Monitoring kybernetickej bezpečnosti – účel dokumentu

Účelom dokumentu je definovať zámer, plánovaný rozsah a kroky na dosiahnutie obstarania a zavedenia do prevádzky služby „Monitoring kybernetickej bezpečnosti“.

Špecifikácia služby

- balík služieb a technológií, ktorý bude poskytovaný dodávateľom, tzv. outsourcing
- doba poskytovania - 5 rokov (1.9.2025 - 31.8.2030)
- služba bude poskytovaná na technológiách umiestnených v cloude a/alebo on-site
- všetky potrebné licencie, hardvér a oprávnenia budú súčasťou dodávky služby
- súčasťou služby bude aj starostlivosť o technológie (prevádzka, aktualizácie a pod.)
- služba bude poskytovaná primárne zabezpečeným vzdialeným prístupom
- služba bude poskytovaná v súlade s ESCB guidelines, legislatívou a best practice
- služba bude poskytovaná v režime 15/5 s opciou 24/7
- služba bude poskytovaná s rozšírenou funkčnosťou a pokrytím ako súčasná služba

Obsah služby

- **SOC** - vyhľadávanie a prešetrenie podozrivých log záznamov, udalostí a alarmov a riešenie bezpečnostných incidentov
- **MBIT (Monitoring bezpečnosti IT) –** monitorovanie a zabezpečenie dostupnosti, výkonu a funkčnosti on-site komponentov MBIT (SIEM a NDR), tvorba a úprava konfigurácie komponentov MBITu, vytváranie nových a údržba existujúcich use casov, pravidelné vyhľadávanie anomálií v nazbieraných dátach, posudzovanie kvality vyhodnocovania bezpečnostných udalostí komponentmi MBITu, vypracovávanie odporúčaní a návrhov na zlepšenie kvality zberu a vyhodnocovania bezpečnostných udalostí
- **Skenovanie zraniteľností** - pravidelné automatizované skenovanie zraniteľností v IT infraštruktúre NBS (servery a zariadenia pripojené do LAN)
- **Sledovanie IT hrozieb a zraniteľností** - sledovanie aktuálnych zraniteľností publikovaných na overených externých zdrojoch s cieľom identifikovať potenciálne hrozby pre IT NBS (PC a mobilné zariadenia)
- **BAS** - pravidelná, systematická a konzistentná kontrola stavu bezpečnosti IT infraštruktúry formou simulácie prienikov a útokov na IT infraštruktúru NBS metodikou Mitre Attack
- **Forenzná analýza** - vyšetrenie bezpečnostných incidentov tak, aby získané fakty a dôkazy boli použiteľné v právnych sporoch, pred súdom, pre znalecké posudky alebo materiál na ďalšie vyšetrovanie počítačovej kriminality
- **Exit služba -** zabezpečenie podpory nábehu nových služieb po ukončení poskytovania služieb „Monitoring bezpečnosti IT“, tak aby nebola narušená kontinuita monitorovania IT bezpečnosti NBS

Obsah

1. Monitoring kybernetickej bezpečnosti – súčasný stav

1.1. Popis IT prostredia NBS

NBS prevádzkuje približne 100 informačných systémov, ktorými podporuje svoju činnosť. Správne fungovanie IS je závislé na IT infraštruktúre (odhadom viac ako tisíc IT infraštruktúrnych zariadení a systémov) ku ktorým pristupujú používatelia z viac ako 2 tisíc koncových zariadení (vrátane virtuálnych PC a mobilných zariadení).

Používané technológie v NBS - detailné informácie v priložených dokumentoch (Príloha č. 8 - Referenčná architektúra IS NBS a Príloha č.9 - Technologické štandardy NBS):

- OS serverov: Microsoft Windows, Oracle Linux, Red Hat Linux
- OS pracovných staníc: Microsoft Windows,
- OS mobilných zariadení (telefóny, tablety): Android, Apple , Apple iOS
- Sieťové prvky (FW, switch, router): Fortigate , HPE, Cisco, Forcepoint
- Databázové platformy: MS SQL, Oracle, MySQL
- Virtualizačné platformy: VMware, OpenShift
- Hlasové služby: Mitel
- MDM: Ivanti
- Cloud: Microsoft 365, Entra ID, SharePoint online, Teams online
- VPN: Fortinet
- LDAP: Microsoft AD
- Elektronická pošta: MS Exchange on premise (správa mailových objektov a smerovanie mailov) a MS Exchange online (mailové schránky)
- Bezpečnostné systémy: Trellix (ePO, EDR, EDS, ATD, Webwasher), F5 DDoS, Flowmon DDoS, Barracuda, WAF, ESET Mail Security,

Informácie o používaných technológiách v NBS sú platné v čase ich publikácie. Postupom času sa technológie môžu obmieňať a dopĺňať.

1.2. MBIT

Súčasný MBIT aktívne monitoruje kybernetickú bezpečnosť informačných systémov a IT infraštruktúry vrátane identifikácie a vyhodnocovania udalostí z pohľadu kybernetickej bezpečnosti.

MBIT infraštruktúra priebežne zbiera a vyhodnocuje udalosti z viac ako 2700 zdrojov IT infraštruktúry.

Zbierajú sa údaje:

- z prevádzky na sieťovej vrstve (toky údajov) v internej sieti a smerujúcej z/do internetu
- z IT infraštruktúry (systémové logy, aplikačné logy, databázové logy, logy zo sieťových zariadení)
- zo systémov zabezpečujúcich ochranu elektronickej pošty
- zo systémov zabezpečujúcich ochranu koncových zariadení
- zo systémov zabezpečujúcich ochranu na perimetri siete

Uvedené zdroje logov generujú približne 1000 miliónov udalostí za týždeň, čo je približne 150 miliónov udalostí za jeden deň. Na sieťovej úrovni sa počas pracovnej doby spracúva a vyhodnocuje približne 2000 flows/s (spolu na HTP a ZTP).

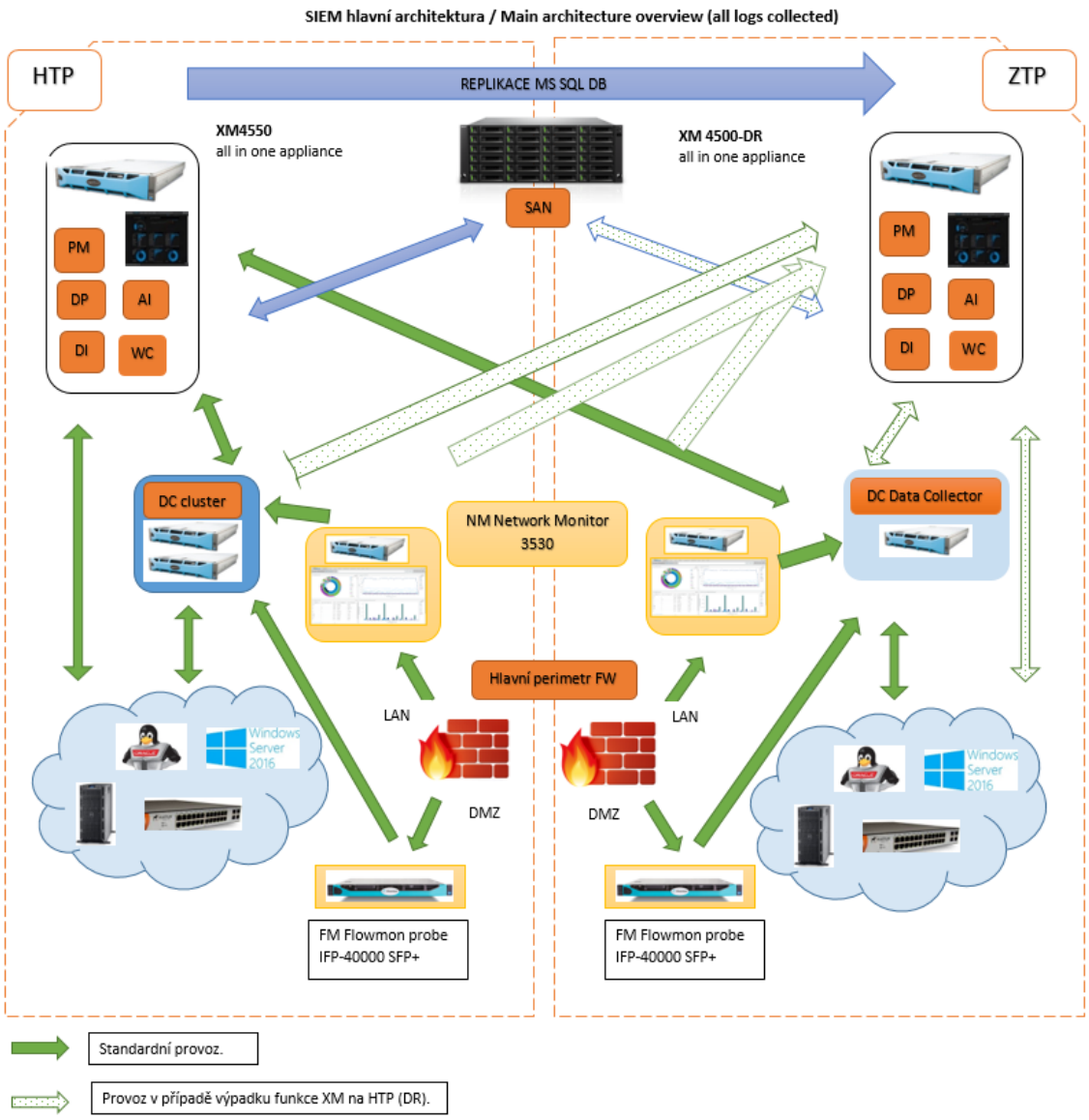
Na monitorovanie bezpečnosti IT sa využívajú technológie LogRhythm, Netmon a Flowmon, spolu 11 fyzických zariadení. Všetky 3 technológie sú zrkadlovito nasadené v lokalitách HTP a ZTP viď obrázok. V prípade, výpadku jednej lokality, druhá lokalita prevezme funkčnosť.

Technológia Flowmon (Flowmon Collector a Flowmon Probe) slúži na monitoring dátových tokov a detekciu anomálií v sieti. Systém zbiera a analyzuje dátové toky typu flow v lokálnej sieti. Na detekciu anomálií slúži modul Flowmon ADS. Detegované anomálie sa posielajú formou alarmov do SIEMu (XM).

Technológia Logrhythm Netmon je nasadená na perimetri a používa sa na detekciu použitých aplikácií a správania používateľov pri komunikácii smerom do internetu. Detegované anomálie sa posielajú formou alertu do SIEMu (XM).

Technológia Logrhythm slúži ako centrálny systém pre zber a vyhodnocovanie dát. XM združuje všetky komponenty SIEMu (PM, DP, DI, AI, WC, SM, SMP) a riadi LR agentov nainštalovaných na monitorovaných zariadeniach. LR agenti aktívne zbierajú dáta z lokálnych log súborov (k dispozícii 415 licencií).

DC zbierajú dáta z bezagentových zariadení. DC nazbierané dáta pripravia a pošlú na spracovanie do XM.



Počet monitorovaných zariadení je približne 700, z toho je cca ½ agentových a ½ bezagentových zariadení.

Verzie používaných MBIT technológií

- Flowmon OS ver. 12.xx
- Flowmon ADS ver.12.xx
- LogRhyhm ver. 7.10.x
- LogRhyhm Netmon ver. 4.x

Podpora poskytovaných technológií a služieb MBIT

Podpora výrobcu a dodávateľa pre všetky technológie MBIT je do 31.8.2025. V rámci tejto podpory sú poskytované nasledovné služby:

- Podpora výrobcu
- Podpora a údržba dodávateľa
- Konzultácie
- Školenie
- Implementácia

1.3. SOC

Od 1.7.2023 sú služby SOC zabezpečované externým dodávateľom. Poskytovanie služby je po formálnej stránke rozdelené do 2 úrovní:

Prvá úroveň SOC – Monitorovanie bezpečnostných zistení a stavu MBIT v režime 15/5.

- Monitorovanie a vyhodnocovanie bezpečnostných zistení (alarmov) - Bezpečnostní analytici priebežne monitorujú a vyhodnocujú alarmy generované v SIEMe. Na podozrivé alarmy vytvárajú bezpečnostné prípady, ktoré ad-hoc rieši 2. úroveň SOC (senior analytici). Prevádzkové incidenty týkajúce sa IT NBS priamo postupujú IT správcom NBS formou žiadosti/incidentu SD alebo cez dedikovaný TEAMS kanál. Počet používaných korelačných pravidiel z ktorých sa automaticky generujú alarmy je približne 130, z toho cca 20 pravidiel sú custom pravidlá.
- Monitorovanie a vyhodnocovanie prevádzky MBIT - Bezpečnostní analytici priebežne monitorujú stav MBIT technológií. Prevádzkové problémy so MBIT servermi postupujú na riešenie 2. úrovni SOC. Prevádzkové problémy so SIEM agentmi nasadenými na monitorovaných serveroch postupujú IT správcom NBS formou žiadosti/incidentu SD alebo cez dedikovaný TEAMS kanál.

Druhá úroveň SOC – Detailná analýza bezpečnostných zistení a riešenie prevádzkových incidentov v režim 8/5 alebo ad-hoc.

- Detailná analýza bezpečnostných zistení – Senior analytici vyhodnocujú bezpečnostné prípady v súčinnosti s IT správcami NBS. Bezpečnostné hrozby a incidenty priamo postupujú IT správcom NBS formou SD incidentu a v prípade bezpečnostných incidentov nahlasujú aj telefonicky službukonajúcemu vedúcemu IT. Za 1 pracovný týždeň rieši druhá úroveň SOC približne 10 bezpečnostných prípadov.
- Riešenie prevádzkových incidentov MBIT - Senior analytici riešia prevádzkové incidenty v súčinnosti s IT správcami NBS.
- Threat Hunting - 1x za týždeň (zvyčajne pondelok) senior analytici vykonávajú aktívny Threat Hunting, t.j. prešetria podozrivé log záznamy, udalosti a alarmy v dlhšom časovom úseku so zameraním na identifikáciu podozrivých vzorov správania a anomálií.

Interný SOC tím NBS

- Poskytuje súčinnosť externému SOC tímu, pravidelne sa stretáva s externým SOC tímom za účelom hľadať riešenie zistených nedostatkov, vyjadrovať sa k návrhom optimalizácie a ďalšieho rozvoja MBIT.
- Kontroluje prácu externého SOC.
- Navrhuje nové use casy pre špecifické systémy NBS.

Komunikačné kanály medzi jednotlivými riešiteľmi

- dedikované TEAMS kanály – bežná komunikácia

- žiadosť/incident v SD NBS – komunikácia pri časovo náročných úlohách
- telefonicky – ad-hoc komunikácia, komunikácia v kritických situáciách
- online stretnutia v MS TEAMS – pravidelné alebo ad-hoc stretnutia

Reporting

- Detailné informácie o alarmoch a bezpečnostných prípadoch sú pravidelne (1x za deň) importované do interného data warehouse (Oracle APEX), kde sú priebežne vyhodnocované a archivované. Reporty o.i. slúžia aj na kontrolu kvality SOC služieb.

1.4. Skenovanie zraniteľností

Použitá technológia spol. Tenable zabezpečuje pravidelné týždenné skenovanie zraniteľností v IT infraštruktúre, ad-hoc skenovanie podľa potreby, aj konfiguračný audit vybraných komponentov.

Technologické komponenty sú prevádzkované on-site pracovníkmi NBS:

1. Tenable.sc (ver. 6.3, správa riešenia, plánovanie skenov, správa používateľov, prístupové údaje, reporting, dashboardy, akceptácia rizík a pod.), 2 repozitáre, 3 skenovacie zóny
2. 2x Nessus skener (ver. 10.7, skenovanie zariadení v IT infraštruktúre)
3. 2x Nessus Manager (ver. 10.7, správa agentov), pričom jeden Nessus Manager je umiestnený v samostatnej zóne bez prepojenia na Tenable.sc

Počet skenovaných zariadení je približne 700, z toho je cca 1/3 agentových a 2/3 bezagentových zariadení.

NBS obstaráva licencie ako aj podporu pre produkty Tenable vždy na obdobie 1 roka.

1.5. Informácie o aktuálnych hrozbách (threat intelligence)

Na získavanie informácií o aktívnych hrozbách sa využíva nástroj ThreatGuard poskytovaný ako online služba.

Verzie používaných technológií na skenovanie zraniteľností a zisťovanie hrozieb

ThreatGuard ver. 3

Podpora poskytovaných technológií a služieb pre skenovanie zraniteľností a

Podpora poskytovaných služieb výrobcu a dodávateľa pre ThreatGuard je do 31.8.2025.

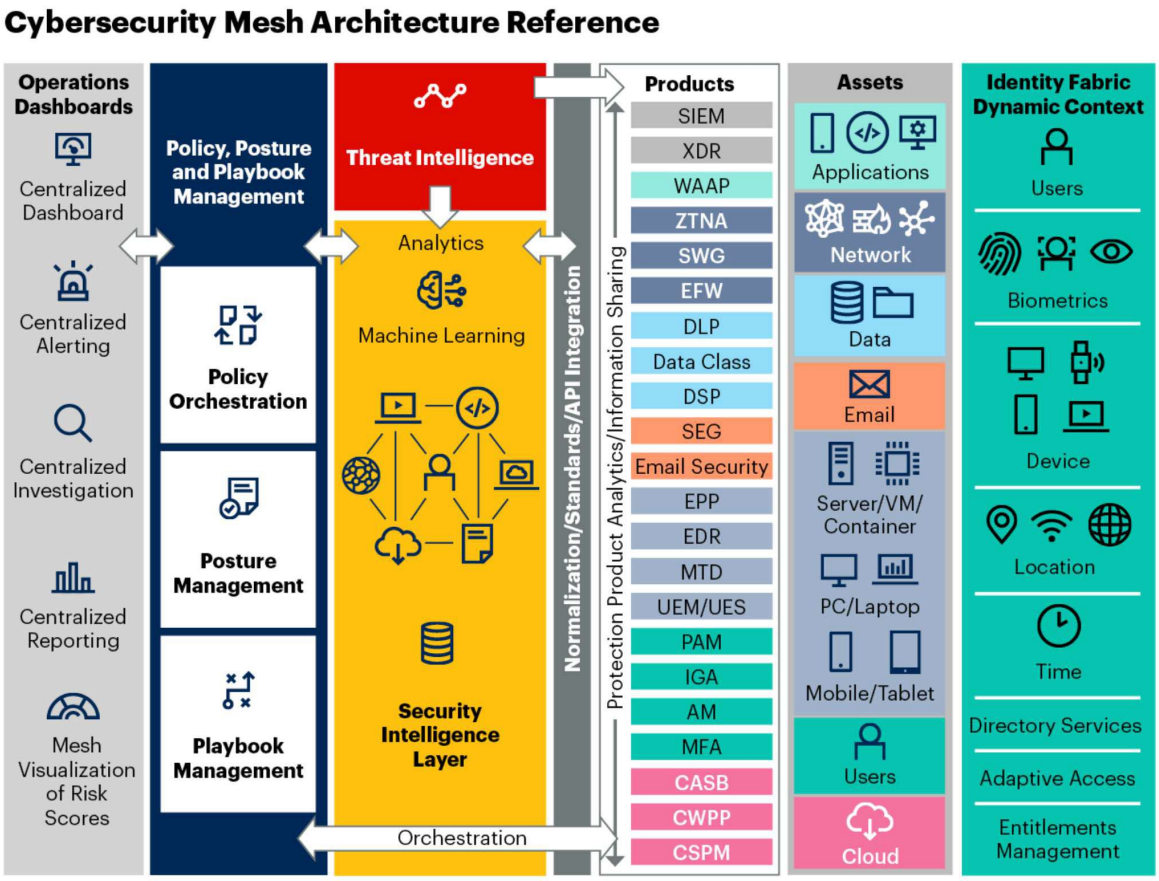
2. Monitoring kybernetickej bezpečnosti – požiadavky

2.1. Všeobecné požiadavky na služby

a) Služba bude poskytovaná na obdobie 5 rokov.
b) Služba musí spĺňať požiadavky na architektúru uvedené v prílohách (Príloha č. 7 - Architektonické princípy NBS, Príloha č. 8 - Referenčná architektúra IS NBS a Príloha č.9 - Technologické štandardy NBS).
c) Služba bude poskytovaná na technológiách umiestnených v cloude a/alebo on-site.
d) Potrebný SW a HW bude súčasťou dodávky služby.
e) Všetky potrebné licencie a oprávnenia budú súčasťou dodávky služby.
f) Súčasťou služby bude aj starostlivosť o technológie (prevádzka, aktualizácie a pod.).
g) Služba bude poskytovaná primárne zabezpečeným vzdialeným prístupom. V prípade potreby a po vzájomnej dohode, službu je možné poskytovať v priestoroch NBS na vopred stanovenú dobu.
h) SOC tím bude mať prístup do SD (riešenie žiadostí a incidentov) a podporných technológií NBS (Trellix ePO, Trellix ATD, Trellix EDR, Barracuda, WAF a pod.) pre potreby prešetrovania bezpečnostných zistení v IT NBS.
i) Služba bude poskytovaná minimálne v rozsahu súčasného monitoringu kybernetickej bezpečnosti vrátane integrácií so systémami (Trellix ATD, EPO, WebWasher, F5 DDoS a Flowmon DDoS, Barracuda WAF NBS a pod.).
j) Migrácia custom use casov zo starého na nové prostredie bude v trvaní max. 6 mesiacov
k) Služba bude poskytovať reporty o stave a kvalite služby a jej komponentov.
l) Súčasťou dodávky budú všetky podporné nástroje (reportovací nástroj, denník bezpečnostných a prevádzkových zistení a pod.)
m) Dodržanie medzinárodných štandardov a best practice.

2.2. Všeobecné požiadavky na technológie

a) Architektúra bezpečnostných nástrojov a technológií vychádzajúca z princípov Cybersecurity Mesh Architecture (CSMA) – viď. obrázok.



b) Technológie bezpečnostných nástrojov podporujúce bezpečnostné štandardy ako sú NIST, CIS, ISO a MITRE ATT&CK.
c) Podpora autentifikácie v súlade referenčnou architektúrou IS NBS (viď príloha).
d) Zber bezpečnostných udalostí z celého IT prostredia a bezpečnostných technológií v reálnom čase do jedného úložiska.
e) Centrálny dashboard pre potreby investigácie a analýzy bezpečnostných zistení.
f) Centrálny dashboard aktuálneho stavu jednotlivých komponentov bezpečnostných technológií.
g) Centrálne nastavenie metód na automatické vyhodnotenie bezpečnostných udalostí.
h) Metódy na automatické vyhodnotenie bezpečnostných udalostí využívajúce ML/AI.
i) Centrálna nastavenie rizikové skóre pre systémy a vyhodnocovacie metódy a výpočet celkového rizikového skóre.
j) Centrálny alertovací systém na základe celkového rizikového skóre.
k) Centrálny notifikačný systém (mail, sms).
l) 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, ...).

m) Centralizované playbook-y a automatizácia pri reakcii na bezpečnostné udalosti.

2.3. Služba: SOC

2.3.1. Požiadavky na službu

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

a) Priebežné monitorovanie bezpečnostných udalostí v systémoch SIEMu.
b) Detekcia bezpečnostných zistení v nazbieraných dátach.
c) Evidencia, kategorizácia a prioritizácia prešetrovaných bezpečnostných zistení.
d) Úvodné prešetrenie bezpečnostných zistení a rozhodnutie či sa jedná o podozrivú udalosť, bezpečnostnú hrozbu, bezpečnostný incident alebo prevádzkový incident.
e) Detailné prešetrenie bezpečnostných incidentov, t.j. zistenie príčiny a súvislostí vzniku bezpečnostného incidentu, vykonanie analýzy rozsahu a dopadu na IT NBS.
f) Nahlásenie prevádzkových incidentov správcom dotknutých systémov do Service Desku NBS.
g) Nahlásenie bezpečnostných incidentov do Service Desku NBS. Bezpečnostné incidenty s vysokou prioritou (ktoré neznesú odklad) nahlásiť aj telefonicky na dedikované telefónne číslo.
h) Poskytovať súčinnosť pri riešení bezpečnostných incidentov až do ich úplného vyriešenia a odstránenia dôsledkov. Aktívny zásah je v kompetencii zamestnancov NBS.
i) 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.
j) 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.
k) 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.

2.3.2. 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 bodov i,j,k)

2.3.3. Monitorovanie a vyhodnocovanie poskytovaných služieb

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

a) Všetky prešetrenia bezpečnostných zistení sú evidované.
b) Detailné prešetrenie bezpečnostného incidentu začne najneskôr do 2 hodín od rozhodnutia, že sa jedná o bezpečnostný incident.
c) Poskytovanie súčinnosti internému SOC tímu pri riešení bezpečnostných incidentov až do ich vyriešenia.

d) 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.).

2.3.4. Požiadavky na technológiu

a) Denník bezpečnostných udalostí určený na evidenciu riešenia bezpečnostných zistení.
b) Komunikačný systém na medzi SOC tímom a NBS správcami prepojený s denníkom bezpečnostných udalostí (v súčasnosti sa na komunikáciu medzi SOC tímom a NBS správcami využívajú TEAMS kanály).
c) Integrácia denníka bezpečnostných udalostí so Service Deskom NBS (CA Service Desk).
d) Zabezpečenie komunikácie SOC tímu s CSIRT, CERT a inými bezpečnostnými platformami (v súčasnosti na prijímanie emailových upozornení).

2.4. Služba: MBIT (SIEM a NDR)

Cieľom služby je monitorovanie a zabezpečenie dostupnosti, výkonu a funkčnosti on-site komponentov MBIT, nepretržitého zberu a spracovania logov a sieťových tokov, vykonávanie bežných prevádzkových činností MBIT za účelom zabezpečenia funkčnosti a aktuálnosti jednotlivých on-site komponentov MBIT a zabezpečenia nepretržitého zberu a spracovania logov z monitorovaných zariadení.

2.4.1. Požiadavky na monitoring a prevádzku MBIT

Cieľom služby je najmä monitorovanie a zabezpečenie dostupnosti, výkonu a funkčnosti on-site 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.

a) Monitorovanie dostupnosti, výkonu a funkčnosti MBIT on-site komponentov.
b) Monitorovanie nepretržitého zberu udalostí z monitorovaných zariadení a ich následného spracovania a vyhodnotenia.
c) Monitorovanie zberu a vyhodnocovania sieťových tokov v LAN NBS.
d) Správa MBIT on-site komponentov (zaraďovanie, vyraďovanie a konfigurácia).
e) Správa a konfigurácia MBIT infraštruktúry (používateľov, dashboardov, detekčných metód, korelačných a parsovacích pravidiel a pod.)
f) Zaevidovanie vzniknutého prevádzkového incidentu do prevádzkového denníka MBIT, v prípade potreby súčinnosti správcov zaevidovať do Service Desku NBS.
g) 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.

2.4.2. Časový harmonogram poskytovania služby

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

2.4.3. Monitorovanie a vyhodnocovanie poskytovaných služieb

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.

2.4.4. Požiadavky na rozvoj a optimalizáciu 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. Služba bude na objednávku.

a) 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.
b) Tvorba a úprava investigácií a reportov.
c) Tvorba a úprava korelačných pravidiel a pravidiel generovania alarmov.
d) Tvorba a úprava detekčných metód.
e) Návrh nových use case-ov, t.j. vyjasnenie zadania use case-u (cieľ, zameranie, rozsah, popis, výstupy), analýzu riešenia a vypracovanie zadania use casu.
f) Vytvorenie nových use case-ov, t.j. zabezpečenie logovania a parsovania relevantných udalostí, vytvorenie korelačných pravidiel, reportov a notifikácií, vyladenie a otestovanie use casu.
g) 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.
h) Dokumentácia nových use case-ov a vykonaných zmien v existujúcich use case-och.
i) Evidencia vykonaných zmien.
j) 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.
k) Vyhodnocovanie stavu parsovania udalostí, t.j. posudzovanie správneho parsovania a normalizácie udalostí.
l) Posudzovanie zmysluplnosti zbieraných údajov a ich ďalšie spracovanie a archivácia.
m) Vypracovávanie odporúčaní a návrhov na zlepšenie kvality fungovania zberu a vyhodnocovania bezpečnostných udalostí. Súčasťou služby sú aj konzultácie k vypracovaným odporúčaniam a návrhom.

n) Stretnutie členov tímu k optimalizácii a rozvoju MBIT, t.j. pravidelná štvrťročná účasť na stretnutiach členov tímu spravujúceho MBIT. Pravidelná štvrťročná analýza prerokovaných a zistených nedostatkov a vypracovanie návrhu ďalšieho rozvoja MBIT.
o) Nešpecifikované konfiguračné úpravy podľa požiadaviek NBS.

2.4.5. Časový harmonogram poskytovania služby

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

2.4.6. Monitorovanie a vyhodnocovanie poskytovaných služieb

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 - stretnutie 1 x za štvrťrok.

2.4.7. Požiadavky na technológiu

Všeobecné požiadavky

1. Každé dodané on-site zariadenie musí:
a) obsahovať min. 2 redundantné napájacie zdroje
b) byť montovateľné do štandardného 19'' technologického stojana (montážna sada súčasťou dodávky)
c) 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)
d) musí spĺňať požiadavky na kabeláž (Príloha č. 5 - PARAMATRE OPTICKÝCH KOMPONENTOV a Príloha č. 6 - PARAMATRE PRE METALICKÚ ŠTRUKTÚROVANÚ KABELÁŽ.pdf)
e) obsahovať všetky potrebné HW a SW komponenty vrátane všetkých licencií umožňujúce ich používať a spravovať v prostredí NBS od prvého dňa nasadenia
f) mať synchronizovaný čas z NTP
g) byť navrhnuté minimálne s výhľadom na 5 rokov, dodávateľ bude počas tejto doby poskytovať na dodané zariadenia zmluvný servis ako aj priebežné aktualizácie
h) byť postavené na štandardných HW a SW produktoch výrobcov
i) spĺňať podmienku, že nie je na zozname výrobcu oznamujúcom koniec predaja (End of Sale) alebo koniec životnosti (End of Life)
j) 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

k) 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

Požiadavky na NDR

2. NDR zariadenia dodávané on-site musia byť nakonfigurované tak, aby boli splnené nasledovné požiadavky:

a) monitorovanie sieťovej komunikácie v LAN (všetky vLANy), DMZ na HTP a ZTP
b) monitorovanie sieťovej komunikácie na perimetroch HTP a ZTP
c) všetky monitorované zariadenia z HTP logujú NetFlow informácie na jeden kolektor umiestnený na HTP
d) všetky monitorované zariadenia zo ZTP logujú NetFlow informácie na jeden kolektor umiestnený na ZTP
e) výpadok NetFlow kolektora v jednej lokalite nesmie znemožniť analýzu a spracovanie NetFlow dát (NetFlow analyzátor) kolektora v druhej lokalite

3. 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
4. NDR musí poskytovať nasledovnú funkcionalitu:

a) NetFlow analyzátor musí umožniť spracovať v jednej lokalite minimálne 150 000 flow/s
b) NetFlow infraštruktúra musí na každej lokalite umožniť uložiť udalosti po dobu min. 10 dní, t.j. min. 10 miliárd záznamov na HTP a min. 10 miliárd záznamov na ZTP
c) zber, zobrazenie, analýzu a dlhodobé uloženie sieťových štatistík (NetFlow v5/v9, IPFIX, sFlow, príp. ďalšie kompatibilné s technológiou NetFlow)
d) 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.
e) customizáciu detekčných metód a vytváranie vlastných metód
f) vytváranie automatických a custom reportov

Požiadavky na SIEM

5. SIEM zariadenia dodávané on-site musia byť nakonfigurované tak, aby boli splnené nasledovné požiadavky na vysokú dostupnosť:

a) všetky monitorované zariadenia a aplikácie z HTP logujú na jeden logserver umiestnený na HTP (logserver môže byť tvorený viacerými zariadeniami)
b) všetky monitorované zariadenia a aplikácie zo ZTP logujú na jeden logserver umiestnený na ZTP (logserver môže byť tvorený viacerými zariadeniami)
c) výpadok jedného zo zariadení zabezpečujúceho funkcionalitu logservera v danej lokalite nesmie znemožniť funkcionalitu samotného logservera
d) v prípade úplného výpadku logservera v jednej lokalite, musí logserver v druhej lokalita prevziať funkcionalitu vypadnutého logservera a to tak, aby nebola potrebná rekonfigurácia agentov/zariadení zasielajúcich dáta do systému SIEM

6. súčasťou dodávky on-site SIEM riešenia musí byť Fiber Channel pripojenie infraštruktúry na externé SAN úložisko s priepustnosťou min. 10Gbit/s. Pripojenie bude slúžiť ako externý a archivačný storage pre logy a dáta
7. SIEM musí minimálne umožniť:

a) centrálne ukladanie logov v pôvodnom tvare (raw logov)
b) spracovať minimálne 2500 záznamov za sekundu
c) uchovávať raw logy ako aj spracované udalosti minimálne po dobu 90 dní
d) zber dát z monitorovaných zdrojov pomocou agentov a/alebo bez agentov
e) zber dát minimálne pomocou syslog, SNMP v2/v3, ODBC/OLE (logy v DB tabuľkách), XML, JSON
f) spracovanie jedno a viacriadkových textových záznamov
g) normalizáciu záznamov do jednotného formátu udalosti (parsing)
h) parsovanie a spracovanie záznamov na základe preddefinovaných pravidiel od výrobcu, ktoré sú automaticky aktualizované
i) definovanie/pridávanie vlastných normalizačných pravidiel a log parserov
j) automatické korelácie udalostí
k) generovanie alarmov, napr. po vyhodnotení korelácie, príp. výskyte špecifickej udalosti
l) nastavenie rizikového skóre pre alarmy, monitorované systémy a pod.
m) automatický výpočet výsledného rizikového skóre
n) vytvárať z monitorovaných systémov logické skupiny
o) využívanie ML/AI pri spracovaní udalostí
p) out-of-the-box konektory do systémov, databáz a pod.
q) out-of-the-box vyhodnocovacie pravidlá, metódy, playbook-y a pod.
r) integráciu udalostí z bezpečnostných systémov: Trellix (ePO, EDR, EDS, ATD, Webwasher), F5 DDoS, Flowmon DDoS, Barracuda WAF, ESET Mail Security
s) investigáciu a vyhľadávanie anomálií v udalostiach
t) automatické vytváranie tiketov do Service Desku NBS
u) dlhodobú archiváciu záznamov a spracovaných udalostí - min. 1 rok
v) analytické nástroje napr. reportovanie, forenznú analýzu, nástroje na určovanie trendov, analýzu zmien, štatistickú analýzu, štatistické reporty nad aktuálnymi aj historickými dátami
w) personalizovaný dashboard
x) out-of-the-box reporty a vytvárať vlastné reporty
y) automatické spúšťanie definovaných reportov (mesačne, týždenne, denne, alebo v definovanom čase) a ich zasielanie e-mailom priamo zo systému

8. SIEM systém musí podporovať monitorovanie minimálne nasledovných IT technológií s :
   - Servery (400 ks): Microsoft Windows, Oracle Linux, Red Hat Linux
   - Sieťové prvky (FW, switch, router) 300 ks : Fortigate , HP, Cisco, Forcepoint
   - Databázové platformy: MS SQL, Oracle, MySQL
   - Virtualizačné platformy: VMware, OpenShift
   - Hlasové služby: Mitel
   - MDM: Ivanti
   - Cloud: Microsoft 365, Entra ID, SharePoint online, Teams online
   - VPN: Fortinet
   - LDAP: Microsoft AD

- Elektronická pošta: MS Exchange on premise (správa mailových objektov a smerovanie mailov) a MS Exchange online (mailové schránky)

2.5. Služba: Skenovanie zraniteľností

2.5.1. Požiadavky na službu

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

1. **Cieľové aktíva:** 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.).
2. Discovery sken infraštruktúry a identifikácia cieľových aktív, ktoré nie sú zahrnuté do pravidelného skenovania zraniteľností (min. 1x mesačne).
3. Zaraďovanie a vyraďovanie cieľových aktív do pravidelných skenov zraniteľností na základe požiadaviek NBS a výsledkov discovery skenu. Riešenie problémov pri zaraďovaní so správcami cieľových aktív.
4. **Pravidelné skenovanie.** Naplánovanie, konfigurácia a realizácia pravidelných skenov známych zraniteľností pre cieľové aktíva (každé cieľové aktívum musí byť skenované min. 1x týždenne).
5. Zohľadnenie prevádzkových obmedzení – cieľové aktíva sú skenované v časoch určených NBS.
6. 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.
7. **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.
8. Pre každú identifikovanú zraniteľnosť je v systéme k dispozícii informácia o odporúčanej nápravnej akcii alebo opatrení.
9. Možnosť akceptovať identifikovanú zraniteľnosť pre vybrané skupiny cieľových aktív do definovaného dátumu, resp. neobmedzene. Možnosť upraviť hodnotenie identifikovanú zraniteľnosť pre vybrané skupiny cieľových aktív.
10. **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.
11. Príprava kontrolných šablón pre jednotlivé typy cieľových aktív formou prispôsobenia štandardných benchmarkov (CIS, resp. definovaných výrobcami) podľa požiadaviek NBS. Údržba a aktualizácia kontrolných šablón.
12. **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 benchmarku) a false-negatives nálezov (chýbajúce detekcie).

13. Údržba, konfigurácia, aktualizácia a kontrola komponentov riešenia pre skenovanie zraniteľností (bez ohľadu na ich umiestnenie on-prem alebo off-prem).
14. **Reporting.** Príprava, definícia a naplánovanie automaticky generovaných reportov o zraniteľnostiach jednotlivých tried cieľových aktív.
    a) Reporty určené pre správcov jednotlivých tried cieľových aktív (podľa technológií).
    b) Reporty určené pre koordinátorov IT služieb a pre analýzy rizík IT služieb (podľa IT služieb).
    c) Ad-hoc reporty podľa špecifických potrieb.
15. Možnosť automatizovane zadávať tickety do Service Desk systému NBS.

2.5.2. Časový harmonogram poskytovania služby

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

2.5.3. Monitorovanie a vyhodnocovanie poskytovaných služieb

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

1. Prístup do portálu služby – nepretržite, s nedostupnosťou max. 3 x mesačne v celkovej úhrnnej dobe najviac 3 hodiny mesačne.
2. Skenovanie: Discovery sken – min. 1 x mesačne, pravidelné skenovanie IT infraštruktúry NBS – min. 1 x týždenne.
3. Kontroly konfigurácie – min. 1 x mesačne.
4. Poskytnutá súčinnosť pri riešení prevádzkových problémov týkajúcich sa skenovaní a kontrol konfigurácie až do vyriešenia.
5. Údržba komponentov systému, vrátane ich aktualizácie a prípadných úprav konfigurácie – min. 1 x mesačne.

2.5.4. Požiadavky na technológiu

1. Prístup do portálu služby pre minimálne 10 zamestnancov NBS s možnosťou nastaviť vlastné dashboardy a filtre.
2. 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.
3. Architektúra riešenia umožní skenovať oddelene tzv. Secure zónu s požiadavkou, že credentials pre prístup k systémom v zóne nemôžu byť uložené mimo tejto zóny.
4. Skenovanie aj kontroly konfigurácie sú možné voliteľne prostredníctvom agentov, resp. prostredníctvom prihlasovania účtom.
5. Predpripravené šablóny konfigurácii CIS, DISA a pod., ktoré je možné upravovať (rozsah, očakávané parametre a atribúty).
6. 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.
7. Podpora pre integráciu s Password Vault riešeniami – napr. HashiCorp Vault a pod.

8. Bezpečný komunikačný kanál medzi komponentami riešenia (obojstranne autentizovaný, so zabezpečenou dôvernosťou prenášaných údajov).
9. Možnosť filtrovať identifikované nálezy (zraniteľnosti, odchýlky od stanovenej konfigurácie) podľa závažnosti, času prvej detekcie, času ostatnej detekcie, triedy cieľových aktív, triedy zraniteľnosti, atď.
10. Možnosť exportovať filtrované údaje do čitateľného formátu (pdf), aj do strojovo spracovateľného formátu (csv).
11. Zdokumentované API pre pripojenie iných systémov a aplikácií
12. 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.
13. 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).
14. 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.
15. Použité riešenie musí byť použité ako hlavné riešenie pre správu zraniteľností v minimálne 3 centrálnych bankách, ktoré sú súčasťou ESCB.

2.6. Služba: Sledovanie IT hrozieb a zraniteľností

2.6.1. Požiadavky na službu

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

a) Denné vyhodnocovanie aktuálnych IT hrozieb a zraniteľností z overených externých zdrojov.
b) Vyhodnotenie relevantnosti IT hrozieb a zraniteľností s identifikáciou IT NBS ktorých sa týka zraniteľnosť.
c) Ohodnotenie závažnosti, resp. rizikovosti relevantných IT hrozieb a zraniteľností.
d) 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.
e) Upozornenie správcov dotknutých IT s návrhom vykonania odporúčaných nápravných opatrení.

2.6.2. Časový harmonogram poskytovania služby

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

2.6.3. Monitorovanie a vyhodnocovanie poskytovaných služieb

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

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

2.6.4. Požiadavky na technológiu

a) Prístup do portálu služby pre minimálne 3 zamestnancov NBS s možnosťou nastaviť filter pre zobrazované zraniteľnosti podľa technológií využitých v IT NBS.

2.7. Služba: BAS

2.7.1. Požiadavky na službu

Cieľom služby je zabezpečiť pravidelnú, systematickú a konzistentnú kontrolu stavu bezpečnosti IT infraštruktúry formou simulácie prienikov a útokov na IT infraštruktúru NBS metodikou Mitre Attack (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.

a) Pravidelné automatické testovanie bezpečnosti IT infraštruktúry formou simulácie techník prienikov a útokov s automatickým vyhodnotením vykonaných testov - minimálne 1 x týždeň.
b) Automatické vyhodnotenie (report) identifikovaných zraniteľností s popis závažnosti, resp. rizikovosti prípadne aj s odporúčaním nápravných opatrení.
c) Poskytovanie súčinnosti pri riešení prevádzkových problémov spojených s nasadením a prevádzkou BAS.
d) Prístup do portálu služby pre minimálne 3 zamestnancov NBS s možnosťou nastaviť vlastné dashboardy a filtre.

2.7.2. Časový harmonogram poskytovania služby

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

2.7.3. Monitorovanie a vyhodnocovanie poskytovaných služieb

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

a) Pravidelné automatické testovanie bezpečnosti IT infraštruktúry - minimálne 1 x týždeň.
b) Poskytnutá súčinnosť pri riešení prevádzkových problémov až do vyriešenia.

2.7.4. Požiadavky na technológiu

1. BAS musí minimálne umožniť:

a) bezpečné a kontrolované prostredie na testovanie kybernetickej bezpečnosti
b) kontrolu bezpečnosti za pomoci agentov a/alebo bez agentov
c) 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.
d) monitorovať o.i. aj bezpečnostné systémy NGFW, IDS, IPS, EDR , Anti-virus and Anti-malware SW, DLP, SIEM, Email GW a pod.
e) prispôsobiť scenáre testovania napr. proti hrozbám zameraným na systémy SWIFT
f) zbierať údaje o priebehu simulácie útokov a poskytovať prehľad o možných rizikách a nedostatkoch v bezpečnostných nastaveniach zariadení
g) po skončení simulácie vygenerovať komplexnú správu o bezpečnostnej situácii s podrobnými informáciami o zisteniach vrátane zistených zraniteľností, nesprávnych konfiguráciách a pod.
h) na základe výsledkov poskytnúť praktické návrhy na zmiernenie/odstránenie zistených nedostatkov
i) posúdiť bezpečnostnú ochranu proti špecifickým hrozbám z reálneho sveta
j) nedeštruktívnu simuláciu útokov, t.j. aby simulácia útoku nevytvorila bezpečnostnú dieru
k) plánovať simulácie v režime 24/7
l) integráciu s existujúcimi bezpečnostnými nástrojmi ako sú systémy SIEM, EDR a skener zraniteľnosti

1.1. Služba: Forenzná analýza

1.1.1. Požiadavky na služby

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. Služba je na objednávku.

a) Zozbierať dôkazy spôsobom, ktorý zabezpečí ich použitie v právnych sporoch, na súde alebo v ďalšom vyšetrovaní, t.j. pôvod, autentickosť a integritu zozbieraných dát.
b) Uchovať získané dôkazy bezpečným spôsobom.
c) Analyzovať získané dôkazy.
d) Vypracovať správu o výsledkoch forenznej analýzy.

1.1.2. Časový harmonogram poskytovania služby

Aktivity spojené s forenznou analýzou môže externý SOC tím vykonávať bez časového obmedzenia, t.j. v ľubovoľný deň a hodinu.

1.1.3. Monitorovanie a vyhodnocovanie poskytovaných služieb

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

1.2. Služba: Exit služba

1.2.1. Požiadavky na službu

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.

a) Poskytnutie súčinnosti novému poskytovateľovi na základe písomnej objednávky objednávateľa:
   i. pri prevzatí všetkých služieb ktoré sú predmetom zmluvy s novým poskytovateľom napr. formou workshopov,
   ii. pri riešení prevádzkových incidentov, v opodstatnených prípadoch aj priame riešenie incidentov,
   iii. pri implementácii novej funkčnosti, v opodstatnených prípadoch aj priama implementácia novej funkčnosti,
   iv. pri vykonaní migrácie case-ov (prípadov),
   v. výmaz informácií z cloudu pôvodného poskytovateľa.
b) Poskytnutie konzultácií novému poskytovateľovi o funkčnosti požadovanej časti systému a takisto k zdrojovému kódu, ktorý uvedenú funkčnosť zabezpečuje.

1.2.2. Časový harmonogram poskytovania služby

Exit služba sa poskytuje po dobu 4 mesiacov, maximálne 300 osobohodín.

1.2.3. Monitorovanie a vyhodnocovanie poskytovaných 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.

Použité skratky a pojmy

HTP – hlavné technologické pracovisko (ústredie NBS) – Imricha Karvaša 1, 813 25 Bratislava
ZTP – záložné technologické pracovisko - Kopčianska ulica 92/D, Bratislava
AD – Active Directory
BAS (Breach and Attack Simulation)
SIEM – Security Information and Event Management
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
HA - High Availability (vysoká dostupnosť)
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
SIEM – Security and Event Management
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
SIEM - Security Information and Event Management
ML/AI – Machine Learning / Artificial Intelligence