monitorovanie a vyhodnocovanie poskytovaných služieb:**

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

* 1. 1 x denne - vyhodnotenie aktuálnych zraniteľností a ich relevantnosti

##### **Špecifikácia služby „Rozvoj use casov“**

Cieľom služby je vytváranie nových a údržba existujúcich use casov. Služba bude na objednávku.

1. Návrh nového use casu zahŕňa vyjasnenie zadania use casu (cieľ, zameranie, rozsah, popis, výstupy), analýzu riešenia a vypracovanie zadania use casu.
2. Vytvorenie nového use casu, t.j. zabezpečenie logovania a parsovania relevantných udalostí, vytvorenie korelačných pravidiel, reportov a notifikácií, vyladenie a otestovanie use casu.
3. 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.
4. Dokumentácia nových use casov a vykonaných zmien v existujúcich use casoch.

**Časový harmonogram poskytovania služby:**

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

**Spôsob poskytovania služby:**

* 1. Služba je poskytovaná zabezpečeným vzdialeným prístupom. Po vzájomnej dohode objednávateľa a poskytovateľa, je možné ju poskytovať v priestoroch objednávateľa.

**Monitorovanie a vyhodnocovanie poskytovaných služieb:**

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

* 1. use case je zrealizovaný podľa požiadaviek NBS a v stanovenom čase,
	2. všetky zmeny v konfigurácii SIEMu sú zaznamenané v prevádzkovom denníku SIEM do 24 hodín od ich vykonania.