Sledování rozsáhlé počítačové infrastruktury

Pavel Tuček

EurOpen 2011

Proč sledovat infrastrukturu?

Proč by měl administrátor sledovat infrastrukturu?

Srovnání přístupů

- Bez přístupu
- Primitivní přístup
- Inteligentní přístup

Co když ani inteligentní přístup nestačí?

Řešení pro tisíce (událostí)

SEM, SIM a SIEM...

SEM – Oblast správy zabezpečení, která se zabývá sledováním infrastruktury, korelací událostí a možnostmi upozornění v reálném čase.

SIM – Oblast správy zabezpečení, která se zabývá dlouhodobým ukládáním událostí, jejich analýzou a hlášením případných problémů.

SIEM – Oblast správy zabezpečení, která v sobě spojuje prvky SEM a SIM, tzn. zajišťuje sběr bezpečnostních logů generovaných hardwarovou a softwarovou částí infrastruktury a jejich uložení do databáze. Dále zajišťuje analýzu a prezentaci těchto dat, mimo jiné pro přehled o plnění kvality služeb.

Řešení pro tisíce (událostí)

Komponenty řešení SIEM

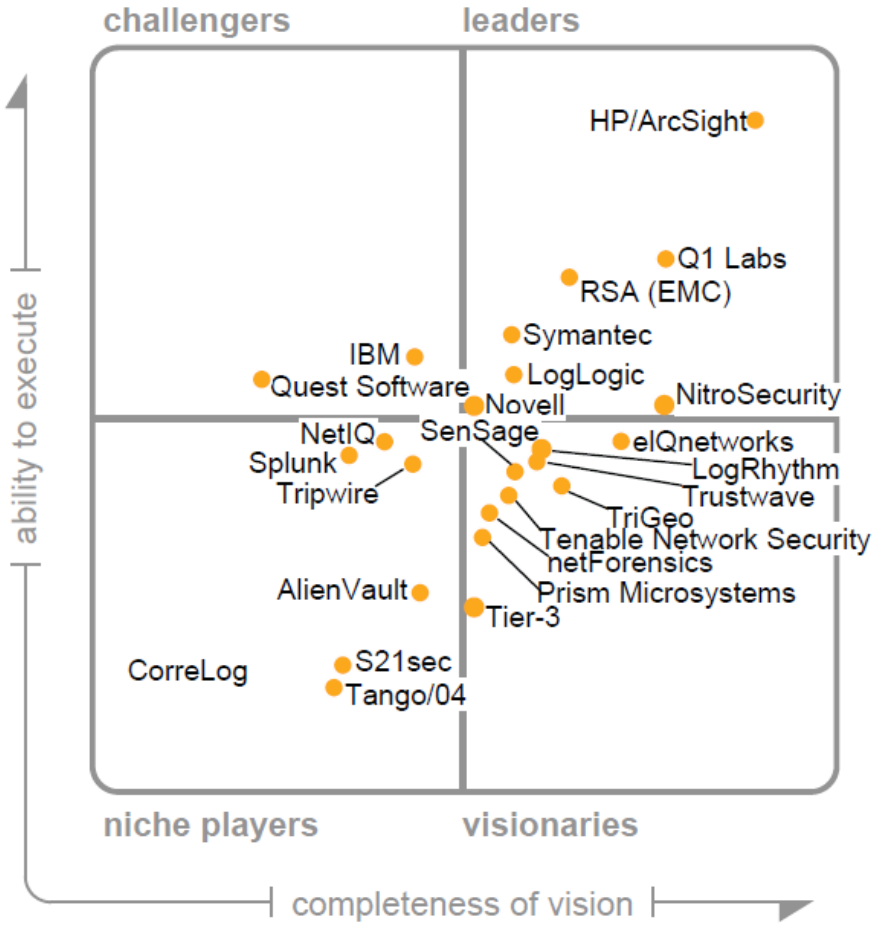
1. Agregace dat
2. Korelace událostí
3. Varování
4. Přehledové sestavy

Řešení pro tisíce (událostí)

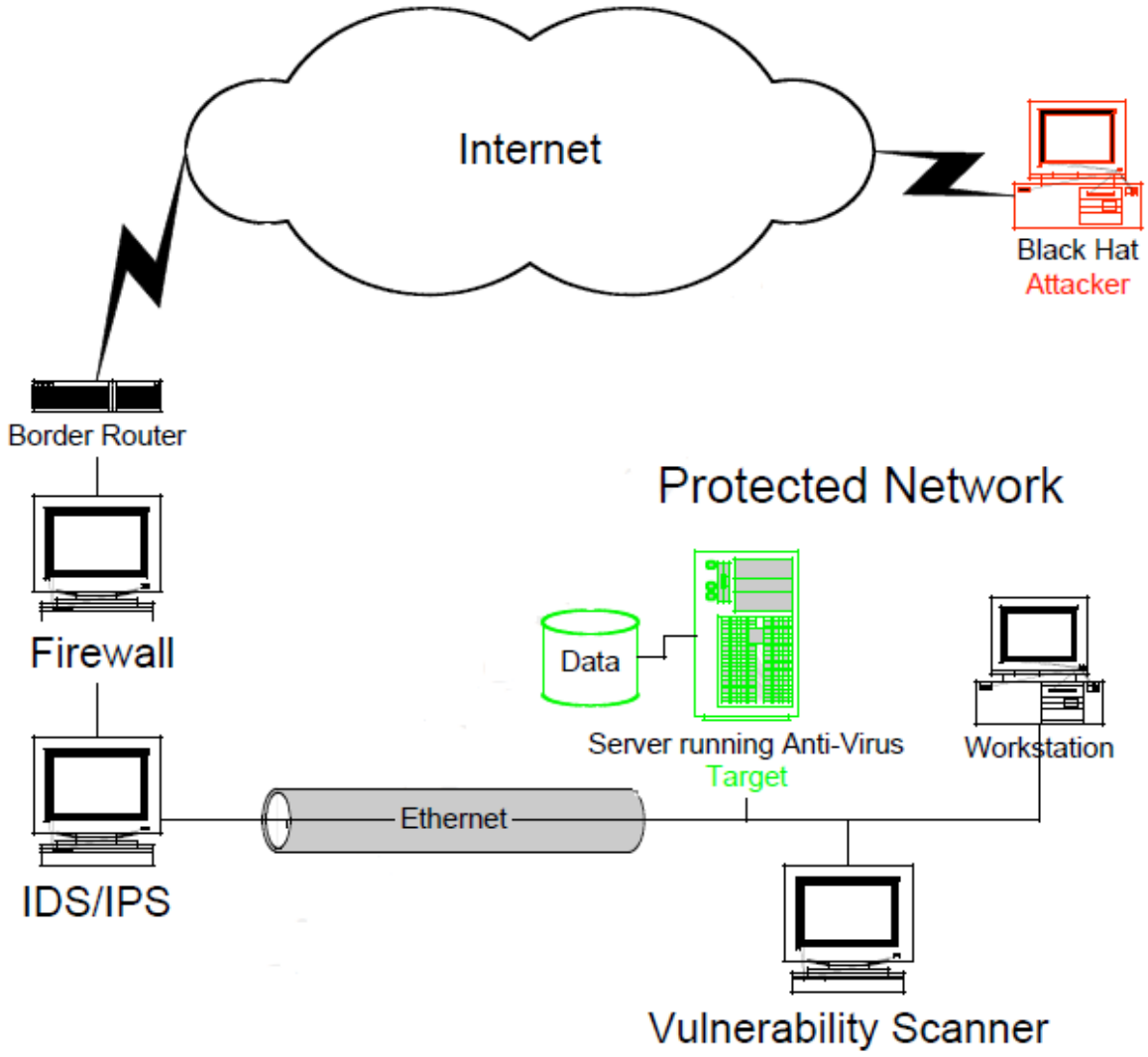
Cíle SIEM

1. Rychlejší reakce na útoky
2. Větší úspěšnost detekce útoků
3. Vyšší efektivita správy infrastruktury
4. Automatické vytváření statistik dostupnosti infrastruktury

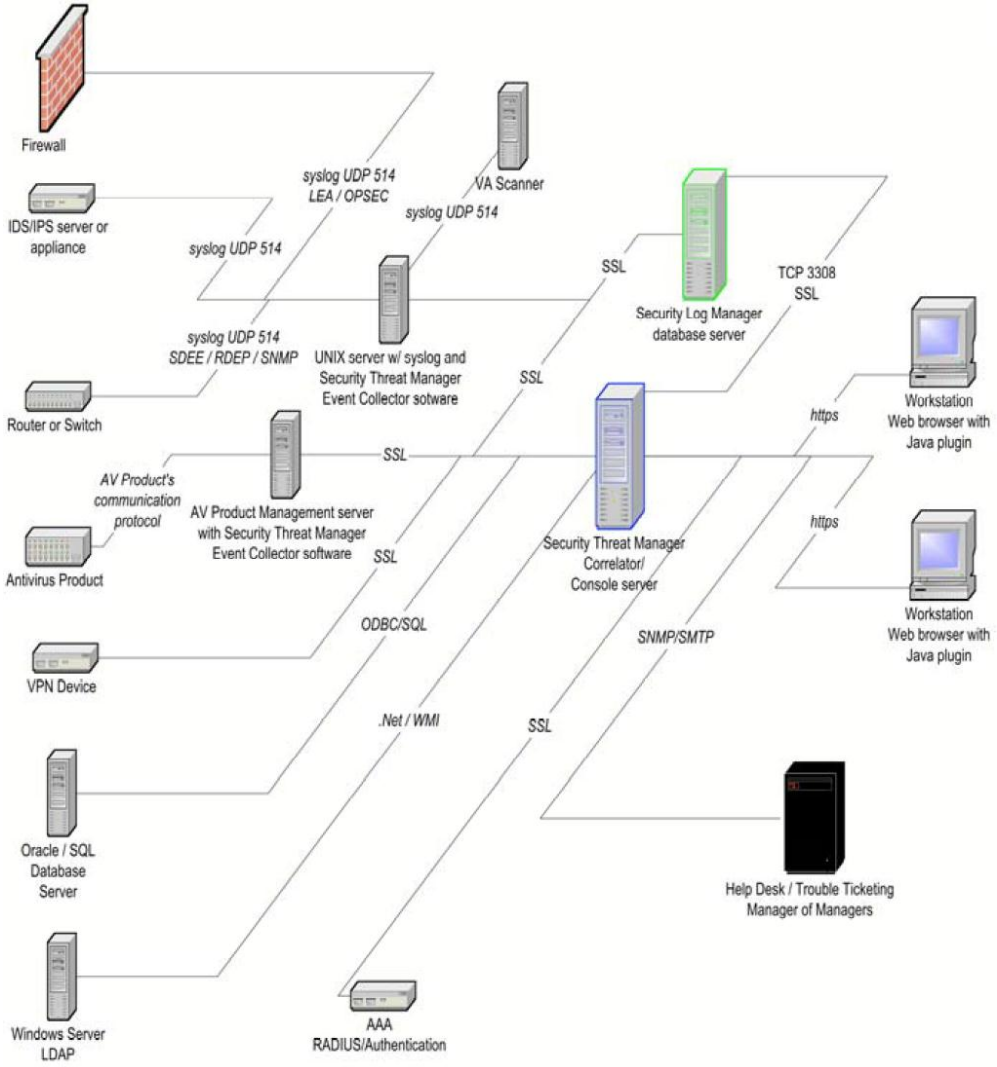
„Magické kvadranty“ dle Gartner



Útok na infrastrukturu bez SIEM



Útok na infrastrukturu se SIEM

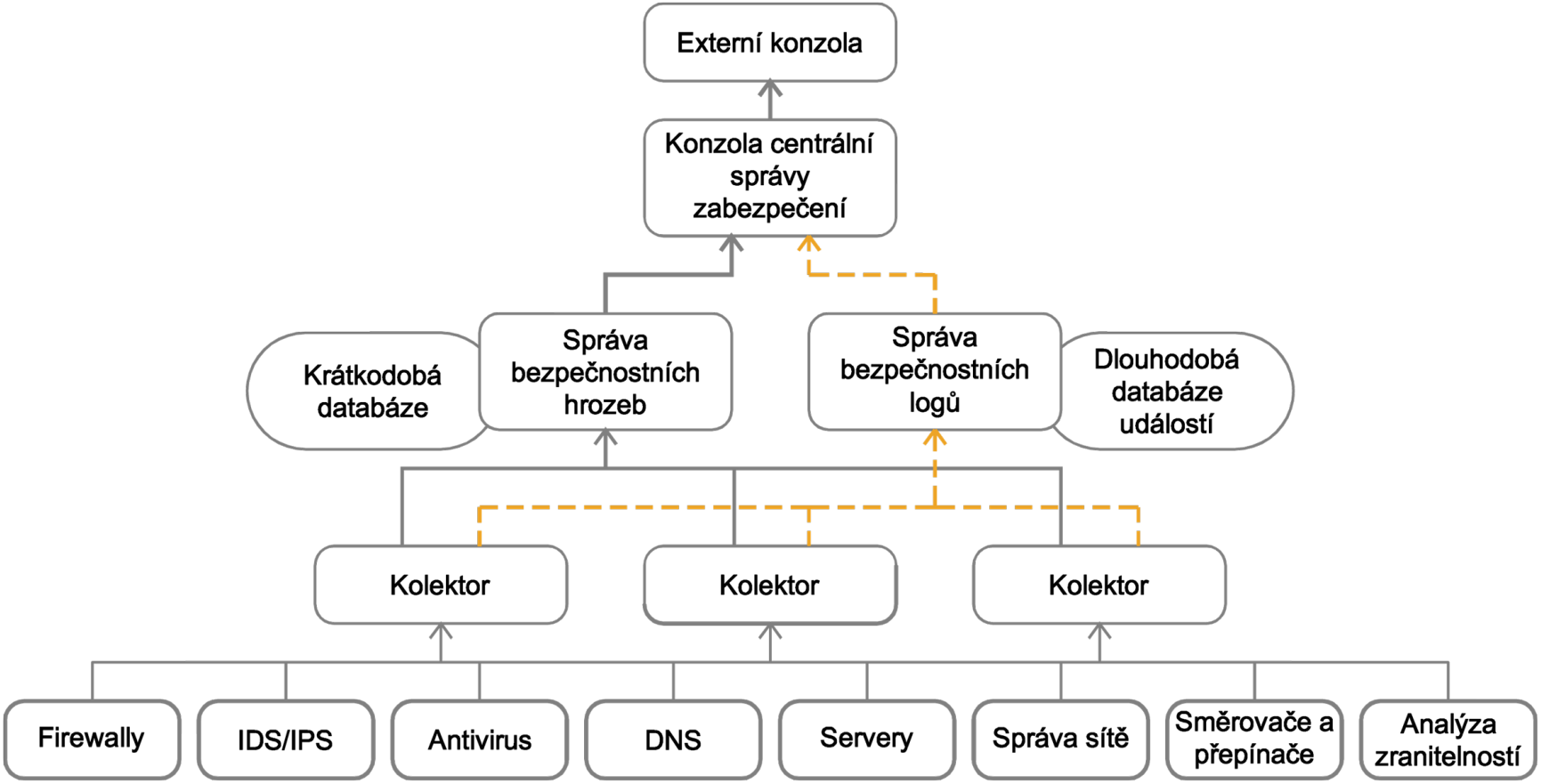


Motivace pro vývoj vlastního řešení

Kritické faktory

- Cena řešení
- Problematika nasazení a konfigurace
- Podpora
- Výkon a přenos
- Mnoho zajímavých otázek

Architektura

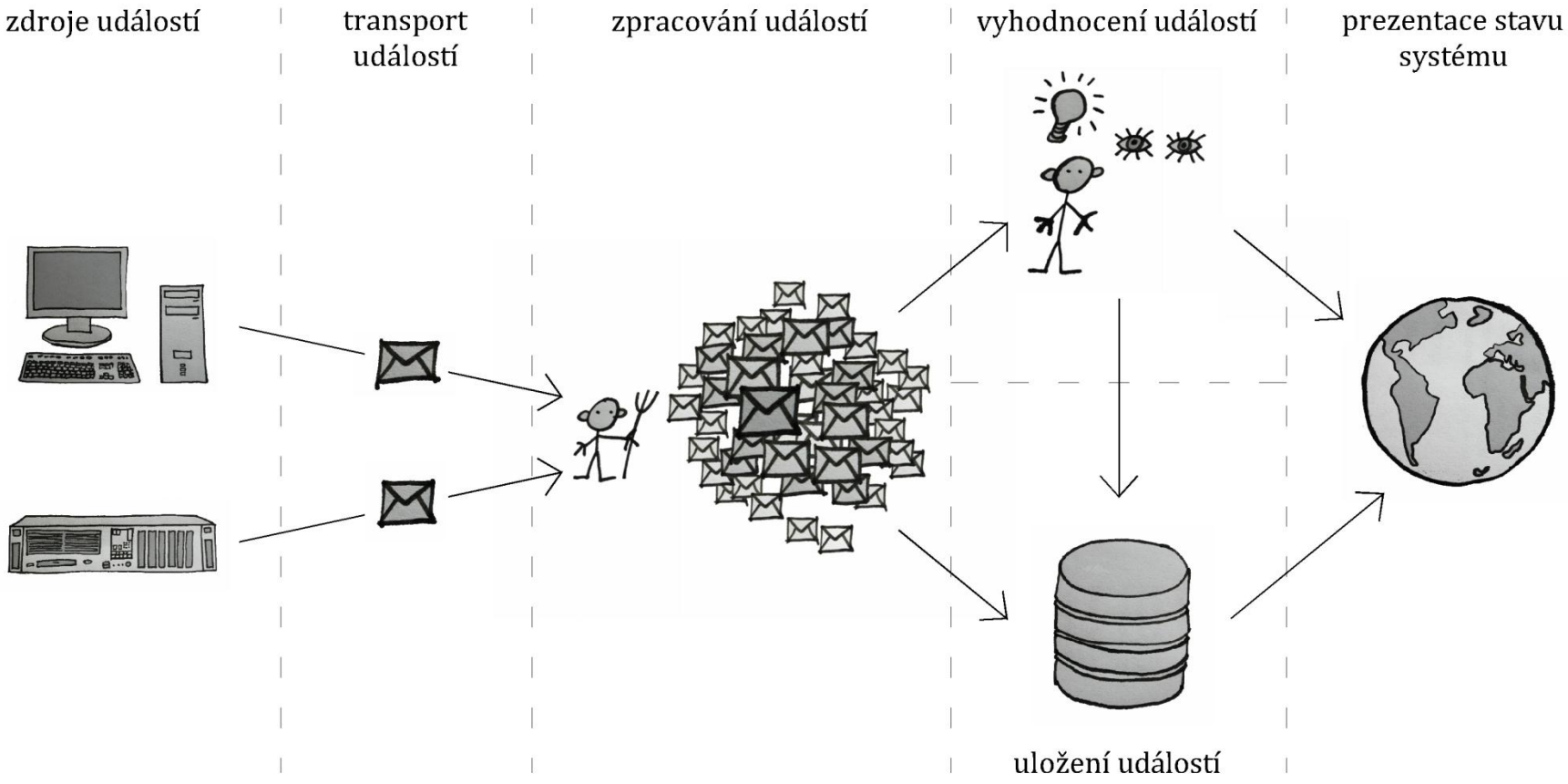


Sledování Microsoft AD infrastruktury

Doména UCN (University Computer Network)

- Více než 1200 počítačů
- Cca 60 serverů
- Cca 50000 uživatelských účtů

Sledování Microsoft AD infrastruktury



Sledování Microsoft AD infrastruktury

WinMon

- Stav antivirového řešení
- Stav lokálního firewallu
- Stav síťových připojení
- Windows updates
- Lokální uživatelé a skupiny
- Základní parametry OS
- Sledování logů OS
- Filtrování logů pomocí „whitelistu“ a „blacklistu“

Sledování Microsoft AD infrastruktury

Namtar

- WinLogonEventTrace, WLETDispatcher & WLETSpooler
- WLETDispatcher odesílá zprávy
- WLETSpooler přijímá zprávy
- Windows Secured RPC
- Omezeno na přenos XML v kódování UTF-16 LE
- WLETCatcher – System Event Notification Service

CloverETL

Databáze

Další vývoj

1. Rozšíření služby WinMon
2. Nový transportní systém
3. Sledování linuxových operačních systémů - LinMon
4. Sledování síťových prvků (Cisco, HP, 3COM,...)
5. Sledování zabezpečovacích systémů, které OVSS ÚVT MU vyvíjí
6. Sledování zálohování stanic a serverů
7. Sledování autentizačních bran využívajících doménu UCN (Radius, Shibboleth a jiné)

Resumé

- Vhodnost/nutnost sledování infrastruktury.
- SIEM.
- Řešení vyvíjené na MU.

Poděkování

- Vašku Lorencovi
- Víťovi Bukačovi a Andrey Číkové
- Vashkovi Matyášovi

Konec

Děkuji za pozornost.

Dotazy?