SIEM NBS

zastrešuje a prevádzkuje oddelenie informačnej bezpečnosti (OIB) pomocou monitoringu bezpečnosti informačných technológií (IS MBIT).

## Ciele SIEMu:

* Detekcia útokov a podozrivých (neobvyklých) aktivít v IT prostredí NBS
* Pružná a rýchla reakcia na podozrivé udalosti a bezpečnostné incidenty
* Identifikácia potenciálnych hrozieb a návrh prevenčných opatrení
* Odhaľovanie anomálií

## Funkcie SIEMu:

* Zber dát a udalostí – log záznamy z OS, systémov, databáz, aplikácií a sieťových zariadení
* Normalizácia dát – zjednotenie rôznych formátov z heterogénnych zdrojov
* Korelácia – definovanie vzťahov medzi generovanými udalosťami
* Log management – uloženie log záznamov a ich indexácia
* Archivácia historických dát (logov)
* Alerting a notifikácia – automatické generovanie alertov s notifikáciu
* Informačné panely (dashboards) - prehľadové zostavy a analytické nástroje
* Reporting – súhrnné reporty

**Súčasný stav:**

NBS prevádzkuje približne 100 informačných systémov (ďalej len „IS), ktorými podporuje svoju činnosť v rámci banky. Správne fungovanie IS podporuje IT infraštruktúra (odhadom viac ako tisíc IT infraštruktúrnych zariadení a systémov) ku ktorým pristupujú používatelia z viac ako 2 tisíc koncových zariadení. SIEM aktívne monitoruje kybernetickú bezpečnosť informačných systémov a IT infraštruktúry vrátane identifikácie a vyhodnocovania udalostí z pohľadu kybernetickej bezpečnosti.

Na monitorovanie bezpečnosti IT sa využívajú SIEM technológie LogRhythm, Netmon a Flowmon. SIEM infraštruktúra priebežne zbiera a vyhodnocuje udalosti z viac ako 3000 zdrojov IT infraštruktúry.

Zbierajú sa nasledujúce 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 143 miliónov udalostí za jeden deň a viac ako 1600 udalostí za sekundu.

**Technické parametre SIEMu a poskytované služby:**

* 11 fyzických zariadení (technológie LogRhyhm, Netmon a Flowmon) umiestnených v dvoch lokalitách
* 420 licencií (agentov) pre monitorovanie serverov
* Vysoká dostupnosť SIEM riešenia (možnosť prevádzky na záložnom pracovisku)
* Monitoring tokov v sieti až po hranicu perimetra
* Monitoring tokov v sieti na úrovni aplikácií smerujúcich na internet
* Zber logov zo systémov IT infraštruktúry
* Vyhodnocovanie udalostí v reálnom čase
* Archivácia logov
* Servisné služby dodávateľa a výrobcu
  + Podpora
  + Údržba
  + Konzultácie
  + Školenie
  + Implementácia
* Služba sledovania aktuálnych IT hrozieb a zraniteľností
* Podpora poskytovaných služieb výrobcu a dodávateľa do 31.8.2025

V roku 2020 bol úspešne zrealizovaný upgrade SIEMu. Súčasťou ugrade SIEMu bola optimalizácia architektúry, predĺženie podpory komponentov a poskytovanie servisných a podporných služieb.