SECURITY 2012

20. ročník konference o bezpečnosti v ICT

SIEM a 6 let provozu

Od požadavků ČNB přes Disaster Recovery až k Log Managementu

Peter Jankovský, Karel Šimeček, David Doležal

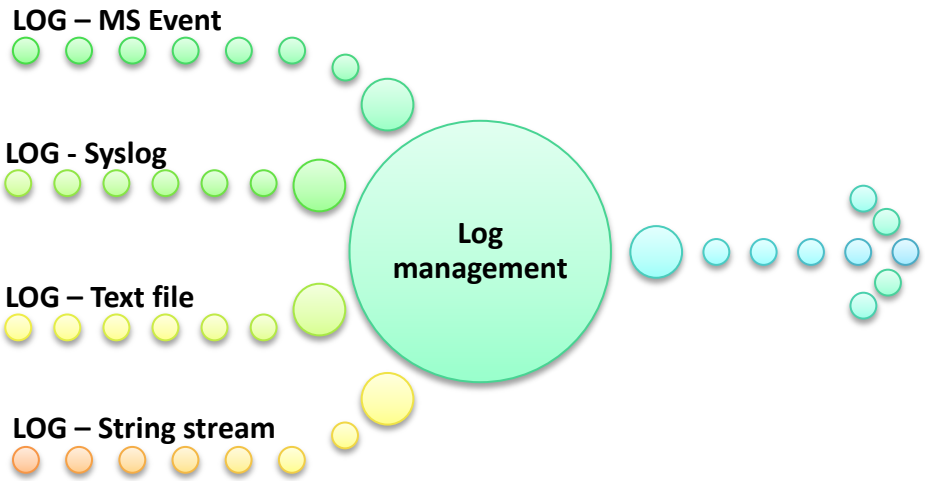
AXENTA, PPF banka

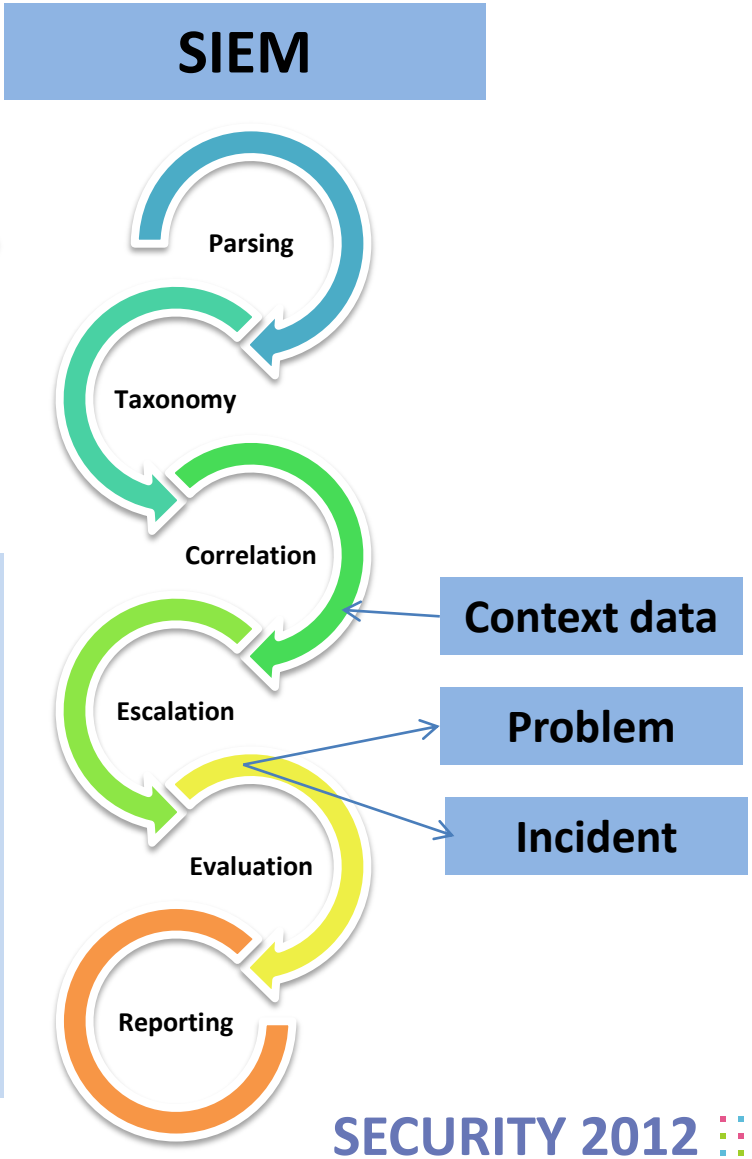
Agenda

- **Úvod**
  - SIEM a jeho provoz
- **Nasazení SIEMu**
  - 2006
- **Disaster Recovery & Log Management**
  - 2008/2009
- **Log Management II & Provozní monitoring**
  - 2011
- **Celkové náklady**

Úvod

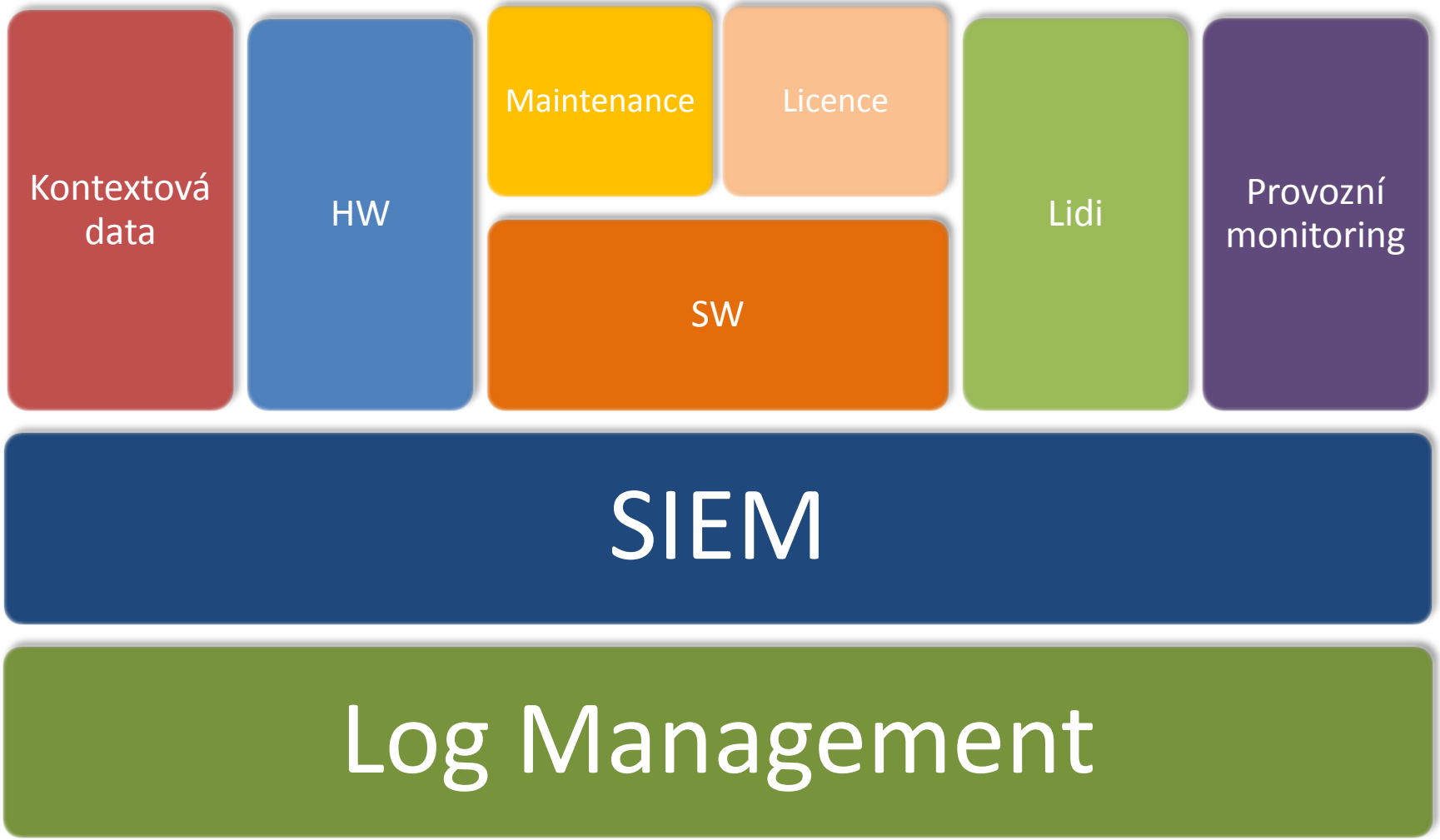
SIEM a řízení bezpečnosti





- **Základní problémy:**
  - Každá událost je identifikována **pouze IP adresou.**
  - Každá doplňující informace k této IP adrese **musí pocházet z důvěryhodného zdroje.**
  - **Neexistuje důvěryhodné propojení** mezi virtuálním a reálným světem, ve kterém je provozován informační systém.
  - Připojená zařízení mohou mít více síťových rozhraní než jednu.
- **Otázkou je:**
  - Jak rychle a správně identifikovat problém v informačním systému s jeho korektním přiřazením k příslušnému správci pro efektivní řešení?

SIEM a jeho provoz



Nasazení SIEMu

2006 – bezpečnosť v PPFB

Audit ČNB v roce 2005

- Zavedení IT Security
- Požadavky na monitoring dle ISO/IEC 27001 z pohledu ČNB

Řízení IT Security v PPFB

- Řídí, ale nevykonává
- Provozuje SIEM a Log Management

Požadavky na SIEM

- **Požadavky na SIEM**
  - funkce Log a Event Management
  - korelace bezpečnostních událostí
  - Monitoring change/config management
- **Kritéria pro výběr**
  - přístup dodavatele
  - uživatelsky konfigurovatelný produkt (3 lidé v BIS)
- **Vybráno**
  - Trustwave SIEM-OE
  - tým Petra Jankovského

SIEM - řešení

Přístup

- **Analýza** (1 měsíc)
- Implementace (vstupy, korelace, školení) (4 měsíce)
- Annual Care (1 rok)
- Servisní podpora (0MD pro rozvoj)

Produkt

- Trustwave SIEM-OE 5.2.1 (TCO)
- SIEM **vs** provozní monitoring **vs** Log management
- **80/15/5**
- Maintenance 15%
- Cena: **3,5M** Kč (produkt + maintenance + práce)

Zhodnocení SIEM

Výhody

- Přehled nad BIS a IT
- Funkce SIEMu jak pro BIS tak pro IT, ale i business
- Spokojené ČNB☺
- Metriky pro měření bezpečnosti

Nevýhody

- HW – 6GB RAM, 4x CORE
- SW – cena za licenci
- SIEM vs Log Management
- SIEM bez korelací „out of the box“ a alert managementu

Náklady

- Interní člověk na 60%
- 3,5M Kč za implementaci
- Požadavky na interní zdroje nejen BIS ale i IT
- HW - 2ks server po 100k

Disaster Recovery
&
Log Management

2008/2009 – Změny

Krize – redukce týmu

- Nákup externích sil
- Support + Enhancement (60k Kč měsíčně)

SIEM-OE 5.7.0

- More tunning, less configuration

Nulový rozpočet

Požadavky

- **SIEM vs Log Management**
  - Upgrade SIEM
  - Archivace 10let a opětovné zpracování
  - Jednoduchost, přehled, spolehlivost
  - Minimalizace výpadků sběru

- **Disaster Recovery**
  - BIA požadavek – 1h
  - DR vs High Availability

Analýza prostředí

Dvě lokality
Active/Active

SAN
mirroring

SIEM na dvou serverech
v jedné lokalitě

Windows
SNARE
agent

TXT
LogSender
agent

Log Management

- **Syslog-ng PE** (300k Kč - HA, 150 IP adres)
- **Archivace**
  - syslog-ng filtry
  - logrotate
  - gzip
- **Relay** – TCP, TLS
- **Licence** - agent pro win/linux a relay (cache)
- **Jedinný** agent pro sběr (txt, evt, multiline) logů

Disaster Recovery

- SIEM - **boot from SAN**
- **High Availability** syslog-ng PE relay

2x server pro DR SIEMu

(no HDD, 8xCORE, 16GB RAM) – 180k Kč

2x server pro RELAY

(RAID1, 4xCORE, 4GB RAM) – 50k Kč

SAN

LUN prostor – **400GB**

Upgrade SIEM

- **Verze 5.7.0**
  - Alert Management & notifikace
  - Korelace
- **Jedna instance/server**
  - management
  - možnost DR
  - záloha
- **Health Monitoring** – level 1

Zhodnocení

Výhody

- Nová verze + support smlouva: interně 5—10%
- Nezávislý log management
- **Licence**: DR != High Availability
- Syslog-ng Agent for Win – TCP, buffer, TXT

Nevýhody

- Bez supportní smlouvy nelze SIEM v 1 osobě rozvíjet
- Vyhledávání & linux knowledge (find, grep, cat, cut,…)
- Expirace/Archivace založená na skriptech
- DR výpadek vyžaduje manuální start druhé lokality
- provozní monitoring je součást SIEMu

Zhodnocení - náklady

Náklady

- 5-10% interního člověka
- **50 - 60k Kč** měsíčné support

- 15% - roční maintenance
- HW SIEM: 2x server po **90k Kč** (součást IT budgetu)
- SAN diskový prostor 400GB

- Syslog-ng PE v HA pro 150 adres: **300k Kč**
- HW RELAY: 2x server po **50k Kč**

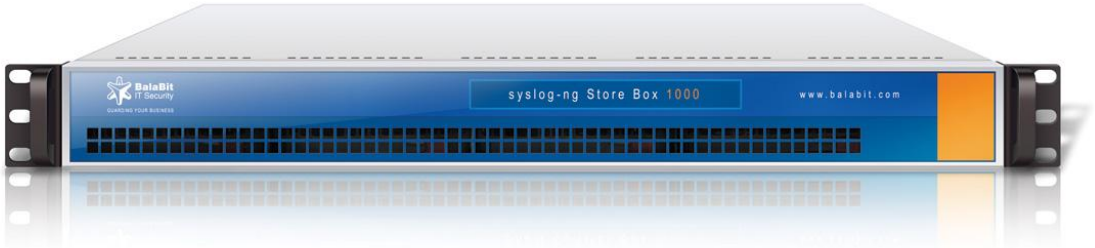
Log Management II
&
Provozní monitoring

Požadavky - 2011

- **Logy jak pro bezpečnost tak i IT**
  - Webové rozhraní
- **Archivace**
  - Automatická expirace bez skriptů
  - Šifrování logů
- **Indexace – rychlé vyhledávání**
  - Snadné nalezení problémové situace
  - Snadné DRILL-DOWN sledování anomálie
- **Nezávislý provozní monitoring**

Log Management II

- **Upgrade syslog-ng PE -> Syslog Storage Box (SSB)**
  - HW appliance (16x core, 24GB RAM, 1TB RAID1, redundant power)
  - Licence: 150 na 250 IP adress/sources
  - podpora AAA přes Radius/LDAP
- **RELAY -> SSB**



- Technologicky je *Log management* **úplně** nezávislý na SIEM

Provozní monitoring

HM služba SIEMu

SNMP pooling

skripty pro N/C

Emaily

SNMP pooling

SNMP trapy

Emaily

SIEM Health Monitoring – 2 úrovně

Monitoring SSB

Zhodnocení

Výhody

- Nezávislý log management / robustní HA/DR řešení
- N/C vs skripty
- Jednoduchost monitoringu přes SNMP (MIB)

Nevýhody

- Cena za appliance vs skripty?

Náklady

- Upgrade PE to SSB: 500k Kč (licence + appliance)
- Práce 250k Kč
- 100k Kč roční support na SSB **(NBD)**

Celkové Náklady

Náklady SIEM

SIEM implementace

- 3,5M Kč(maintenance + licence + práce)
- 6 měsíců implementační doba
- HW – 200k Kč

SIEM provoz

- Interně – 40% člověka +5% externě přes support
- Externě – 10% interního člověka + 50-60k Kč měsíčně (outsourcing)
- Maintenance – 15% ceny
- HW 1x za 4roky – 80 až 90k Kč jednorázová investice

Náklady Log Management

DR a Log Management implementace

- 1M Kč (licence + práce + maintenance/support)
- HW pro DR SIEMu – 90k Kč

Log Management provoz

- Interně – 2% člověka
- Externě – 5% (součást SIEM support)

Náklady za 6 let

SW+HW – 4,8M Kč

Maintenance/Support – 2,7M Kč

Práce

- Interně – 40% & 10%
- Externě – 1,8M Kč

SECURITY 2012

20. ročník konference o bezpečnosti v ICT

Děkujeme za pozornost.

Peter Jankovský
AXENTA
jankovsky@axenta.cz