

Dashboard – logické vyústenie SIEM

Marek Zeman
Tatra banka, a.s.



Logo partnera

° Tatra banka, a.s. – 25 years of experience



- **Established in 1990** as the first private bank in Slovakia.
- Member of the RBI Group
- One of its most successful subsidiaries in CEE
- Modern universal bank offering complex banking services
- and solutions for corporate and individual clients.
- Third largest bank in Slovakia according to total assets.
- The aim of the bank is to achieve continuous growth of financial indicators and increased production rate combined with rationalization and strict control of operational costs.



RHODOS
CENA ZA IMAGE



TREND:

- Bank of the Year 1998, 1999, 2000, 2001, 2002 (1. place)
- Bank of the Year 2003 (3. place)
- Bank of the Year 2004 (2. place)
- Bank of the Year 2005, 2007, 2008 (1. place)
- Bank of the Year 2011 (3. place)



Tatra banka keeps strong position on bank market:

- | | |
|------------------------------------|------------------|
| • POS terminals | the 1st position |
| • loans to enterprises | the 1st position |
| • funds assets (TAM) | the 1st position |
| • client assets in private banking | the 1st position |
| • factoring turnover | the 1st position |
| • suppl.pension assets (DDS) | the 2st position |
| • number of branches | the 3rd position |
| • number of employees | the 3rd position |
| • loans to customers | the 3rd position |
| • deposits from customers | the 3rd position |
| • ATM network | the 3rd position |
| • payment cards | the 3rd position |
| • number of clients | the 5th position |

Soure: Trend, June 2012, October 2012

° Tatra Banka - Innovation leader



- Internet banking **application Tatra banka for iPhone, Android**, pre-approved loan withdrawal function, bar code scanner, etc.
- **Spending report** – Internet banking feature for managing expenses
- Card & Reader , Reader application
- Art Consulting application
- **Contactless payment cards, Mobile Pay**
- **Instantly issued Card**
- **Gift Card** – prepaid Gift Card
- New Internet banking
- **117 ATMs for blind and partially sighted**
- Digitalised signature, Document scanner
- **Socially Responsible Fund, Smart fond**
- **Mobile office** for corporate clients
- Virtual mortgage consultant (video consultation)
- Voice biometry
- Application for Google glas
- Výber z bankomatu cez mobil



Prečo sme tu práve z TB?

- 2002
 - Prvé komplexné riešenie logov pre databázy
 - Definícia procesu a pravidiel a KPI
- 2004 – Centrálné logovacia webová stránka
- 2005 – Zapojenie logovania do SDLC Tatra banky, a.s.
- 2007 – SIEM riešenie
 - 2013 – CeMoL – BI analýza nad logmi
- 2014 – Spájanie IT a non IT logov
- 2015 – Security Dashboard

Požiadavky logovania

- Logický pohľad
 - Služby
 - Jednotlivé aplikácie, zariadenia
- Otázky
 - Čo?
 - Kto?
 - Kedy?
 - Ako ?
 - Prečo?

Čo logujeme?

- HW (info o stave, funkcionalite,zmenách)
- Aplikácie (info o stave, funkcionalite,zmenách)
- Bezpečnostné riešenia (FW, WAF, AF, proxy,...)
- Interná aplikačná logika (CBS, HB,...)
- Výstupy aplikácii
(napočítané hodnoty, napr. počet prihlásení za hodinu)

Čo zobrazujeme?

- Aktuálny status funkčnosti systému
- Incidenty
 - HW
 - SW (aplikácie, DB,...)
 - Rule based
- Korelácie
 - Security incidents – rule baseddirect – in SIEM (DLP, USB, proxy,...)
 - Advanced security incidents
 - Behaviorálny scoring
- Toky
 - Sieťové
 - aplikačné

Kam zobrazujeme?

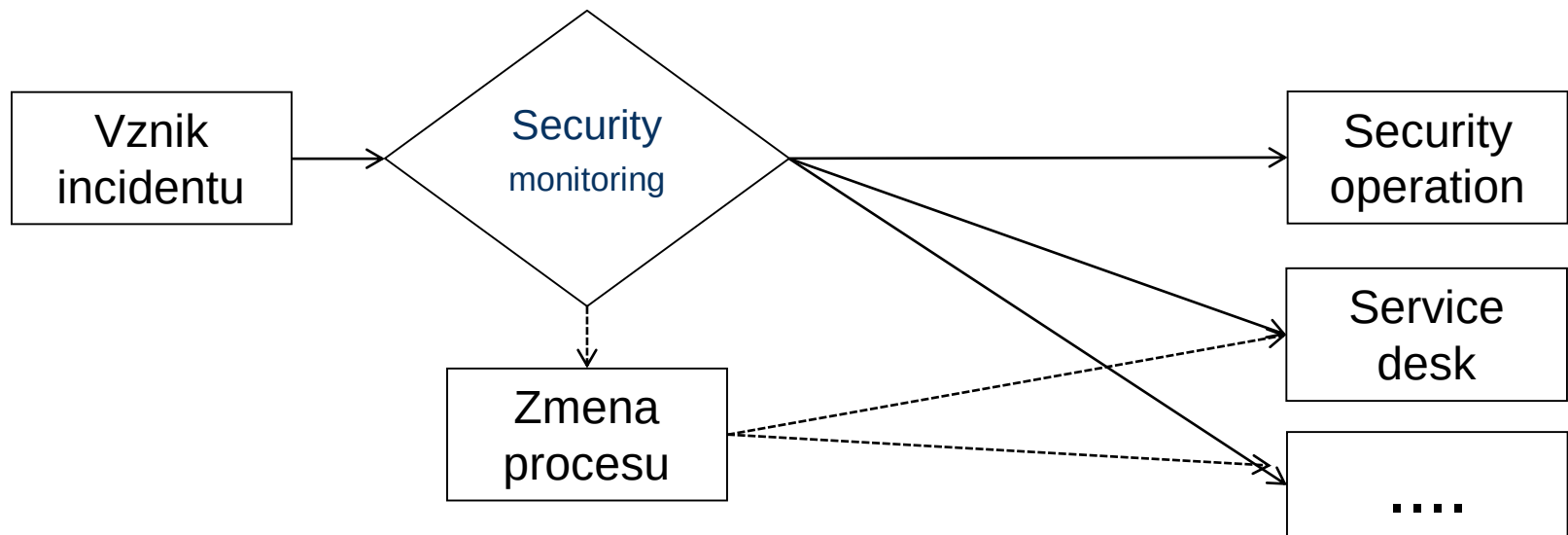
- Security Dashboard
 - Interné riešenie
 - Čo obsahuje?, okamžité a vulnerability a botnet a vírus informácie.
- SIEM
 - Potrebujete školenia
- Service desk solution
 - Integrácia
- Emails
 - Ťažké definovanie obsahu. 😊

Security dashboards



Komu to zobrazujeme?

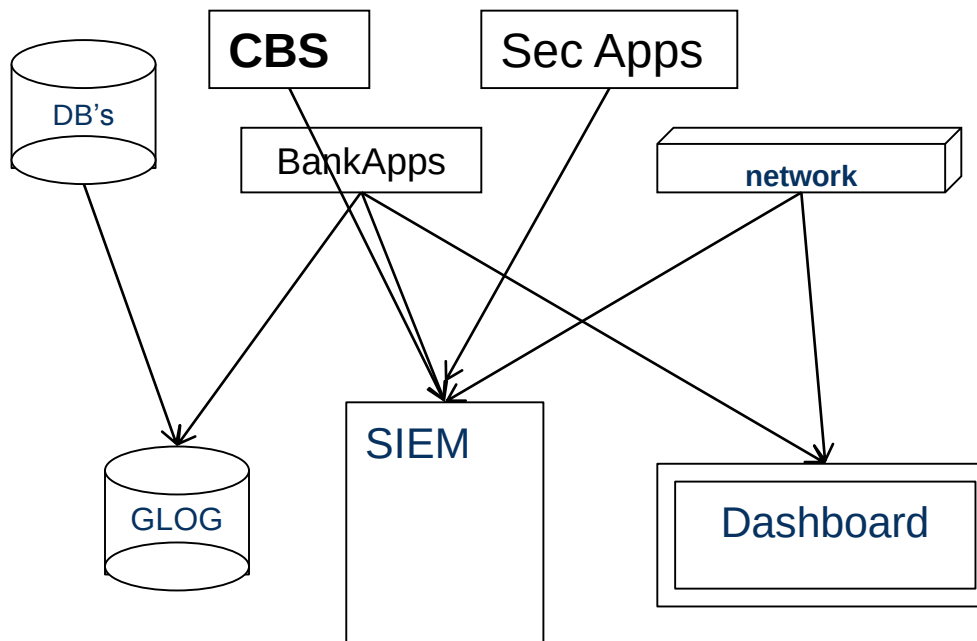
- Security monitoring (Security related)
 - Service desk (chyba v aplikáciach)
 - IT Administrators (chybná funkčnosť HW, SW, network)
 - Compliance and AntiFraud mngm t(podozrenia na fraud)
 - Business owners (chyba v procese, podozrenia na Fraud)
- Náčrt procesu:



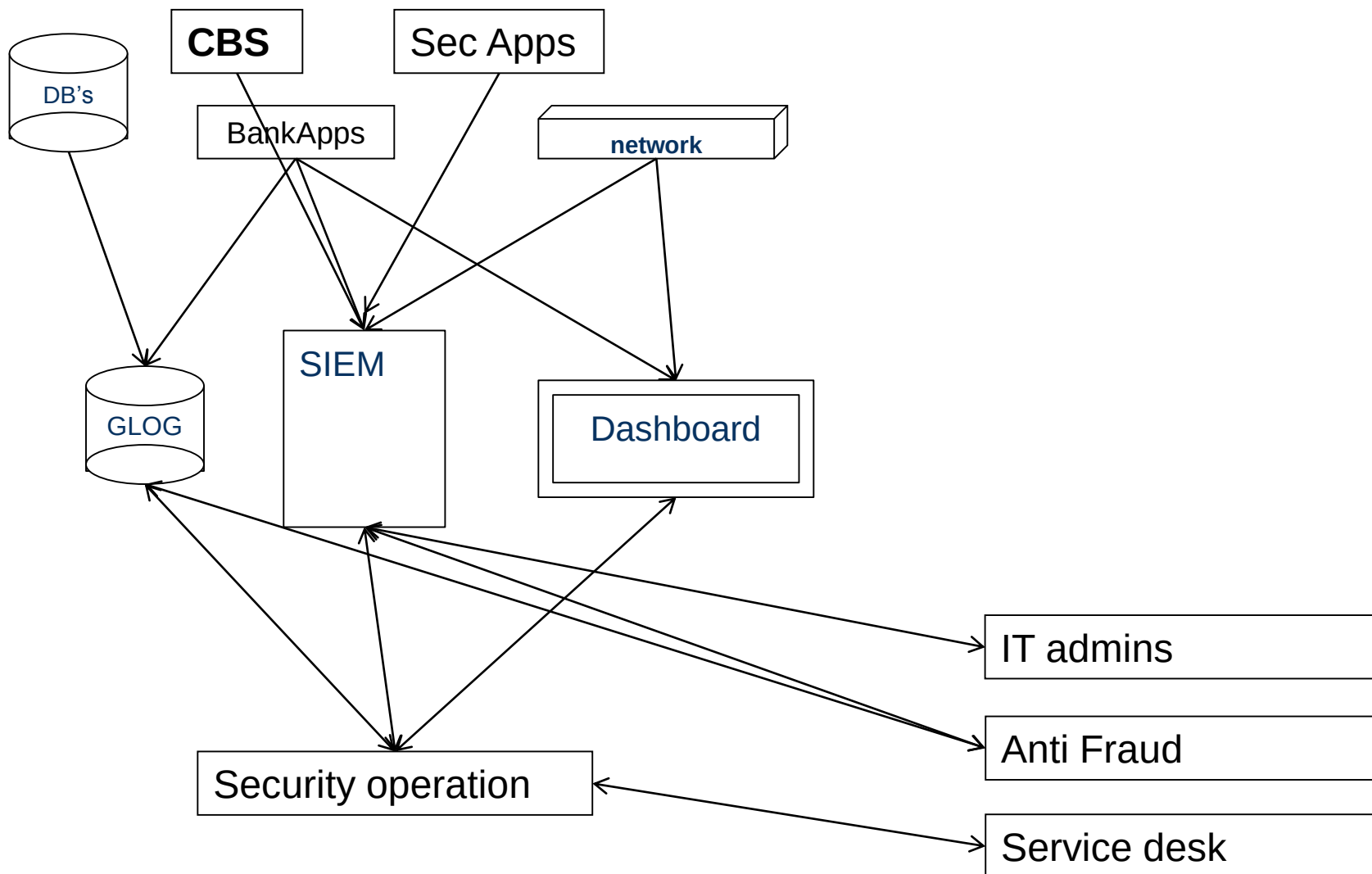
Otázky a odpovede pre proces Dashboardu.

- Nebolo by lepšie všetko dať na Service desk?
- Prečo čakáme na template incidentov a negenerujeme?
- Čo s dátami, keď sú ľudia doma, alebo 24x7?
- Nenasadzujte proces bez KPI.

Ako vypadá pracovní proces?



Ako vypadá pracovní proces?



Čo je užitočné?

- Need to know princíp.
- Vyskúšajte, ak si myslíte, že ste dostali dobrý nápad.
- Spolupráca, spolupráca, spolupráca....

Ďakujeme za pozornost

Logo partnera

