Deloitte.

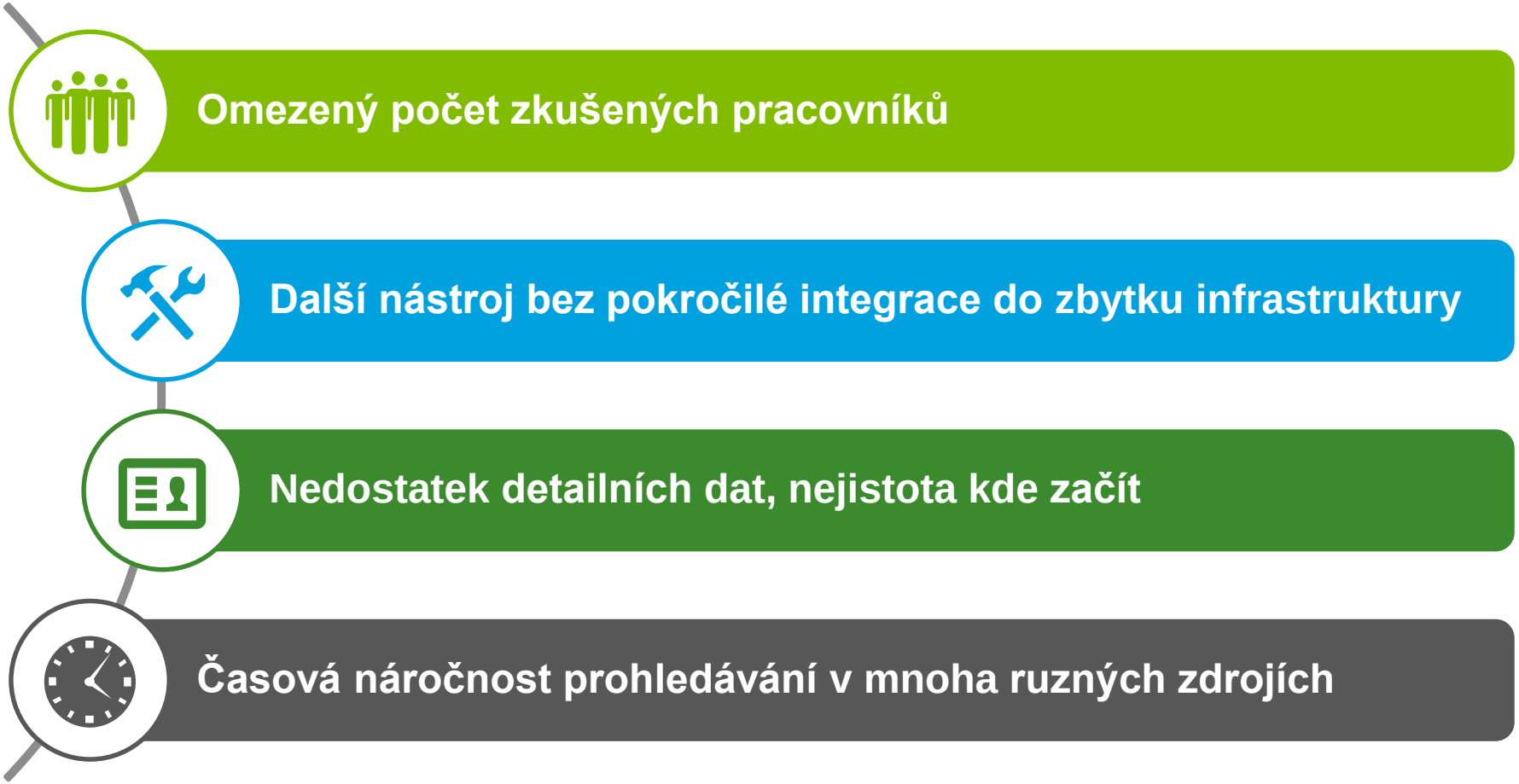
Forenzní analýza jako doplněk SIEMu

Jiří Slabý

31.3.2015

Policejní akademie ČR, Praha

Běžné problémy při zavádění forenzní analýzy



Nová generace forenzních nástrojů

Integrované do nástroje SIEM

Upozorní na incident

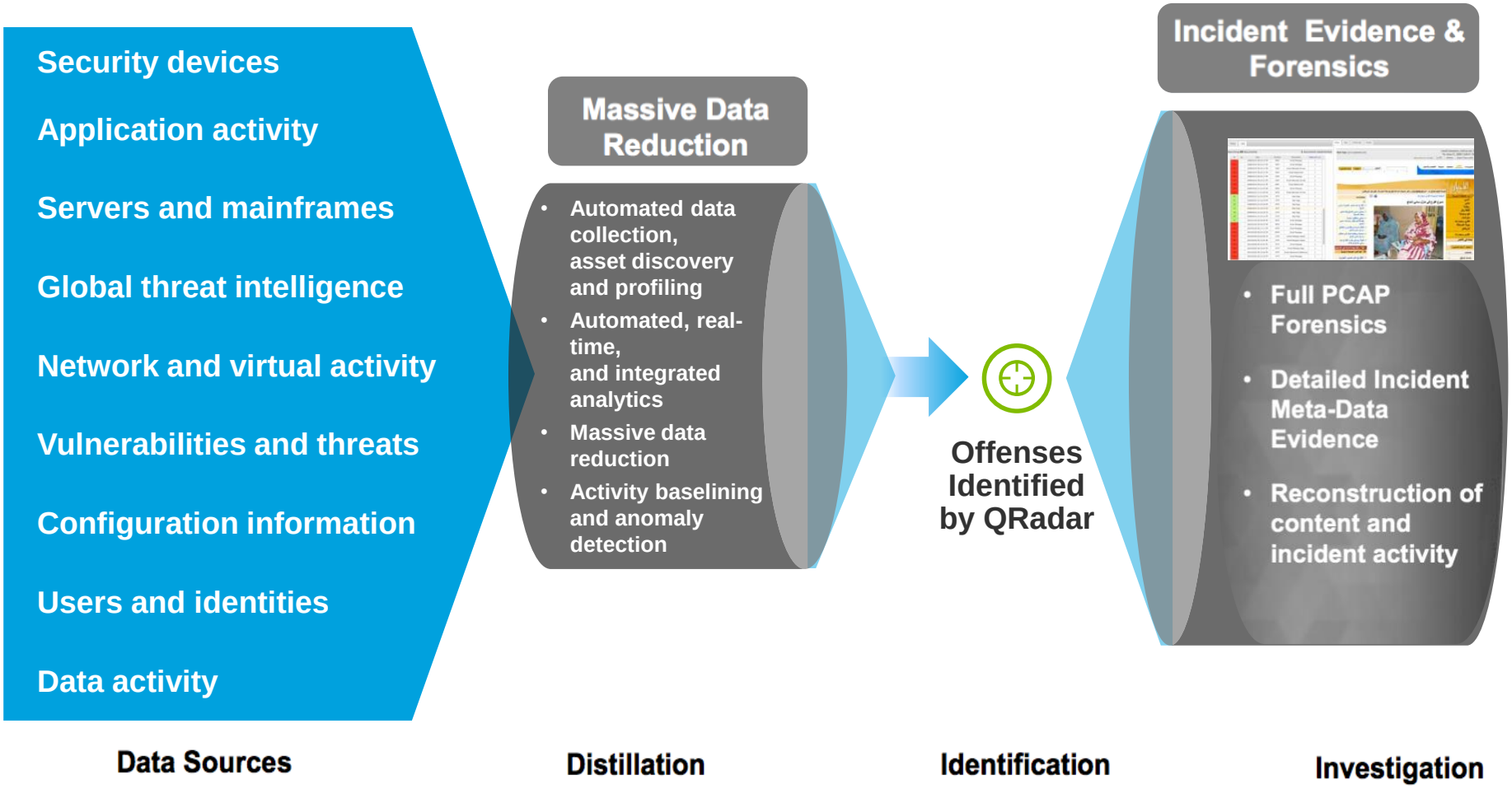
- Integrovaný s Qradar SIEM
- Využívá interní search technologii nad metadaty
- Během vteřin zobrazuje výsledky

Umožní se podívat do historie

- Plný PCAP pro detailní historii
- Taxonomizace
- Chronologické zobrazení událostí

Poskytne kontext k datům

- Možnost vizuálních výstupů, zobrazujících vztahy a entity
- Spojování entit dle atributů

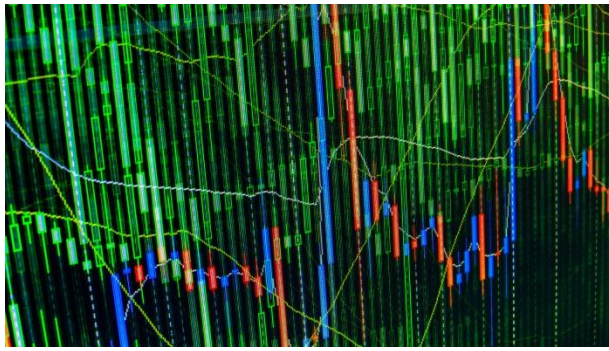


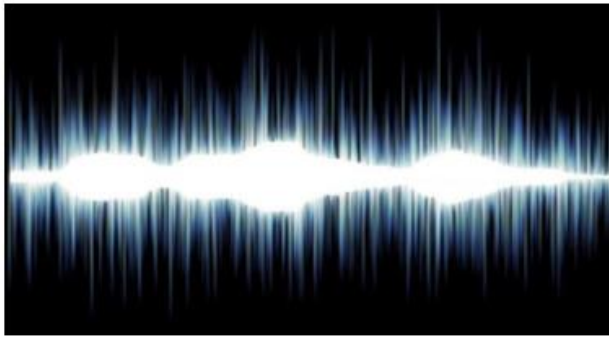
Typické použití forenzní analýzy

Network security	Identifikujte podezřelé transakce
Insider analýza	Identifikujte podvodníky a dotčené systémy
Detekce fraudu	Odhalte komplikovaný podvod
Shromáždění důkazů	Zkompletujte evidenci o činnosti malware

Jeden systém pro validní výstupy

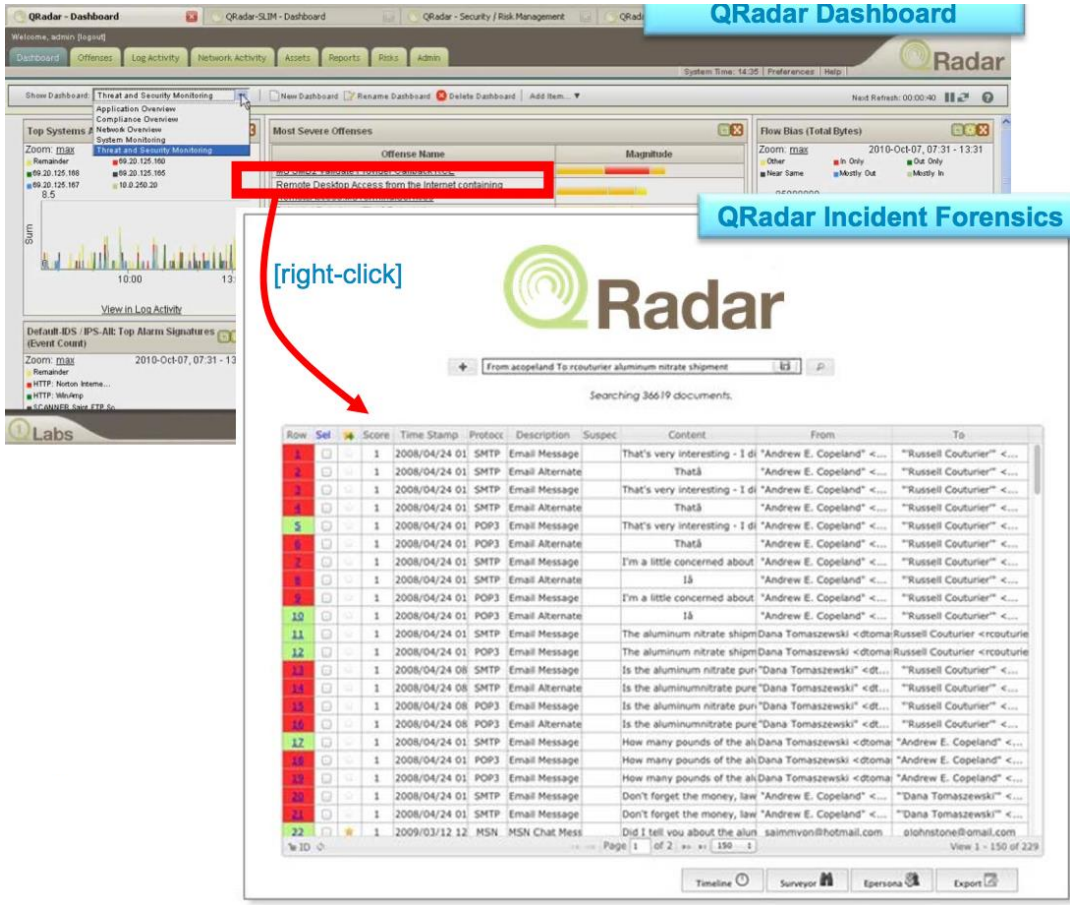
- Poskytuje vyhledávání nad indexovaným, taxonomickým úložištěm:
  - Síťová data
  - Soubory
  - Identity
- Zpracovává a convertuje:
  - PCAP
  - XML
  - Dokumenty (běžné formáty)
  - Archivy
- Navrací detailní výsledky v krátkém čase





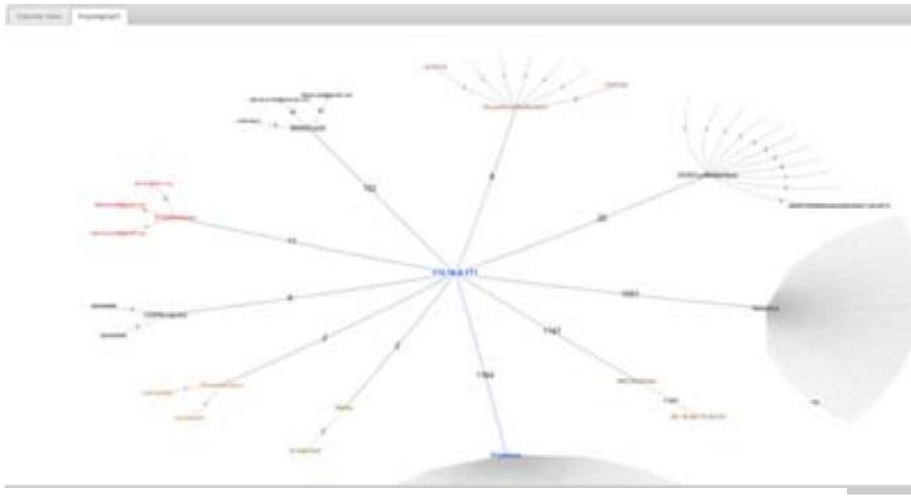
Jako parametr daného incidentu nebo ad-hoc dotazy

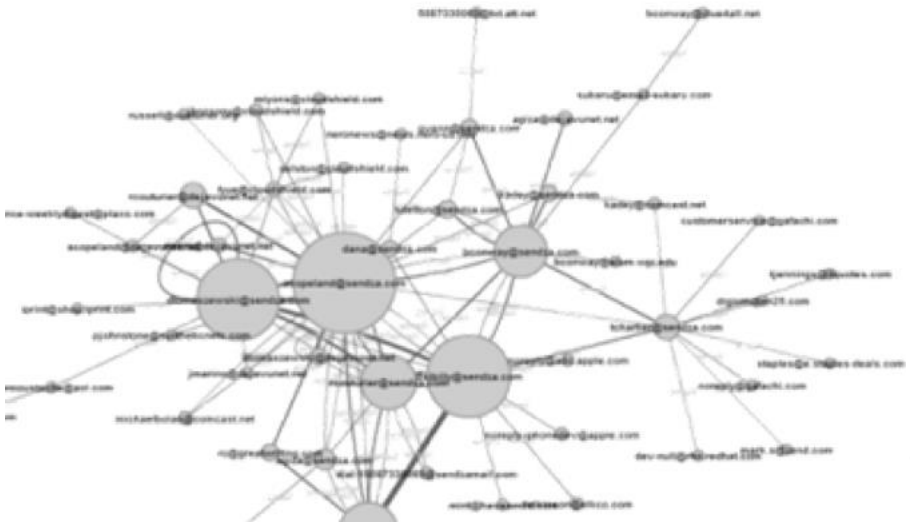
- Plně integrované do Qradar SIEM konzole
- Jednotné zobrazení detailních informací pro uživatele, incident, síťový tok
- Deep packet inspection
- Full packet capture pro komplet rekonstrukci



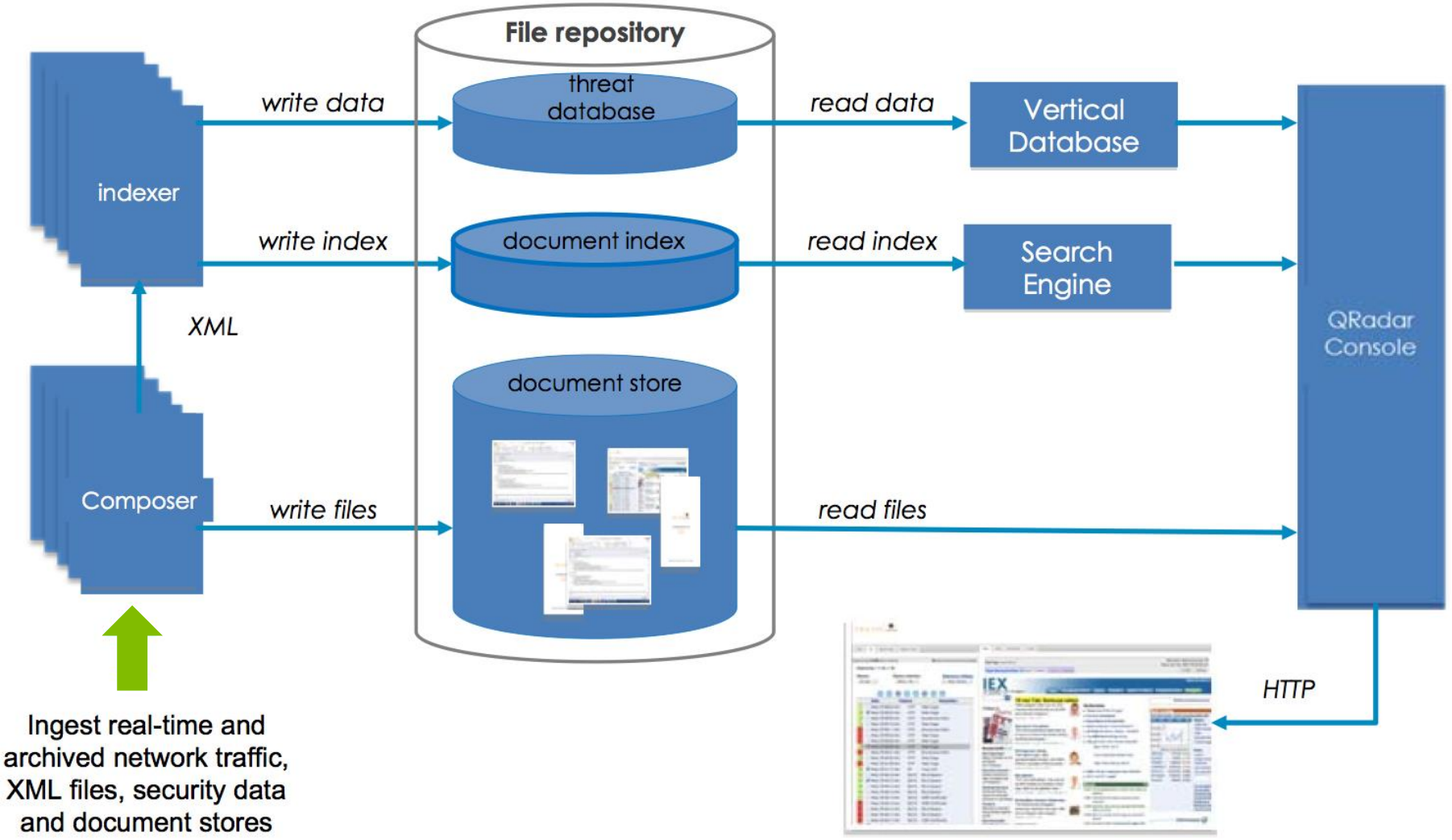
Vizualizace a analýza

- Spojení entit na různá ID, data na která bylo přistoupeno, URL atd.
- Vizuální rekonstrukce s kým kdo komunikoval a jak
- Out-of-the-box pravidla pro detekci citlivého obsahu
- Využití X-Force IP reputation databáze pro detekci podezřelého v PCAP
- Kategorizace web dat (media, vzdělání, xxx, sociální media,…)





Architektura



Video

Mobilní aplikace Deloitte CZ

Android iOS

Zpravodaje I Studie I Semináře I Novinky I Videa

Deloitte.