**Základné informácie**

1. Základné informácie o IT prostredí NBS:
	1. NBS prevádzkuje približne 100 zákazníckych služieb IT, ktorými podporuje svoju činnosť. Správne fungovanie IS podporuje IT infraštruktúra (34 technických služieb IT, ktoré predstavuje 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).
	2. Používané technológie v NBS. Informácie o týchto používaných technológiách v NBS sú platné v čase vyhlásenia predmetnej zákazky. V priebehu plnenia predmetu zákazky (t. j. po uzavretí zmluvy) sa tieto technológie môžu obmieňať a dopĺňať.
* OS serverov (cca 470): Microsoft Windows, Oracle Linux, Red Hat Linux z toho je cca 450 virtuálnych serverov a 20 fyzických
* OS pracovných staníc (cca 500 PC a 1100 notebookov): MS Windows 10 a 11
* OS mobilných zariadení (telefóny, tablety): Android, Apple , Apple iOS
* Sieťové prvky v počte cca 450 (FW, switch, router): Fortigate, 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, GenieATM DDoS, Barracuda, WAF, ESET Mail Security, IAM (RedHat SSO)
	1. Priepustnosť liniek: pripojenie do internetu na HTP 10Gb/s, na ZTP 1 Gb/s. Prepojenie medzi HTP a ZTP je 40 Gb/s.
	2. Segmentácia siete: cca 300 vLAN
	3. Počet prevádzkovaných AD domén: 3
1. Základné informácie o monitoringu bezpečnosti IT (ďalej len MBIT) v prostredí NBS:
	1. Súčasný MBIT aktívne monitoruje kybernetickú bezpečnosť zákazníckych služieb IT a IT infraštruktúry vrátane identifikácie a vyhodnocovania udalostí z pohľadu kybernetickej bezpečnosti.
	2. V MBIT infraštruktúre je zaregistrovaných cca 4700 zdrojov. Z toho MBIT aktívne zbiera a vyhodnocuje udalosti z viac ako 2650 zdrojov IT infraštruktúry z toho cca 2600 štandardných zdrojov cca 70 typov a cca 60 zdrojov sú špecifické logy 18 typov. Nelogujúce zdroje sú najmä nevyužívané monitory SIEM agentov.
	3. Zbierajú sa údaje:
	4. z prevádzky na sieťovej vrstve (toky údajov) v internej sieti a smerujúcej z/do internetu
	5. z IT infraštruktúry (systémové logy, aplikačné logy, databázové logy, logy zo sieťových zariadení)
	6. zo systémov zabezpečujúcich ochranu elektronickej pošty
	7. zo systémov zabezpečujúcich ochranu koncových zariadení
	8. zo systémov zabezpečujúcich ochranu na perimetri siete
	9. Uvedené zdroje logov generujú približne 1000 miliónov udalostí za týždeň, čo je približne 150 miliónov udalostí za jeden deň a viac ako 1600 udalostí za sekundu. Na sieťovej úrovni sa počas pracovnej doby spracúva a vyhodnocuje približne 5000 flows/s (spolu na HTP a ZTP).
2. Základné informácie o technickej infraštruktúre MBIT:
	1. Na monitorovanie bezpečnosti IT sa využívajú SIEM technológie LogRhythm a NDR technológie (Logrhythm Netmon a Flowmon), spolu 11 fyzických zariadení.
	2. Všetky 3 technológie sú zrkadlovito nasadené v lokalitách HTP a ZTP. V prípade, výpadku jednej lokality, druhá lokalita prevezme funkčnosť.
	3. Technológia Flowmon (Flowmon Collector R5-6000 Pro a Flowmon Probe 40000 SFP+) 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 s pridanou funkcionalitou Suricata IDS. Detegované anomálie sa posielajú formou alarmov do SIEMu (XM).
	4. Technológia Logrhythm Netmon (model NM3530) 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).
	5. Technológia Logrhythm (all-in-one appliance XM 4550) 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.
	6. DC (DELL PowerEdge R340 Server) zbierajú dáta z bezagentových zariadení. DC nazbierané dáta pripravia a pošlú na spracovanie do XM.



1. Základné informácie o technickej infraštruktúre MBIT:
	1. Počet monitorovaných zariadení je približne 700, z toho je cca ½ agentových a ½ bezagentových zariadení.
	2. Počet používaných korelačných pravidiel je približne 140, z toho cca 100 pravidiel je implementovaných na báze MITRE ATT&CK techník, cca 25 pravidiel sú custom pravidlá, ktoré sú vytvorené na základe špecifických use casov (Príloha č. 7 - Zoznam špecifických use casov.xlsx) a cca 15 pravidiel sa využíva na vyhodnocovanie prevádzky komponentov SIEMu. Počet pravidiel nie je konečný, časom pribúda.
	3. Počet dashboardov, t.j. rôznych pohľadov v LogRhythm web konzole je približne 40.
	4. Počet využívaných LogRhythm reportov je približne 20.
2. Základné informácie o technickej infraštruktúre a konfigurácii skenovania zraniteľností a hrozieb:
	1. Na aktívne skenovanie zraniteľností na serveroch sa využíva technológia Tenable, ktorá zabezpečuje pravidelné týždenné skenovanie zraniteľností v IT infraštruktúre, ad-hoc skenovanie podľa potreby, aj konfiguračný audit vybraných komponentov.
	2. Počet skenovaných zariadení je približne 680, z toho je cca 1/3 agentových a 2/3 bezagentových zariadení.
	3. Tenable.sc (správa riešenia, plánovanie skenov, správa používateľov, prístupové údaje, reporting, dashboardy, akceptácia rizík a pod.), 2 repozitáre, 3 skenovacie zóny
	4. 2x Nessus skener (skenovanie zariadení v IT infraštruktúre)
	5. 2x Nessus Manager (správa agentov), pričom jeden Nessus Manager je umiestnený v samostatnej zóne bez prepojenia na Tenable.sc
	6. Na rok 2025 je naplánovaná realizácia monitorovania vybraných systémov bežiacich na platforme OpenShift a cloudových služieb Office365.
	7. Na získavanie informácií o aktívnych bezpečnostných hrozbách (threat intelligence) sa využíva nástroj ThreatGuard poskytovaný ako online služba.
3. Verzie používaných technológií
	1. Flowmon OS ver. 12.xx
	2. Flowmon ADS ver.12.xx
	3. LogRhyhm ver. 7.16.x
	4. LogRhyhm Netmon ver. 4.x
	5. Tenable.sc ver. 6.4
	6. Nessus skener a Manager ver. 10.8
	7. ThreatGuard ver. 3
4. Licencie – počty
	1. LogRhyhm agent Lite - 405 z toho využitých 337
	2. LogRhyhm Netmon HTP - 1 Gb/s (priemerné využitie takmer 100%)
	3. LogRhyhm Netmon ZTP - 500 Mb/s (priemerné využitie cca 20%)
	4. Flowmon HTP ADS - licencia na detekciu 5000 flows/s (priemerné využitie 1500 flows/s)
	5. Flowmon ZTP ADS - licencia na detekciu 5000 flows/s (priemerné využitie 1500 flows/s)
	6. Tenable - licencia na 800 IP adries (využitie cca 680)
5. Podpora poskytovaných služieb výrobcu a dodávateľa pre všetky technológie SIEM je do 31.8.2025. V rámci tejto podpory sú poskytované nasledovné služby:
	1. Podpora
	2. Údržba
	3. Konzultácie
	4. Školenie
	5. Implementácia
	6. Služba sledovania aktuálnych IT hrozieb a zraniteľností
6. Podpora poskytovaných služieb výrobcu a dodávateľa pre ThreatGuard je do 31.8.2025.
7. Podpora poskytovaných služieb výrobcu a dodávateľa pre Tenable je do 14.2.2026.
8. Základné informácie o SOC službe:
	1. Poskytovanie služby je po formálnej stránke rozdelené do 2 úrovní:
	2. Prvá úroveň SOC – Monitorovanie bezpečnostných zistení a stavu MBIT v režime 15/5.
	3. 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.
	4. Monitorovanie a vyhodnocovanie prevádzky MBIT - Bezpečnostní analytici priebežne monitorujú stav MBIT technológií. Prevádzkové problémy s 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.
	5. Druhá úroveň SOC – Detailná analýza bezpečnostných zistení a riešenie prevádzkových incidentov v režim 8/5 alebo ad-hoc.
	6. 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.
	7. Riešenie prevádzkových incidentov MBIT - Senior analytici riešia prevádzkové incidenty v súčinnosti s IT správcami NBS.
	8. Analýza historických záznamov - 1x za týždeň (zvyčajne pondelok) senior analytici prešetria podozrivé log záznamy, udalosti a alarmy v dlhšom časovom úseku so zameraním na identifikáciu podozrivých vzorov správania a anomálií.
	9. 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.
	1. 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
	1. Reporting
	2. Detailné informácie o alarmoch, bezpečnostných prípadoch a dostupnosti komponentov SIEMu 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.
	3. Priemerný počet alarmov za týždeň je niekoľko tisíc, z toho rádovo stovky sú spracovávané na prvej úrovni SOC
	4. Za posledný rok sa druhou úrovňou SOC podrobne skúmalo spolu 590 bezpečnostných zistení a z toto 286 senior analytici detailne došetrovali v rámci Trellix EDR.

**Použité skratky 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

**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

**ML/AI** – Machine Learning / Artificial Intelligence

**Interný SOC tím** – tvoria zamestnanci NBS

**Externý SOC tím** - tvoria zamestnanci dodávateľa

**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,

3. 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.