

BusinessConnect 2014

Partner pro váš růst

10. června 2014 | La Fabrika, Praha



BusinessConnect 2014

Partner pro váš růst



Jiří Slabý

Business Solution Architect IBM



BusinessConnect 2014

Partner pro váš růst



Video

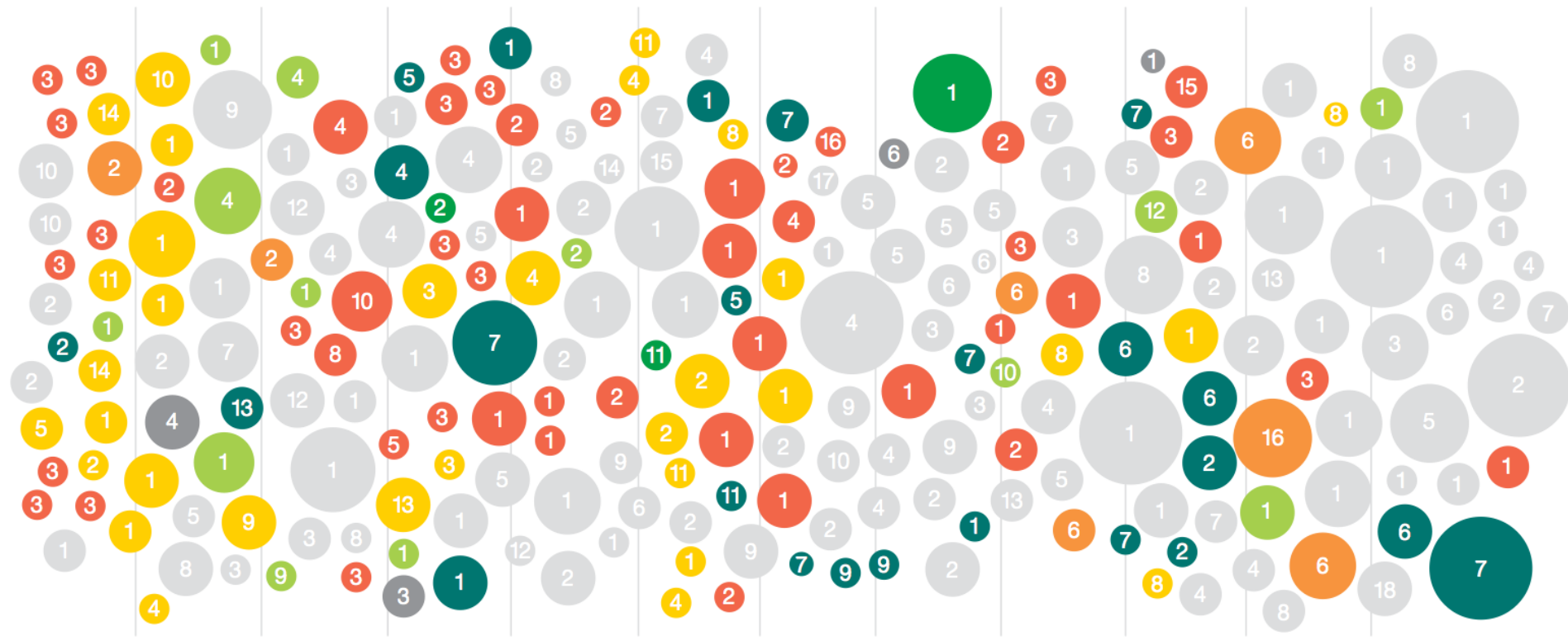




Sampling of 2013 security incidents by attack type, time and impact

conjecture of relative breach impact is based on publicly disclosed information regarding leaked records and financial losses

January February March April May June July August September October November December



Attack types SQL injection Spear phishing DDoS Physical access Malware XSS Watering hole Undisclosed

Size of circle estimates relative impact of incident in terms of cost to business.

IBM X-Force Threat Intelligence Quarterly Q1 2014

BusinessConnect 2014

Partner pro váš růst



Zabezpečení dat

Je třeba? Již nyní? V pohodě, máme firewal...





Datová exploze

IT využívají netechničtí lidé

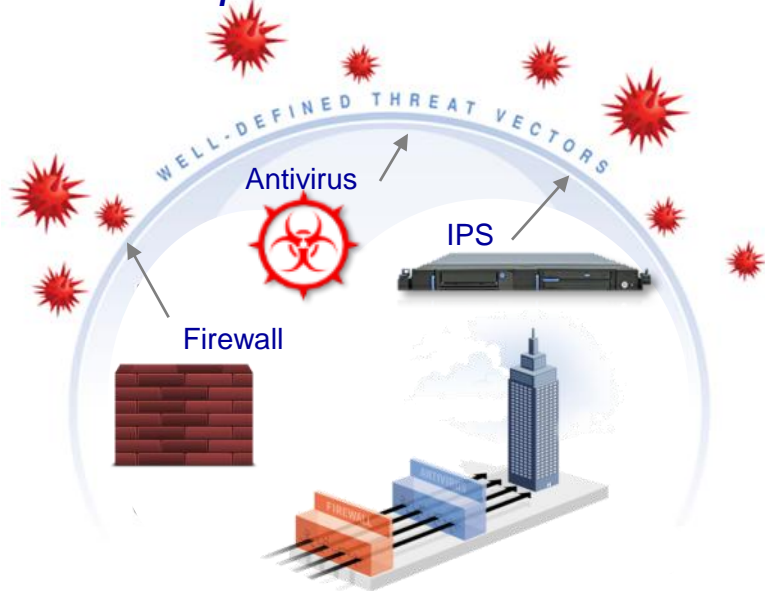
Více zařízení

Sofistikovanější útoky

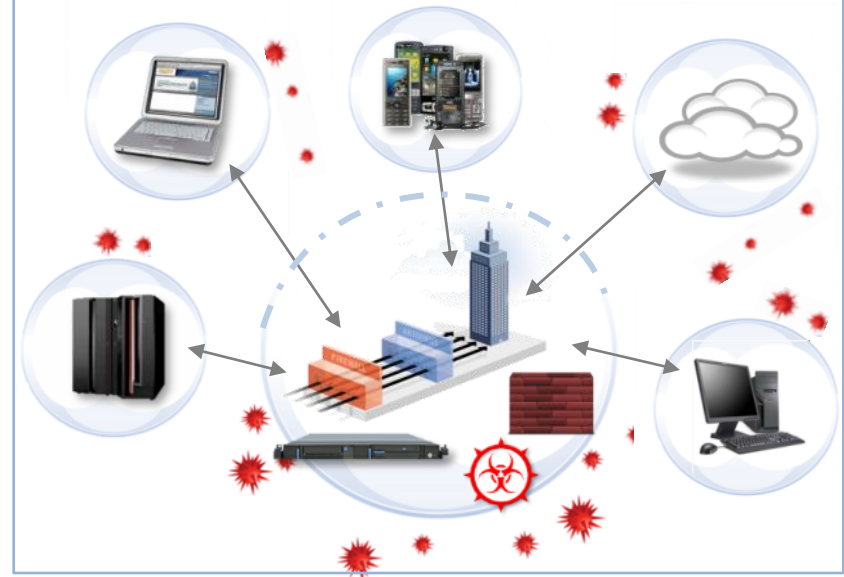


Od perimetru k ochraně zevnitř

Posun od tradiční perimetrové bezpečnosti...



...k cílenému zabezpečení tam, kde je potřeba.





Data jsou největším cílem útočníků

% of Records Breached (2010)

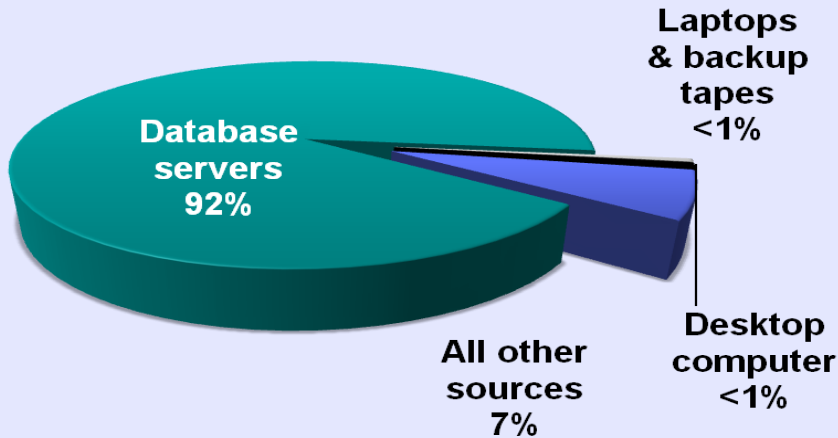
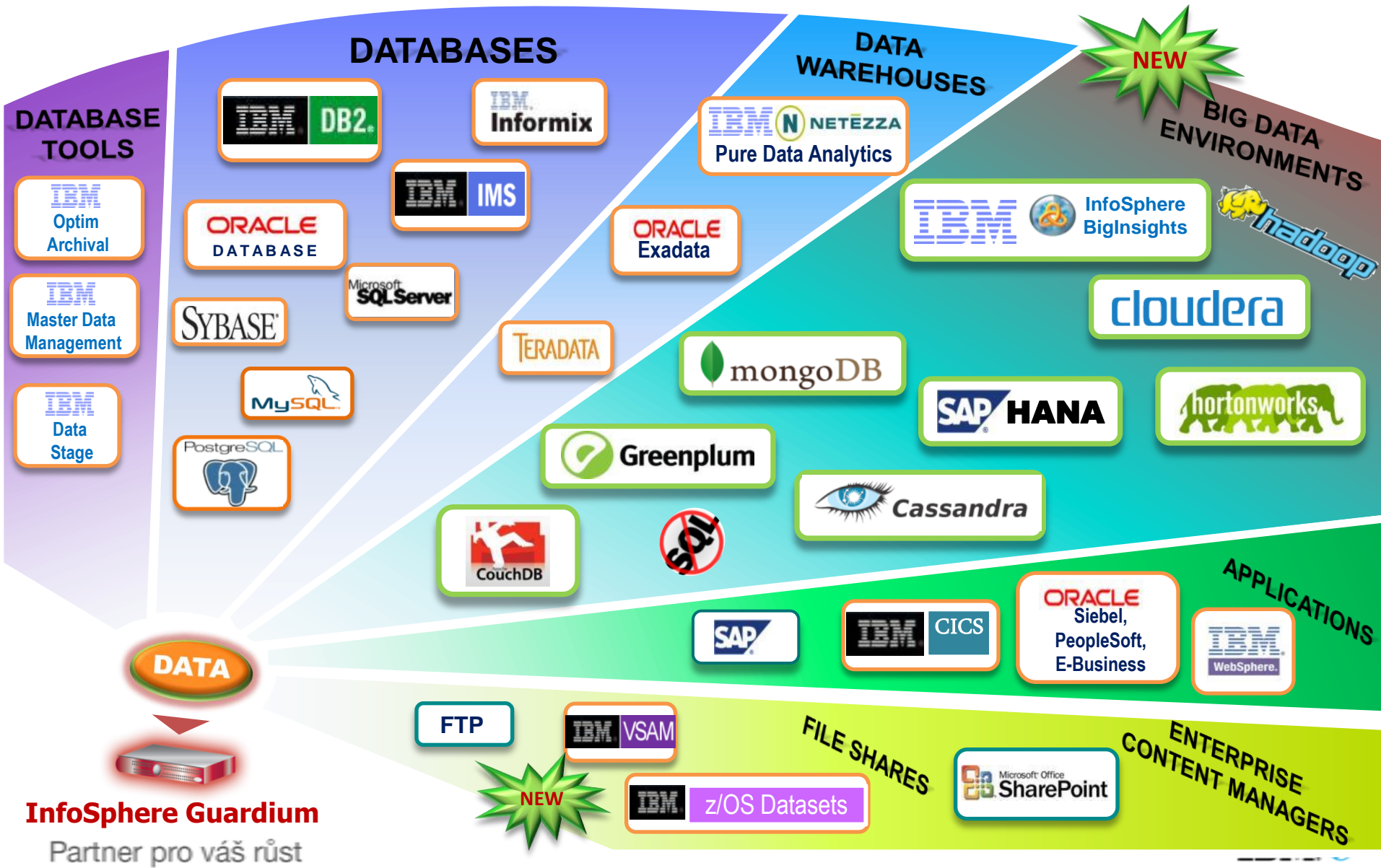


Table 10. Compromised assets by percent of breaches and percent of records*

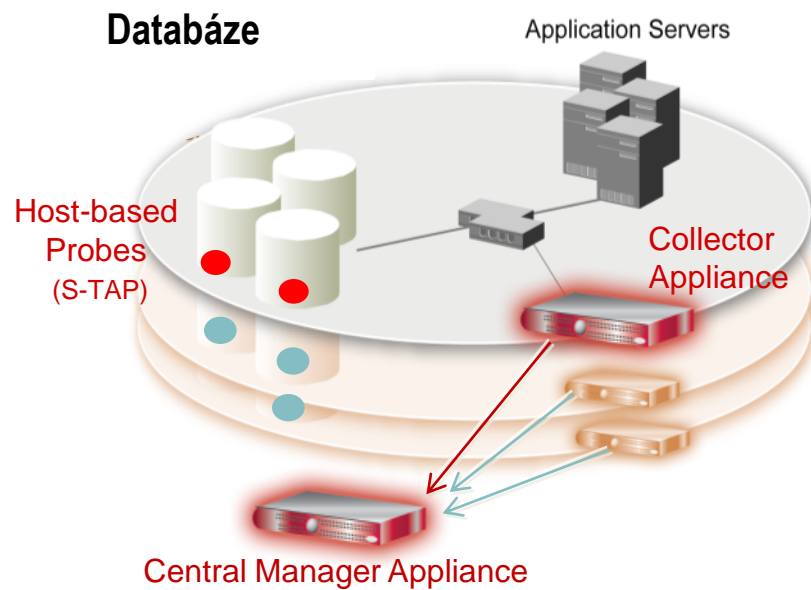
Type	Category	All Orgs		Larger Orgs	
POS server (store controller)	Servers	50%	1%	2%	<1%
POS terminal	User devices	35%	<1%	2%	<1%
Desktop/Workstation	User devices	18%	34%	12%	36%
Automated Teller Machine (ATM)	User devices	8%	<1%	13%	<1%
Web/application server	Servers	6%	80%	33%	82%
Database server	Servers	6%	96%	33%	98%
Regular employee/end-user	People	3%	1%	5%	<1%
Mail server	Servers	3%	2%	10%	2%
Payment card (credit, debit, etc.)	Offline data	3%	<1%	0%	<1%
Cashier/Teller/Waiter	People	2%	<1%	2%	<1%
Pay at the Pump terminal	User devices	2%	<1%	0%	<1%
File server	Servers	1%	<1%	5%	<1%
Laptop/Netbook	User devices	1%	<1%	5%	<1%
Remote access server	Servers	1%	<1%	7%	<1%
Call Center Staff	People	1%	<1%	7%	<1%

2012 and 2013 Data Breach Report from Verizon Business RISK Team

http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf



InfoSphere Guardium
Partner pro váš růst



BusinessConnect 2014

Partner pro váš růst



Zabezpečení databází v praxi

Aleš Tumpach, IT Security Specialist
Raiffeisenbank



BusinessConnect 2014

Partner pro váš růst



Pomoc při forenzní analýze IT incidentu

...snímání otisků, ultrafialová lampa, analýza DNA...





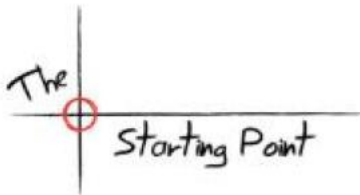
Problémy při zavádění forenzní analýzy



Omezený počet zkušených pracovníků



Další nástroj bez pokročilé integrace



Nedostatek detailních dat, nejistota kde začít



Časová náročnost
prohledávání v mnoha
různých zdrojích



Security devices

Application activity

Servers and mainframes

Global threat intelligence

Network and virtual activity

Vulnerabilities and threats

Configuration information

Users and identities

Data activity

Massive Data Reduction

- Automated data collection, asset discovery and profiling
- Automated, real-time, and integrated analytics
- Massive data reduction
- Activity baselining and anomaly detection



Offenses Identified by QRadar

Incident Evidence & Forensics



- Full PCAP Forensics
- Detailed Incident Meta-Data Evidence
- Reconstruction of content and incident activity

Data Sources

Distillation

Identification

Investigation

Nová generace síťového forenzního nástroje



Nový modul IBM QRadar Forensics

Upozorní na incident

- Integrovaný s IBM 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 analysis

Odhalte kolaboranty, identifikujte podvodníky a dotčené systémy



Detekce fraudu

Odhalte komplikovaný podvod



Shromáždění důkazů

Zkompletujte evidenci o činnosti malware



Jeden systém pro validní výstupy

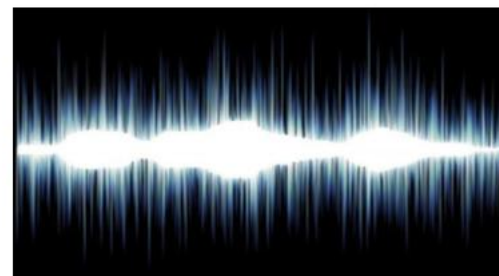
Poskytuje vyhledávání nad vysoce indexovaným, taxonomickým úložištěm:

- Síťová data
- Soubory
- Identity

Zpracovává, convertuje

- PCAP
- XML
- Dokumenty (běžné formáty)
- Archivy

Navrací detailní výsledky během vteřin



Jako parametr daného incidentu nebo ad-hoc dotazy

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

The screenshot shows the Qradar Dashboard interface. A search query 'From:acopeland To:rcouturier aluminum nitrate shipment' is entered. The results table is as follows:

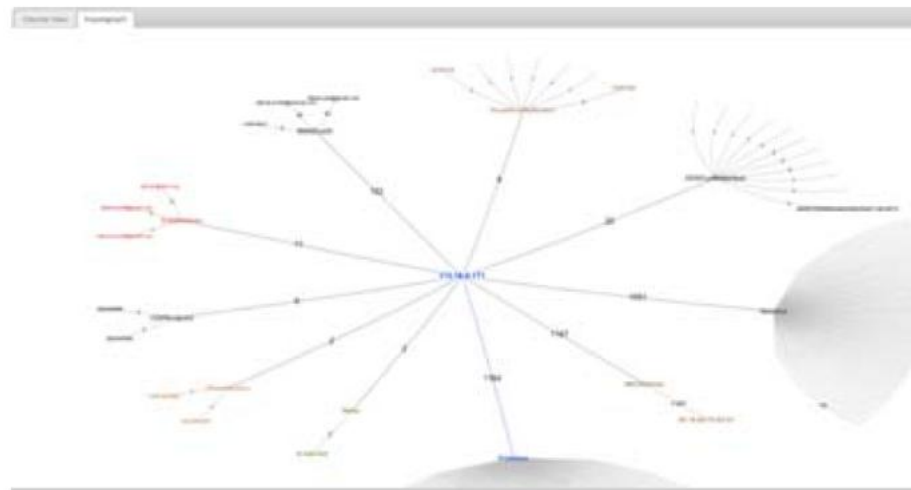
Row	Sel	Score	Time Stamp	Protoc	Description	Suspec	Content	From	To
1	<input type="checkbox"/>	1	2008/04/24 01	SMTP	Email Message		That's very interesting - I di	"Andrew E. Copeland" <...>	"Russell Couturier" <...>
2	<input type="checkbox"/>	1	2008/04/24 01	SMTP	Email Alternate		Thatã	"Andrew E. Copeland" <...>	"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		Thatã	"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		Thatã	"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		ã	"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		ã	"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 ah	Dana Tomaszewski <dtoma>	"Andrew E. Copeland" <...>
18	<input type="checkbox"/>	1	2008/04/24 01	POP3	Email Message		How many pounds of the ah	Dana Tomaszewski <dtoma>	"Andrew E. Copeland" <...>
19	<input type="checkbox"/>	1	2008/04/24 01	SMTP	Email Message		Don't forget the money, law	"Andrew E. Copeland" <...>	"Dana Tomaszewski" <...>
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	2009/03/12 12	MSN	MSN Chat Mess		Did I tell you about the alu	saimmivon@hotmail.com	alohntone@omail.com

A red box highlights the search query in the top dashboard, and a red arrow labeled '[right-click]' points to the search results table. A 'QRadar Incident Forensics' label is also present.



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,...)





BusinessConnect 2014

Partner pro váš růst



Děkuji.

#BCCZ14

