SECURITY 2013

21. ročník konference o bezpečnosti v ICT

Log v kupce sena

Robert Šefr

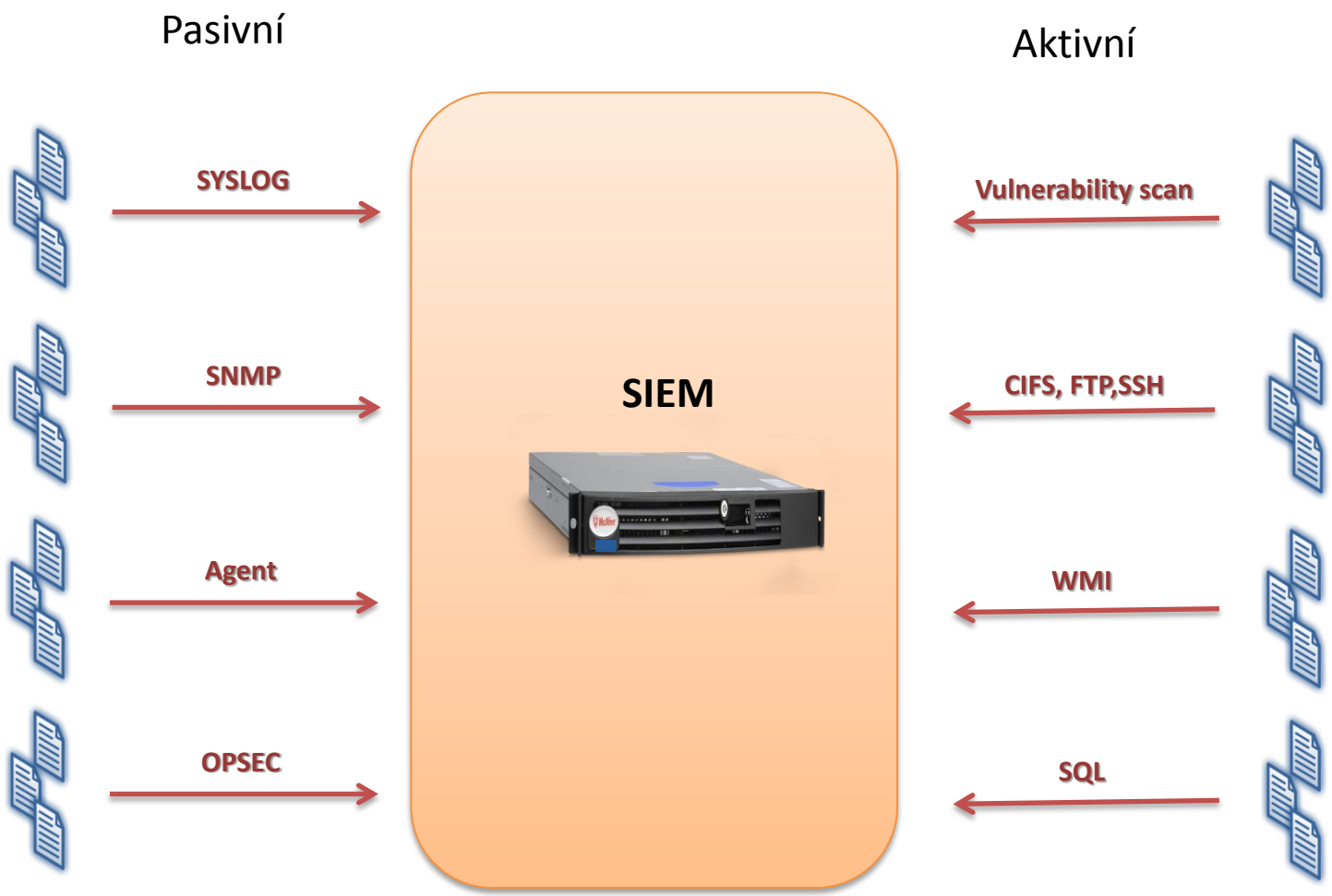
COMGUARD a.s.

SIEM není zbytečný luxus

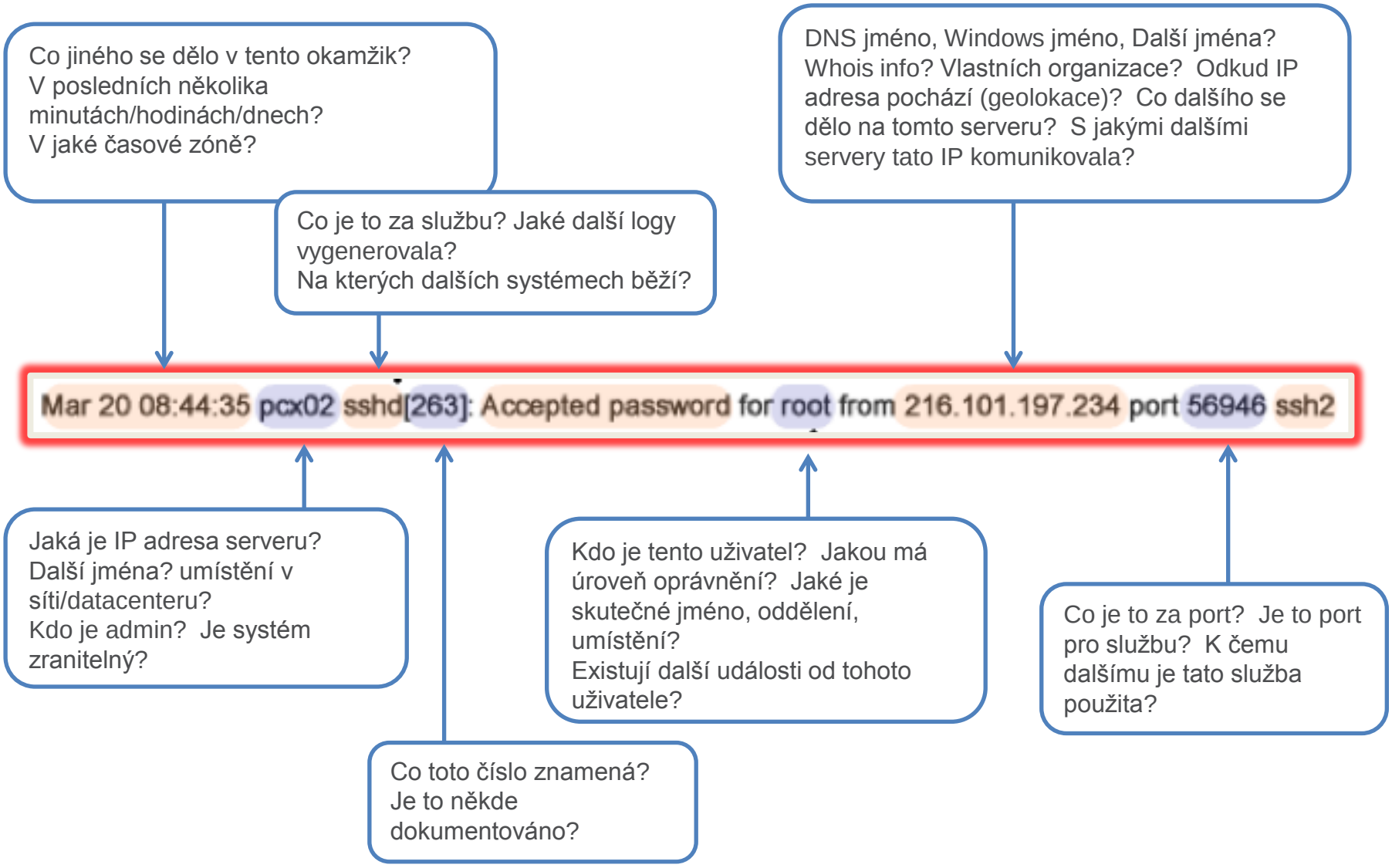
Najít jedno konkrétní stéblo …

… ve více různých kupkách

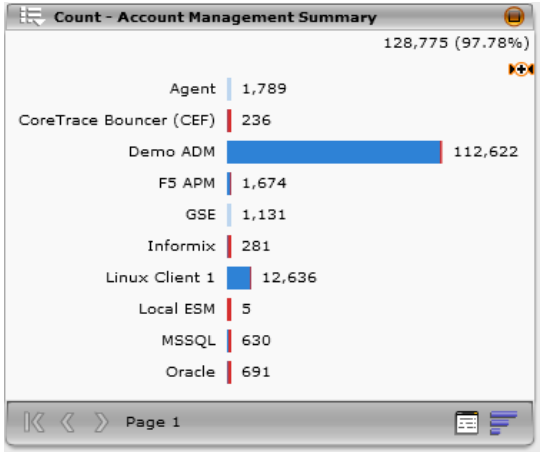
Sběr dat

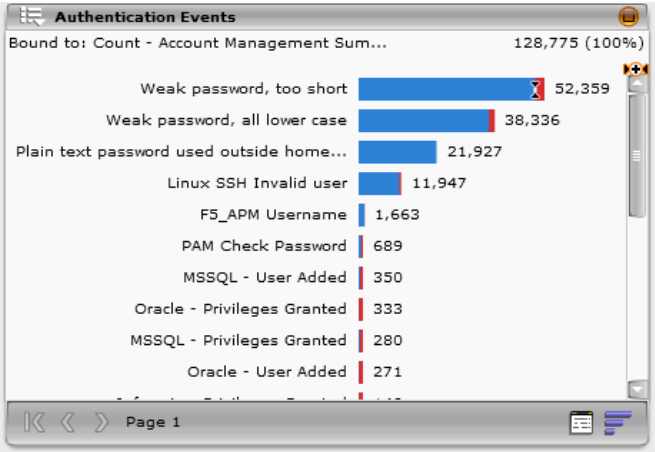

Pasivní
Aktivní
SYSLOG
SNMP
Agent
OPSEC
SIEM
Vulnerability scan
CIFS, FTP,SSH
WMI
SQL

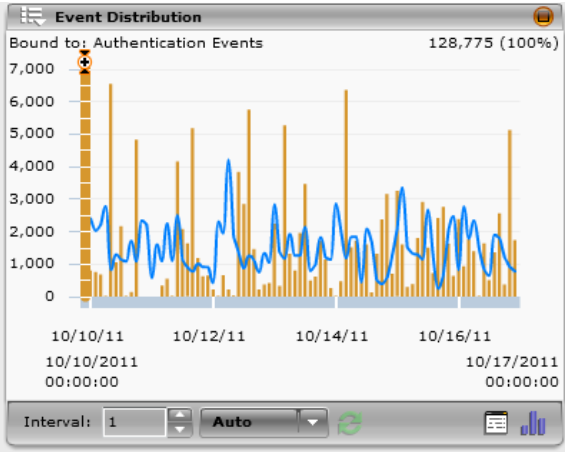
Zpracování logů



Interpretace







Events

Bound to: Event Distribution

Last Time	Source User	Rule Message	Application	Event Count	Severity	First Time	Device Name
10/16/2011 23:43:14	tkpuryea	Weak password, all lower case	Post Office Protocol v3 (POP3)	10	100	10/16/2011 22:46:40	Demo ADM
10/16/2011 23:43:11	rschwar2	Weak password, too short	Internet Mail Access Protocol (IMA	7	70	10/16/2011 22:13:08	Demo ADM
10/16/2011 23:42:29	asami	F5_APM Username	apd	36	900	10/16/2011 17:50:26	F5 APM
10/16/2011 23:42:06	mesmall	Weak password, too short	Post Office Protocol v3 (POP3)	8	80	10/16/2011 22:12:15	Demo ADM
10/16/2011 23:41:54	kebell	Weak password, too short	Post Office Protocol v3 (POP3)	8	80	10/16/2011 22:12:02	Demo ADM
10/16/2011 23:41:54	kebell	Weak password, all lower case	Post Office Protocol v3 (POP3)	8	80	10/16/2011 22:12:02	Demo ADM
10/16/2011 23:40:16		MSSQL - Privileges Granted	TSQL	1	80	10/16/2011 23:40:16	MSSQL
10/16/2011 23:40:16		MSSQL - Privileges Granted	TSQL	1	80	10/16/2011 23:40:16	MSSQL
10/16/2011 23:40:15		MSSQL - User Added	TSQL	1	80	10/16/2011 23:40:15	MSSQL
10/16/2011 23:40:15		MSSQL - User Added	TSQL	1	80	10/16/2011 23:40:15	MSSQL
10/16/2011 23:35:28	cjspeake	Weak password, too short	Post Office Protocol v3 (POP3)	32	320	10/16/2011 22:38:16	Demo ADM
10/16/2011 23:30:53	anonymous	Plain text password used outside home network	File Transfer Protocol (FTP)	2	20	10/16/2011 22:34:21	Demo ADM
10/16/2011 23:30:53	anonymous	Weak password, too short	File Transfer Protocol (FTP)	2	20	10/16/2011 22:34:21	Demo ADM
10/16/2011 23:27:43		MSSQL - Privileges Granted	TSQL	1	80	10/16/2011 23:27:43	MSSQL
10/16/2011 23:27:38		MSSQL - Privileges Granted	TSQL	1	80	10/16/2011 23:27:37	MSSQL
10/16/2011 23:27:36		MSSQL - User Added	TSQL	1	80	10/16/2011 23:27:36	MSSQL
10/16/2011 23:27:26	sdundis	Weak password, too short	Post Office Protocol v3 (POP3)	4	40	10/16/2011 22:30:55	Demo ADM

Page 1 — All events

Komu SIEM slouží?

- Různé logy jsou interpretovány jednotně a čitelně různým lidem na různých pozicích

- Bezpečnostní manažer
- IT oddělení
- Auditor
- Helpdesk
- Management

Ověřené řešení

- SIEM je již ustálená a vyspělá technologie
  - Stále se vyvíjí ale provozovatel není pokusný králík
    - Rozšiřuje se podpora zařízení
    - Zvyšuje se kvalita uživatelského rozhraní
  - Hmatatelné přínosy
    - Centralizovaný log management
    - Rychlost řešení incidentů
    - Nalezení dosud skrytých problémů
- Stále více společností poptává SIEM řešení

Výběr nejvhodnějšího řešení

Kupa SIEMů …

… a všechny jsou jedinečné ☺

Komplikované na výběr

- Nutná spolupráce s velkým množstvím zařízení
  - Různé typy logů
  - Různé způsoby doručení, technologie a protokoly
  - Logy proprietárních aplikací
- Různé výstupy
  - Velmi odlišná grafická rozhraní
  - Různé přístupy k interpretaci dat
- Nejednoznačné požadavky na implementaci
  - Velmi složité odhadnout časovou náročnost
  - A náročnost následné údržby?

Jak si vybrat?

1. Dát dohromady základní požadavky
   - Co má být cílem nasazení SIEMu?
   - Log management?
   - Jaké korelace?
   - Kolik pracovišť?
   - Jaké objemy logů? Jaká zařízení?
2. Vybrat několik prověřených řešení
3. Poptat dodavatele
4. Vybrat dvě až tři řešení a provést Proof of Concept

Průběh Proof of Concept

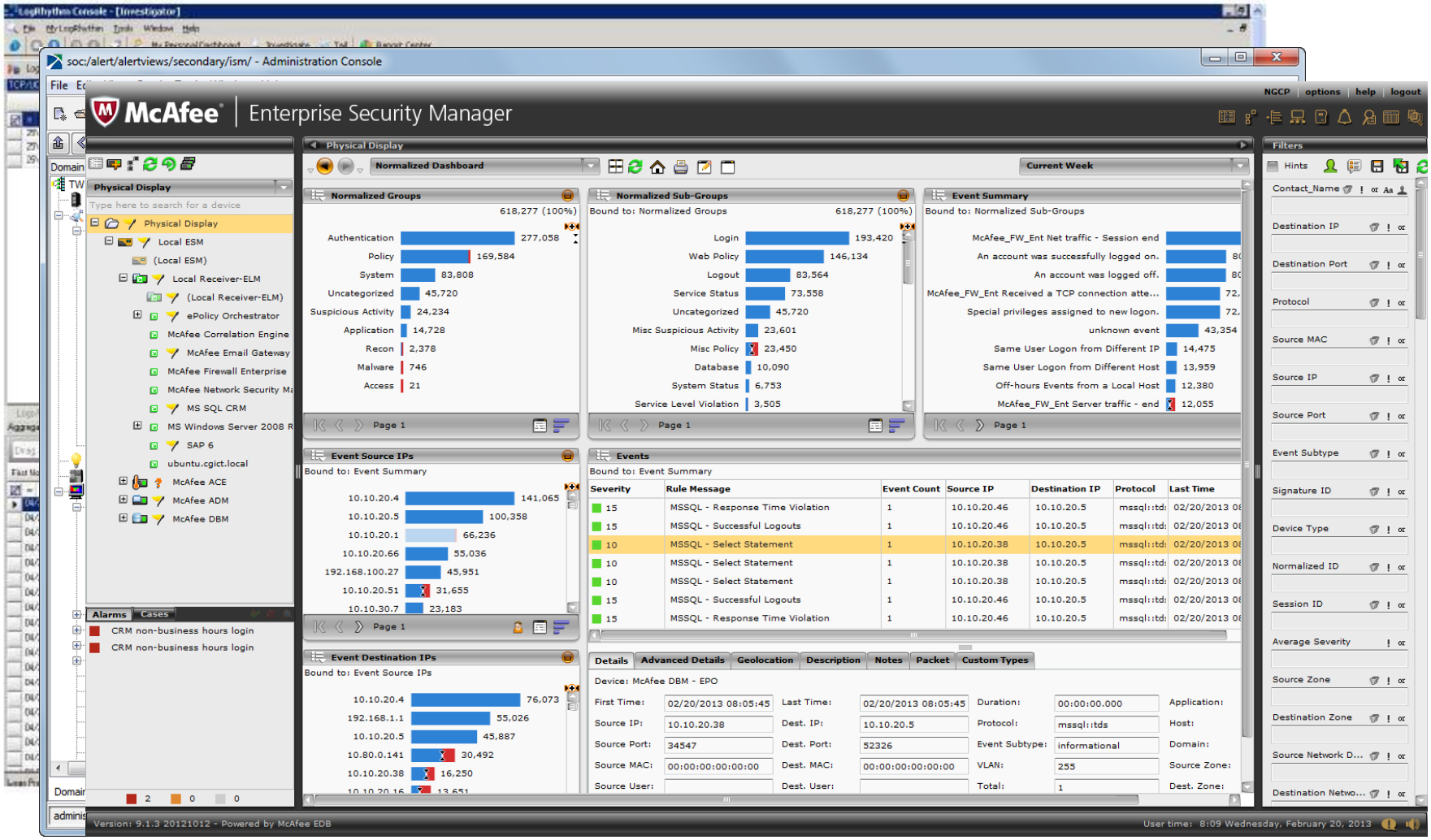
Kvalitně a jasně naplánovat

- Délka testování
- Rozsah testování
  - Jaká a kolik zařízení budou do PoC zapojena
- Součinnost
  - Která strana je odpovědná za jaké činnosti
  - Kolik času bude vyžadováno po administrátorech jakých řešení
- Jasně definované scénáře
  - Lze vyhodnotit vhodnost SIEMu
  - Zhodnocení dodavatele

Co ověřovat?

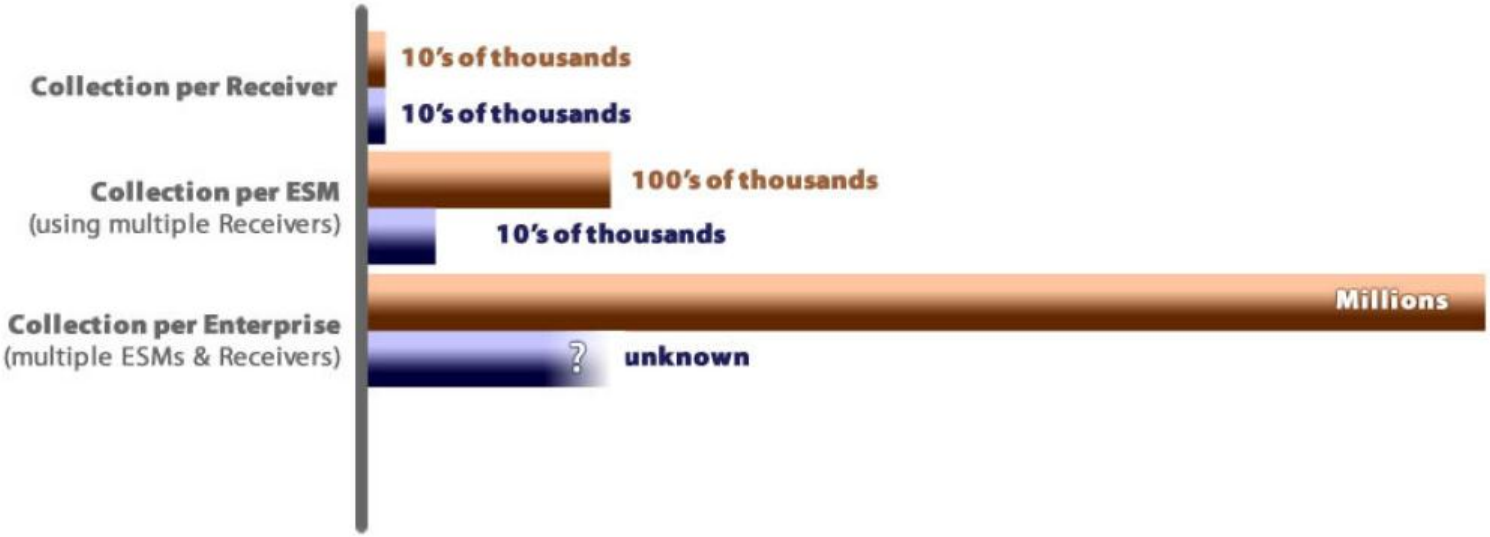
- Jednotlivé předem odsouhlasené scénáře
- Náročnost GUI na zaučení nových uživatelů
- Rychlost nasazení v rozsahu PoC - z té se dá usoudit rychlost kompletní implementace
- Rychlost a kvalita customizace
- Přístup a schopnosti integrátora
- Do jaké míry (jaké činnosti) jste schopni provozovat řešení vlastními silami a kdy již bude nutný zásah dodavatele?

Složitost a informační hodnota GUI



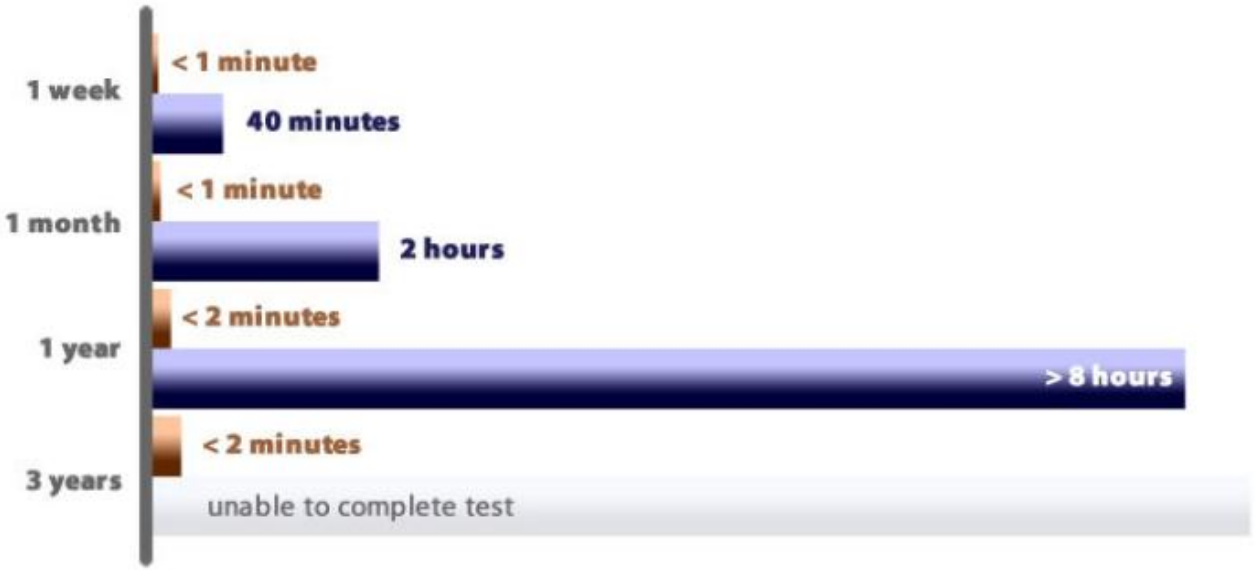
Výkon řešení - logy

- Sběr logů – lze porovnávat např. poměr cena/EPS



Výkon řešení - reporting

- Generování reportů nad velkým množstvím událostí nebo za delší období může být zdlouhavý proces



Ukázka možností

- Nový zdroj logů
- Vlastní dashboard
- Příprava korelace
- Drilldown

SECURITY 2013

21. ročník konference o bezpečnosti v ICT

Děkuji za pozornost.

Robert Šefr
COMGUARD a.s.
robert.sefr@comguard.cz