

# Forenzní analýza jako doplněk SIEMu

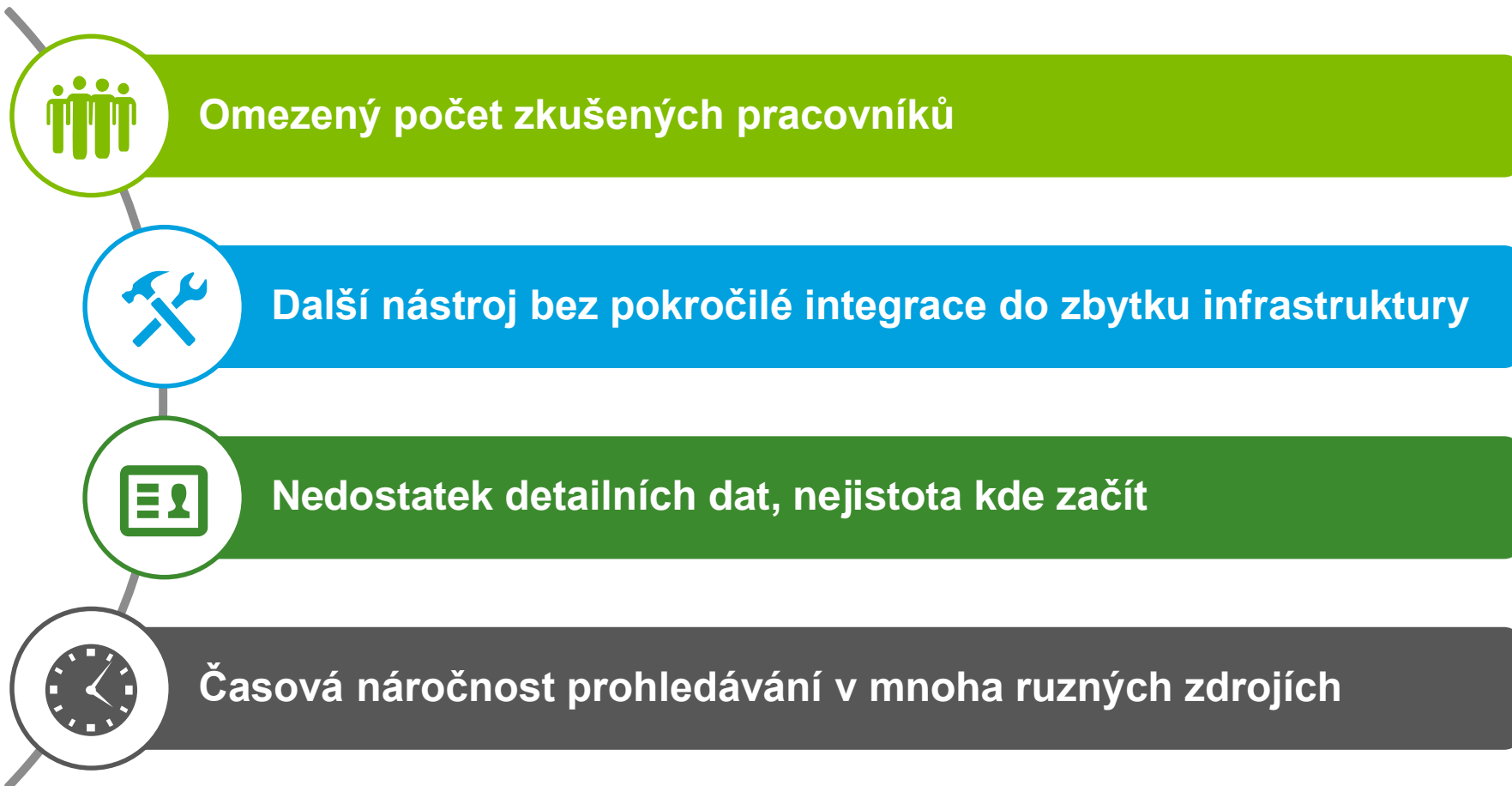
Jiří Slabý

31.3.2015

Policejní akademie ČR, Praha



# Běžné problémy při zavádění forenzní analýzy



# Nová generace forenzních nástrojů

## Integrované do nástroje SIEM

### Upozorní na incident

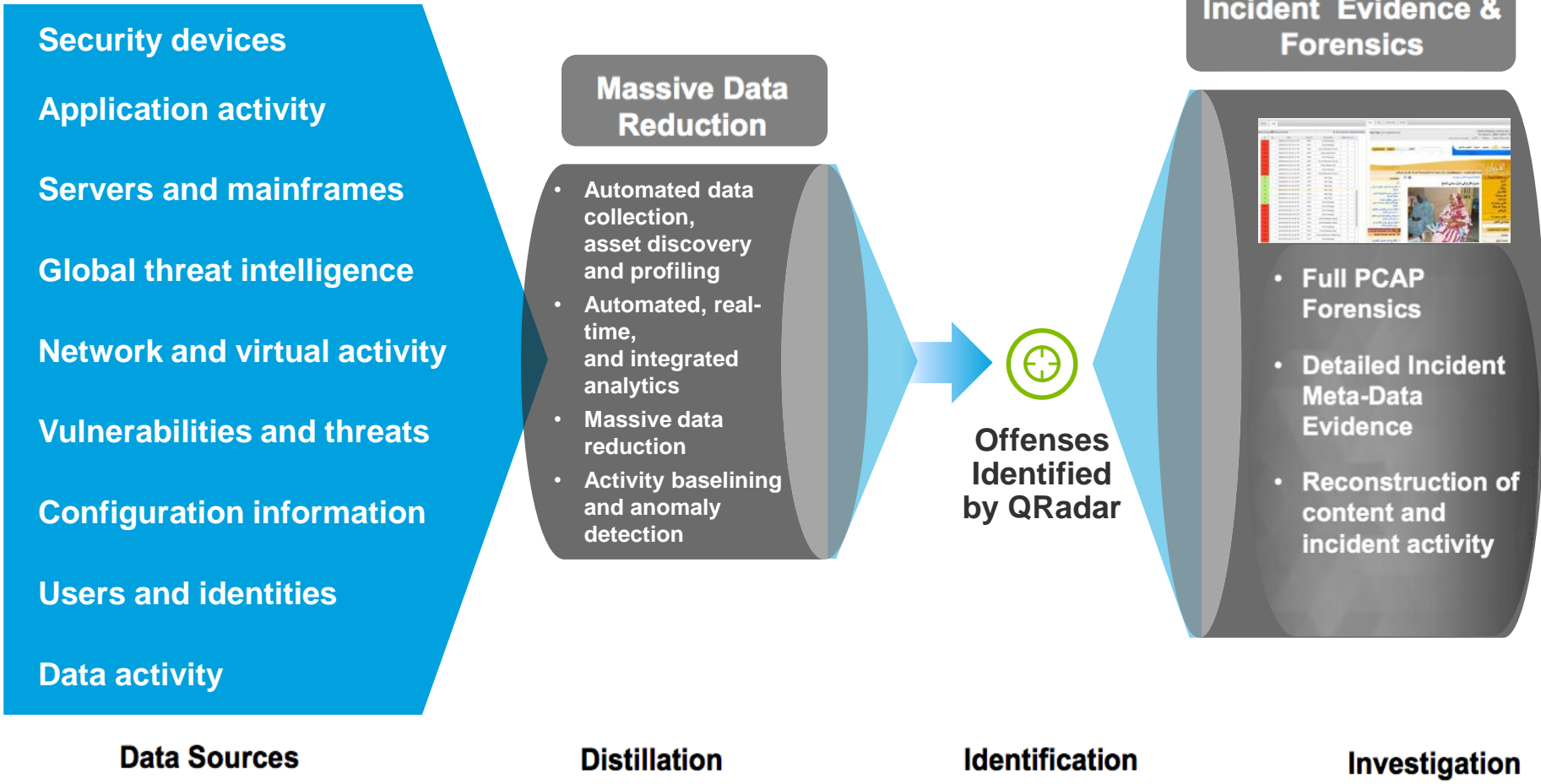
- Integrovaný s Qradar SIEM
- Využívá interní search technologii nad metadaty
- Během vteřin zobrazuje výsledky

### 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

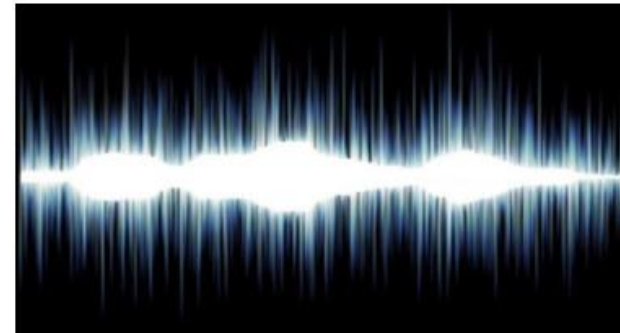
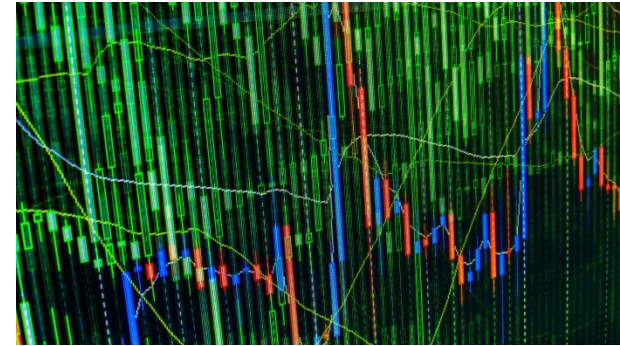


## Shromáždění důkazů

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

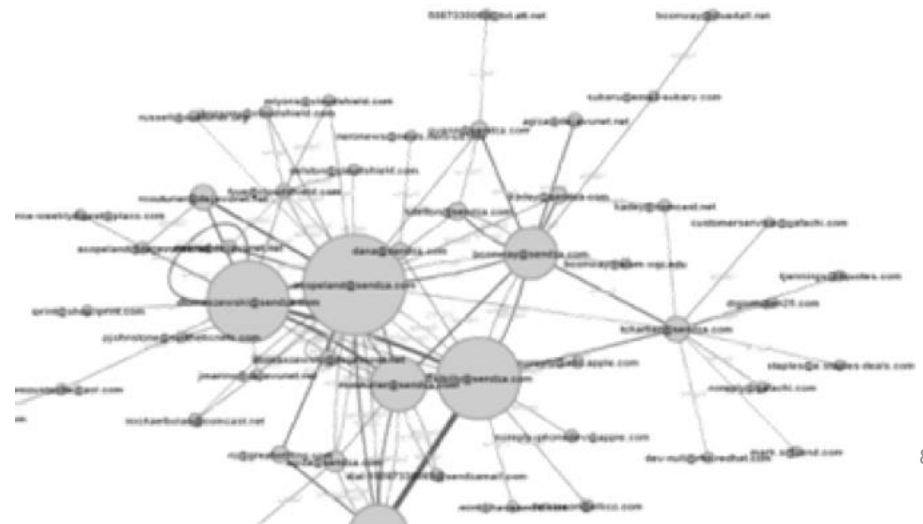
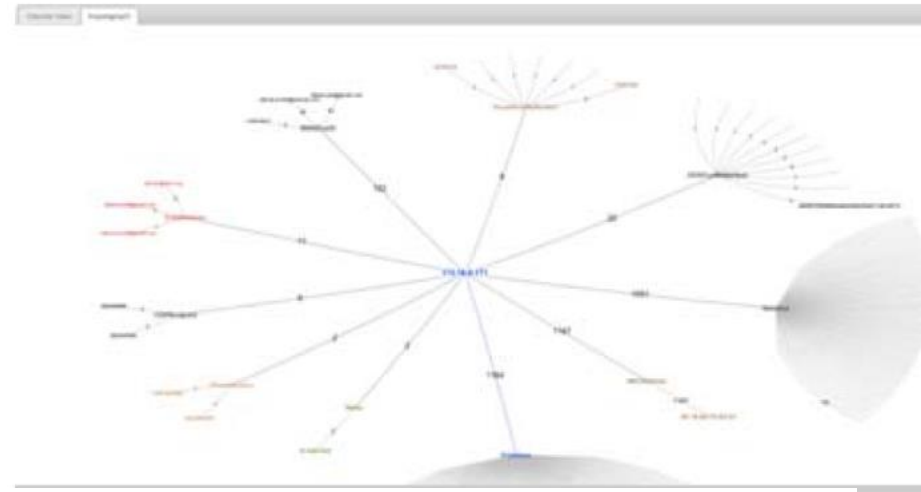
- Plně integrované do Qradar SIEM konzole
- Jednotné zobrazení detailních informací pro uživatele, incident, síťový tok
- Deep packet inspection
- Full packet capture pro komplet rekonstrukci

The screenshot displays the Qradar Dashboard interface. The top navigation bar includes 'Qradar - Dashboard', 'Qradar-SLIM - Dashboard', and 'Qradar - Security / Risk Management'. The main content area is divided into several sections: 'Threat and Security Monitoring', 'Most Severe Offenses', and 'Flow Bias (Total Bytes)'. A red box highlights the search query 'Remote Desktop Access from the Internet containing' in the 'Offense Name' column. A red arrow labeled '[right-click]' points to the search results table. The table has columns for Row, Sel, Score, Time Stamp, Protoc, Description, Suspec, Content, From, and To. The search results show a list of email messages and chat messages related to the search query.

Row	Sel	Score	Time Stamp	Protoc	Description	Suspec	Content	From	To
1	<input type="checkbox"/>	1	2008/04/24 01	SMTP	Email Message		That's very interesting - I di	"Andrew E. Copeland" <...>	"Russell Couturier" <...>
2	<input type="checkbox"/>	1	2008/04/24 01	SMTP	Email Alternate		That's	"Andrew E. Copeland" <...>	"Russell Couturier" <...>
3	<input type="checkbox"/>	1	2008/04/24 01	SMTP	Email Message		That's very interesting - I di	"Andrew E. Copeland" <...>	"Russell Couturier" <...>
4	<input type="checkbox"/>	1	2008/04/24 01	SMTP	Email Alternate		That's	"Andrew E. Copeland" <...>	"Russell Couturier" <...>
5	<input type="checkbox"/>	1	2008/04/24 01	POP3	Email Message		That's very interesting - I di	"Andrew E. Copeland" <...>	"Russell Couturier" <...>
6	<input type="checkbox"/>	1	2008/04/24 01	POP3	Email Alternate		That's	"Andrew E. Copeland" <...>	"Russell Couturier" <...>
7	<input type="checkbox"/>	1	2008/04/24 01	SMTP	Email Message		I'm a little concerned about	"Andrew E. Copeland" <...>	"Russell Couturier" <...>
8	<input type="checkbox"/>	1	2008/04/24 01	SMTP	Email Alternate		lâ	"Andrew E. Copeland" <...>	"Russell Couturier" <...>
9	<input type="checkbox"/>	1	2008/04/24 01	POP3	Email Message		I'm a little concerned about	"Andrew E. Copeland" <...>	"Russell Couturier" <...>
10	<input type="checkbox"/>	1	2008/04/24 01	POP3	Email Alternate		lâ	"Andrew E. Copeland" <...>	"Russell Couturier" <...>
11	<input type="checkbox"/>	1	2008/04/24 01	SMTP	Email Message		The aluminum nitrate shipm	Dana Tomaszewski <dtoma...>	Russell Couturier <rcouturie...>
12	<input type="checkbox"/>	1	2008/04/24 01	POP3	Email Message		The aluminum nitrate shipm	Dana Tomaszewski <dtoma...>	Russell Couturier <rcouturie...>
13	<input type="checkbox"/>	1	2008/04/24 08	SMTP	Email Message		Is the aluminum nitrate puri	"Dana Tomaszewski" <dt...>	"Russell Couturier" <...>
14	<input type="checkbox"/>	1	2008/04/24 08	SMTP	Email Alternate		Is the aluminumnitrate pure	"Dana Tomaszewski" <dt...>	"Russell Couturier" <...>
15	<input type="checkbox"/>	1	2008/04/24 08	POP3	Email Message		Is the aluminum nitrate puri	"Dana Tomaszewski" <dt...>	"Russell Couturier" <...>
16	<input type="checkbox"/>	1	2008/04/24 08	POP3	Email Alternate		Is the aluminumnitrate pure	"Dana Tomaszewski" <dt...>	"Russell Couturier" <...>
17	<input type="checkbox"/>	1	2008/04/24 01	SMTP	Email Message		How many pounds of the al	Dana Tomaszewski <dtoma...>	"Andrew E. Copeland" <...>
18	<input type="checkbox"/>	1	2008/04/24 01	POP3	Email Message		How many pounds of the al	Dana Tomaszewski <dtoma...>	"Andrew E. Copeland" <...>
19	<input type="checkbox"/>	1	2008/04/24 01	POP3	Email Message		How many pounds of the al	Dana Tomaszewski <dtoma...>	"Andrew E. Copeland" <...>
20	<input type="checkbox"/>	1	2008/04/24 01	SMTP	Email Message		Don't forget the money, law	"Andrew E. Copeland" <...>	"Dana Tomaszewski" <...>
21	<input type="checkbox"/>	1	2008/04/24 01	SMTP	Email Message		Don't forget the money, law	"Andrew E. Copeland" <...>	"Dana Tomaszewski" <...>
22	<input type="checkbox"/>	1	2009/03/12 12	MSN	MSN Chat Mess		Did I tell you about the alu	saimvnon@hotmail.com	olohstone@romail.com

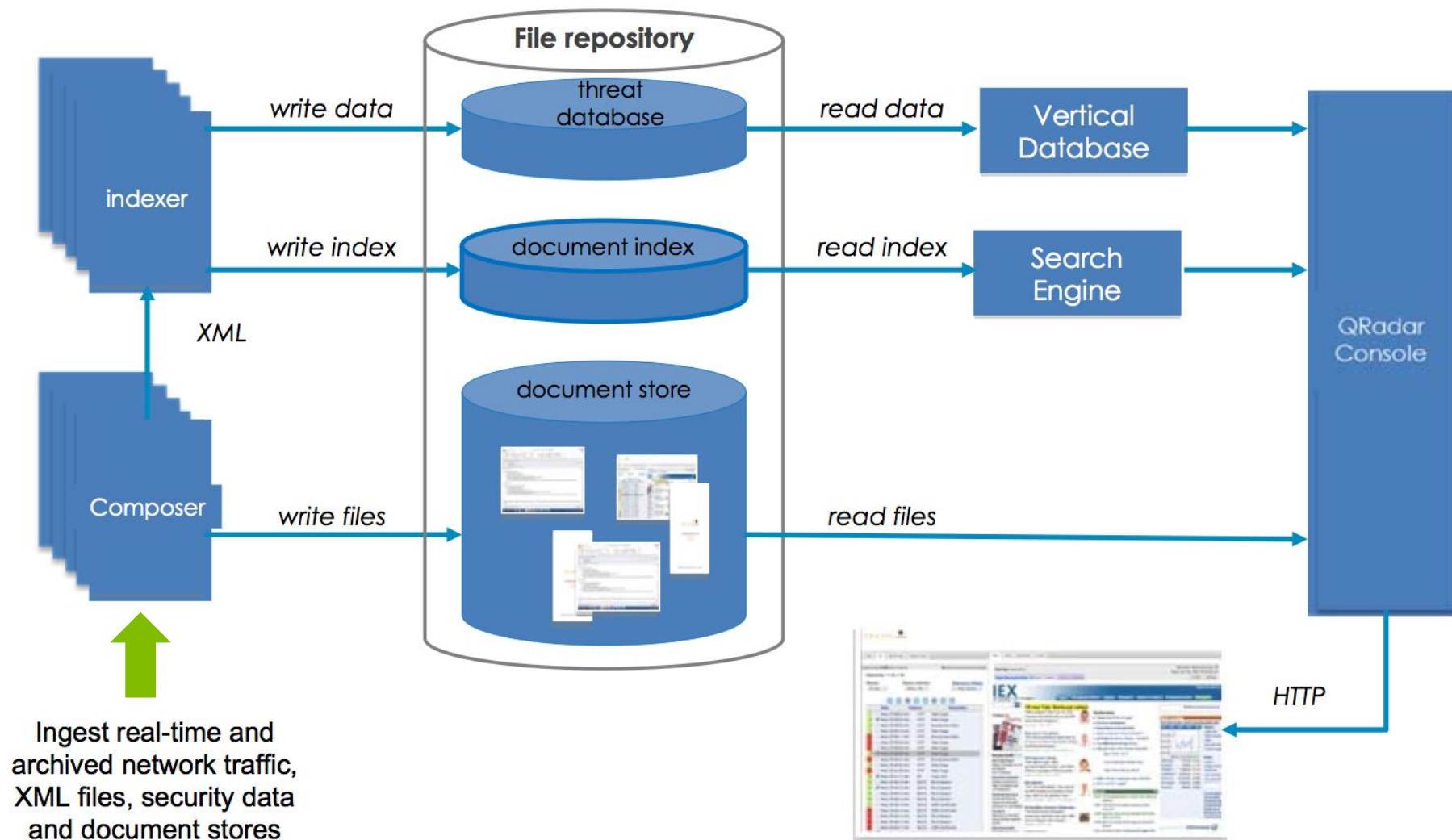
# Vizualizace a analýza

- 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



[Zpravodaje](#) | [Studie](#) | [Semináře](#) | [Novinky](#) | [Videa](#)

# Deloitte.

Deloitte označuje jednu či více společností Deloitte Touche Tohmatsu Limited, britské privátní společnosti s ručením omezeným zárukou („DTTL“), jejich členských firem a jejich spřízněných subjektů. Společnost DTTL a každá z jejich členských firem představuje samostatný a nezávislý právní subjekt. Společnost DTTL (rovněž označovaná jako „Deloitte Global“) služby klientům neposkytuje. Podrobný popis právní struktury společnosti Deloitte Touche Tohmatsu Limited a jejich členských firem je uveden na adrese [www.deloitte.com/cz/onas](http://www.deloitte.com/cz/onas).

Společnost Deloitte poskytuje služby v oblasti auditu, daní, poradenství a finančního a právního poradenství klientům v celé řadě odvětví veřejného a soukromého sektoru. Díky globálně propojené síti členských firem ve více než 150 zemích a teritoriích má společnost Deloitte světové možnosti a poskytuje svým klientům vysoce kvalitní služby v oblastech, ve kterých klienti řeší své nejkompexnější podnikatelské výzvy. Přibližně 200 000 odborníků usiluje o to, aby se společnost Deloitte stala standardem nejvyšší kvality.

Společnost Deloitte ve střední Evropě je regionální organizací subjektů sdružených ve společnosti Deloitte Central Europe Holdings Limited, která je členskou firmou sdružení Deloitte Touche Tohmatsu Limited ve střední Evropě. Odborné služby poskytují dceřiné a přidružené podniky společnosti Deloitte Central Europe Holdings Limited, které jsou samostatnými a nezávislými právními subjekty. Dceřiné a přidružené podniky společnosti Deloitte Central Europe Holdings Limited patří ve středoevropském regionu k předním firmám poskytujícím služby prostřednictvím více než 4 700 zaměstnanců ze 37 pracovišť v 17 zemích.