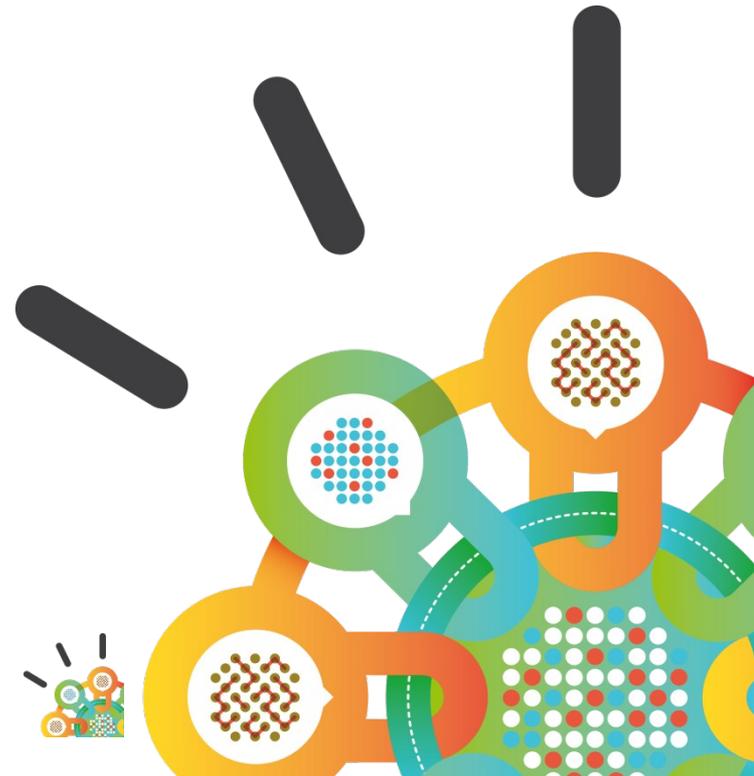


Security Intelligence.
Think Integrated.

IBM Security Intelligence

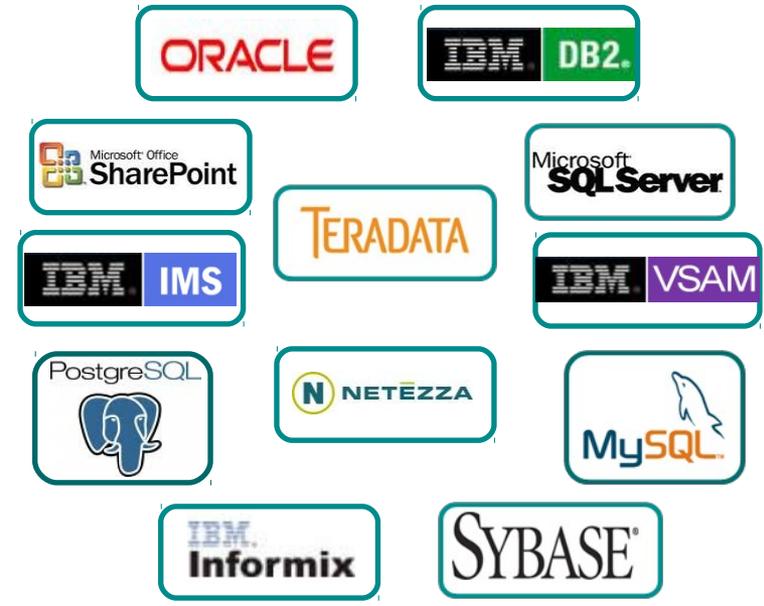
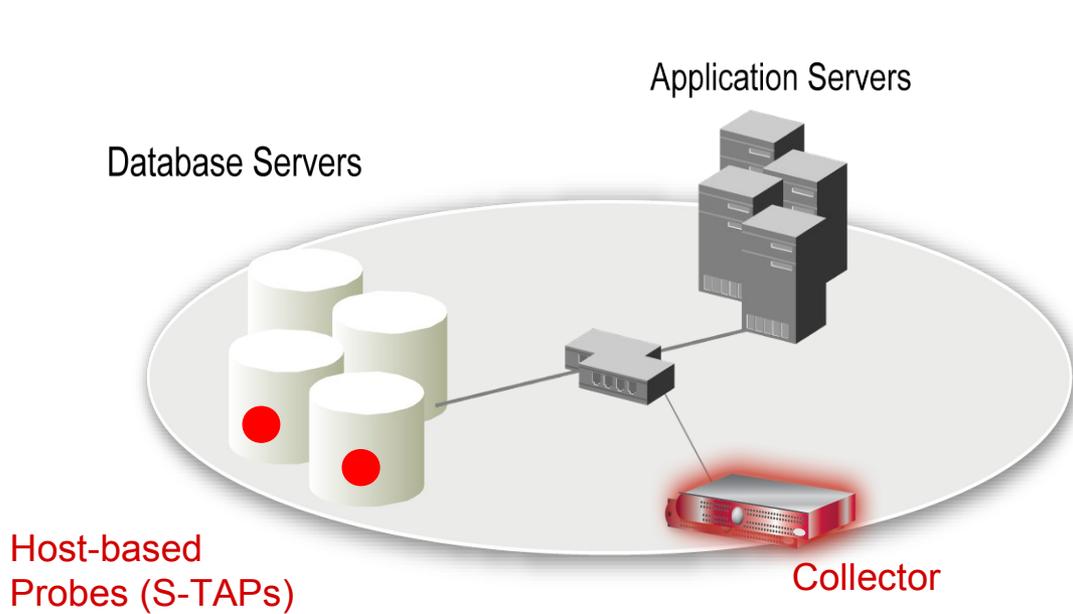
January 2013



Kas ir risku vadība?

Risinājums 1. - Insider attacks

Reāla-laika datu bāzes monitorings un aizsardzība ar IBM Guardium



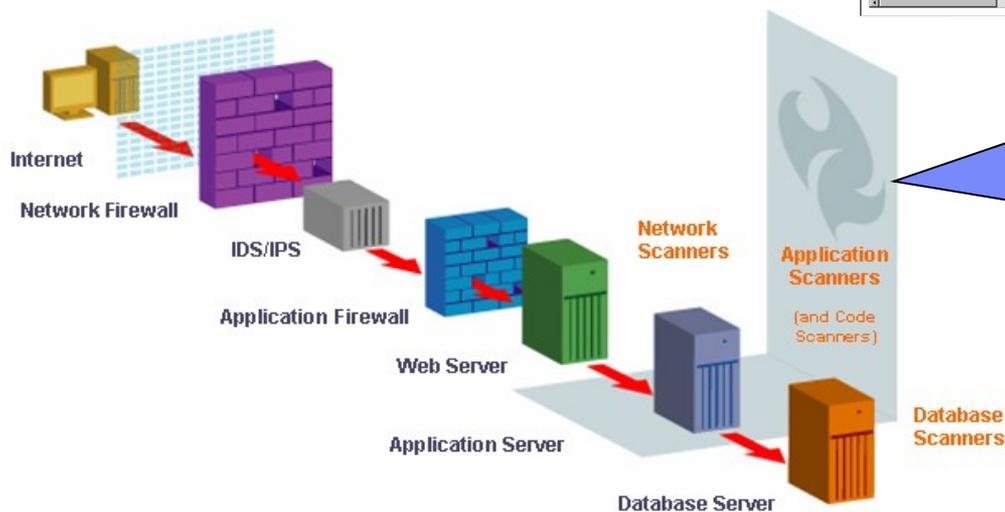
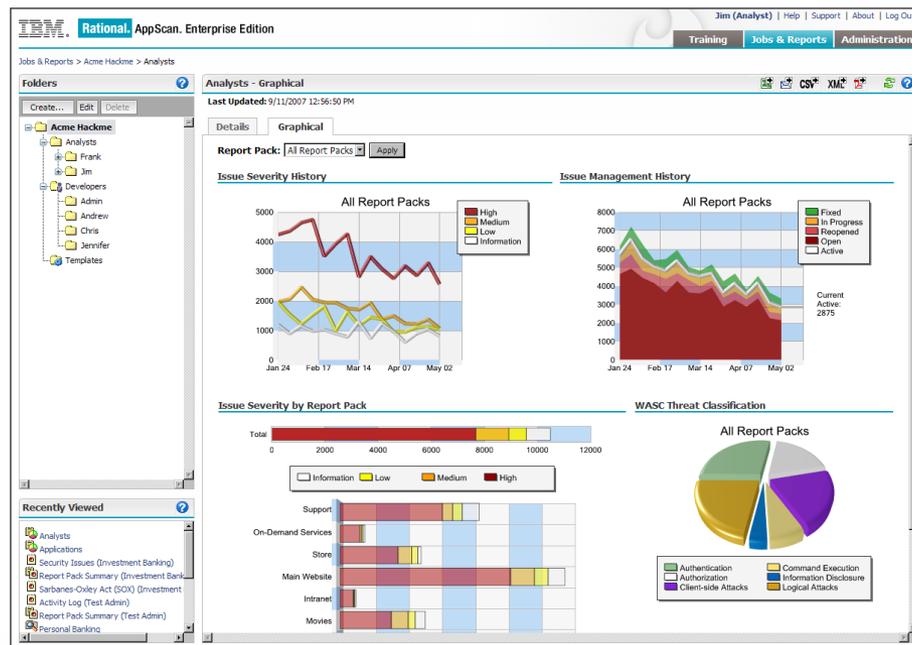
- Nav nepieciešamas DBMS izmaiņas
- Neizmanto DBMS izveidotos logus kurus var viegli izdzēst uzbrucējs vai negodīgs darbinieks
- 100% redzamība ietverot arī tiešu DBA servera piekļuvi
- Minimāla ietekme uz veiktspēju

- Cross-DBMS risinājums
- Detalizētas, reāla-laika politikas & auditēšana
 - Kurš, ko, kad, kā
- Automatizētas atbilstības atskaites un eskalācijas

Risinājums 2. - Application security

Rational Appscan

- Aplikāciju ievainojamību automātisks meklētājs
- Atklātās ievainojamības apraksts un risinājums kā to izlabot
- Plašas skenēšanas iespējas iekļauj arī sarežģītas Web 2.0 tehnoloģijas
- Ērti izmantojams gan testētājiem, gan aplikāciju izstrādātājiem



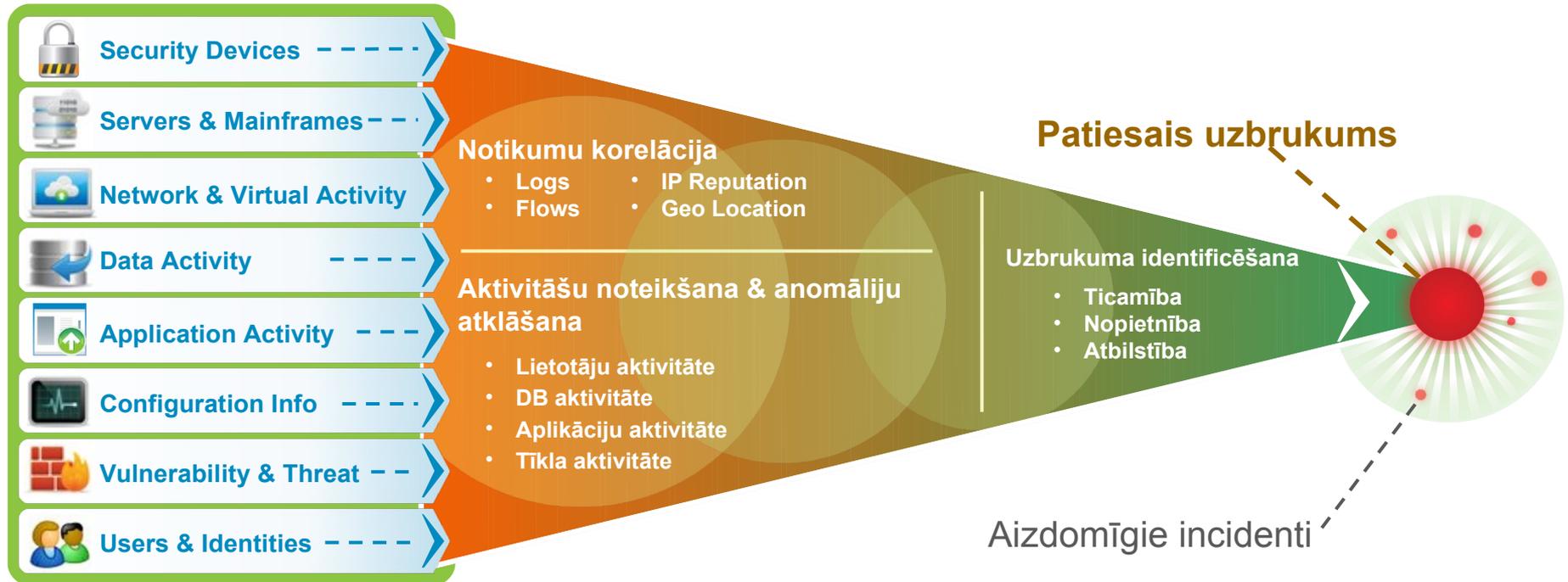
53 Security Issues (368 variants) for 'My Application'

- Blind SQL Injection (4)
 - http://demo.testfire.net/bank/account.aspx (1)
 - http://demo.testfire.net/bank/login.aspx (2)
 - http://demo.testfire.net/bank/transaction.aspx (1)
- Cross-Site Scripting (5)
- Format String Remote Command Execution (1)
- HTTP Response Splitting (1)
- SQL Injection (6)
- XPath Injection (1)
- Cookie Poisoning SQL Injection (1)



Risinājums 3. - Security Information and Event Management

QLabs – Konteksts un korelācija sniedz dziļāko ieskatu



Apjomīgi datu avoti + Padziļināta izmeklēšana = Ārkārtīgi precīzs un pielietojams ieskats

Pilnībā integrēta drošības izmeklēšana

Log Management

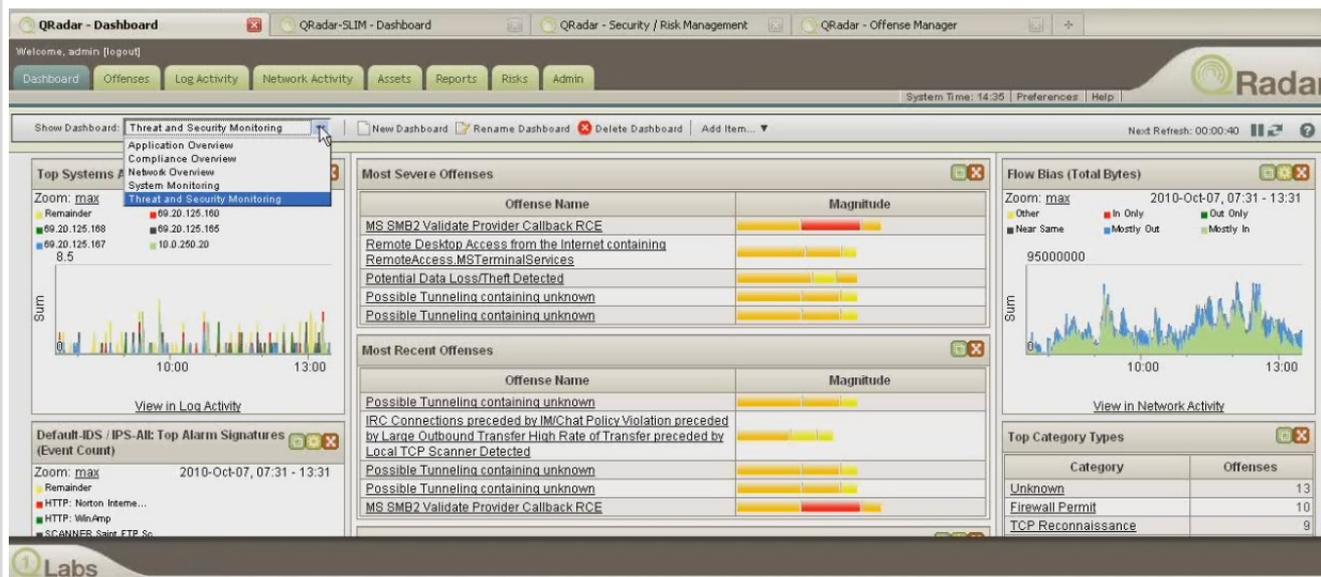
SIEM

Configuration & Vulnerability Management

Network Activity & Anomaly Detection

Network and Application Visibility

Viena drošības konsole



Izbūvēta uz vienotas datu arhitektūras

Jautājumi?

Edijs Tanons

tanons@lv.ibm.com

+371 2-919-7-313