



The Dictatorship of Data

Technology Services @ Hewlett-Packard Slovakia

Peter Mikeska



Agenda

Robert McNamara „body count“

Big Data – zber údajov a bezpečnosť

HP HAVEn

HP ArcSight – HP Autonomy v akcii



Robert McNamara

World War 2

Saving 3,6bl \$\$ in procurement by data-driven decision making / 1943

FORD „Whiz Kid“

fellow could walk on water

Vietnam War

Measurement of progress - „body count“ data point



Robert McNamara – after 70 years

Education problem ?

Push standardized tests to measure performance and penalize teachers or schools

Loose weight ?

Buy an app to count every calorie but eschew actual exercise

Want to prevent terrorism?

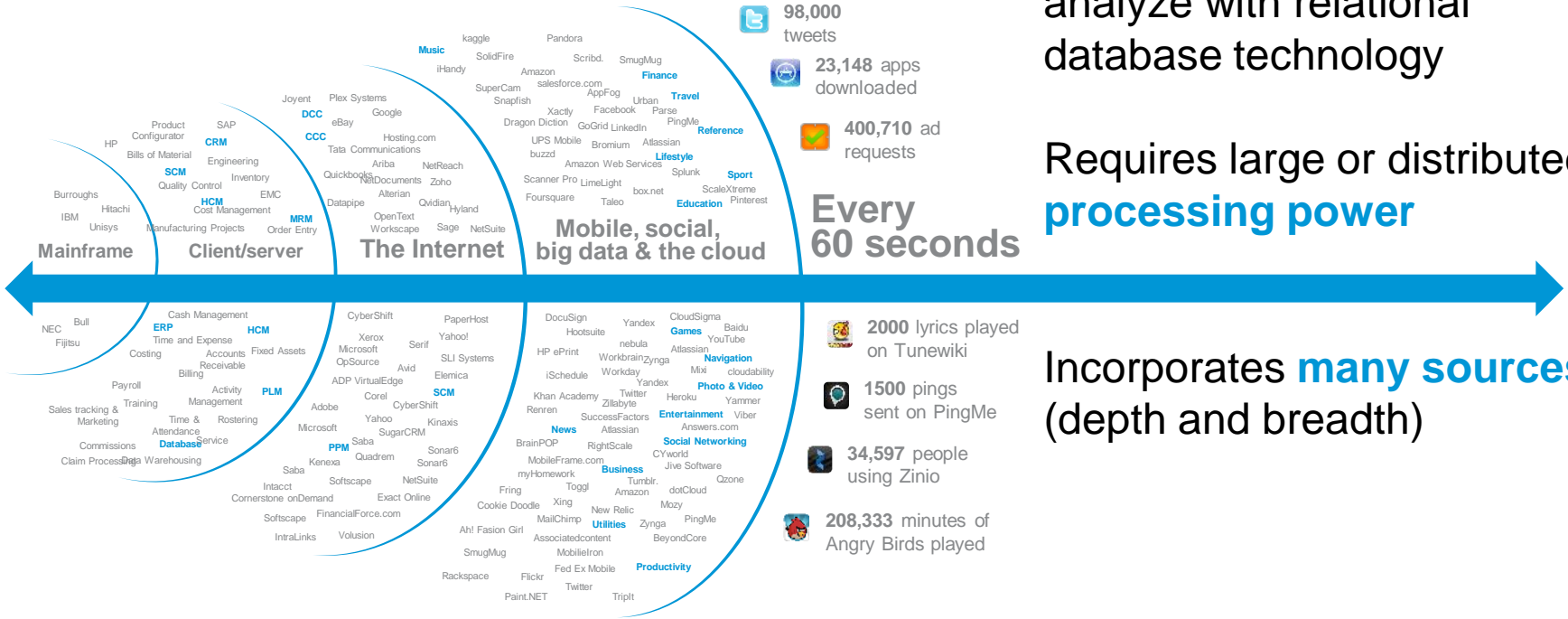
Create layers of watch lists and no-fly lists in order to police the skies

GOOGLE way

best color of a toolbar on the website – staff ordered to test 41 gradations of blue



What is big data?



Requires large or distributed
processing power

Incorporates **many sources**
(depth and breadth)

Applying big data to security challenges

Incorporate Unstructured data

Enhance security monitoring to develop improved intelligence capability

Use Cases

Email monitoring, social network monitoring, behavioral analysis

Security Operations

Leverage big data analytics for investigation, research, and real-time alerting



Information security challenges

Primary Challenges

1

Nature & Motivation of Attacks
(Fame → fortune, market adversary)

A new market adversary



Research



Infiltration



Discovery



Capture



Exfiltration

Information security challenges

Primary Challenges

1

Nature & Motivation of Attacks
(Fame → fortune, market adversary)

Traditional



Delivery

Private



Managed



Public



2

Transformation of Enterprise IT
(Delivery and consumption changes)

Virtual Desktops



Consumption

Notebooks



Tablets



Smart phones



Information security challenges

Primary Challenges

1

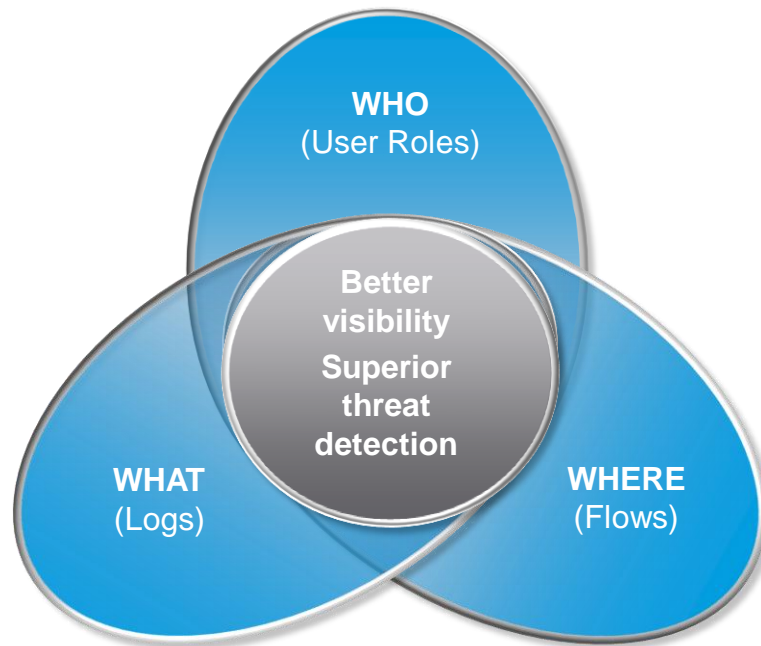
Nature & Motivation of Attacks
(Fame → fortune, market adversary)

2

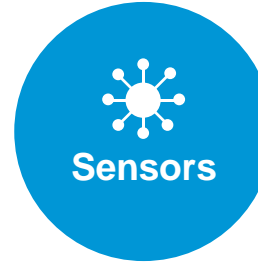
Transformation of Enterprise IT
(Delivery and consumption changes)

3

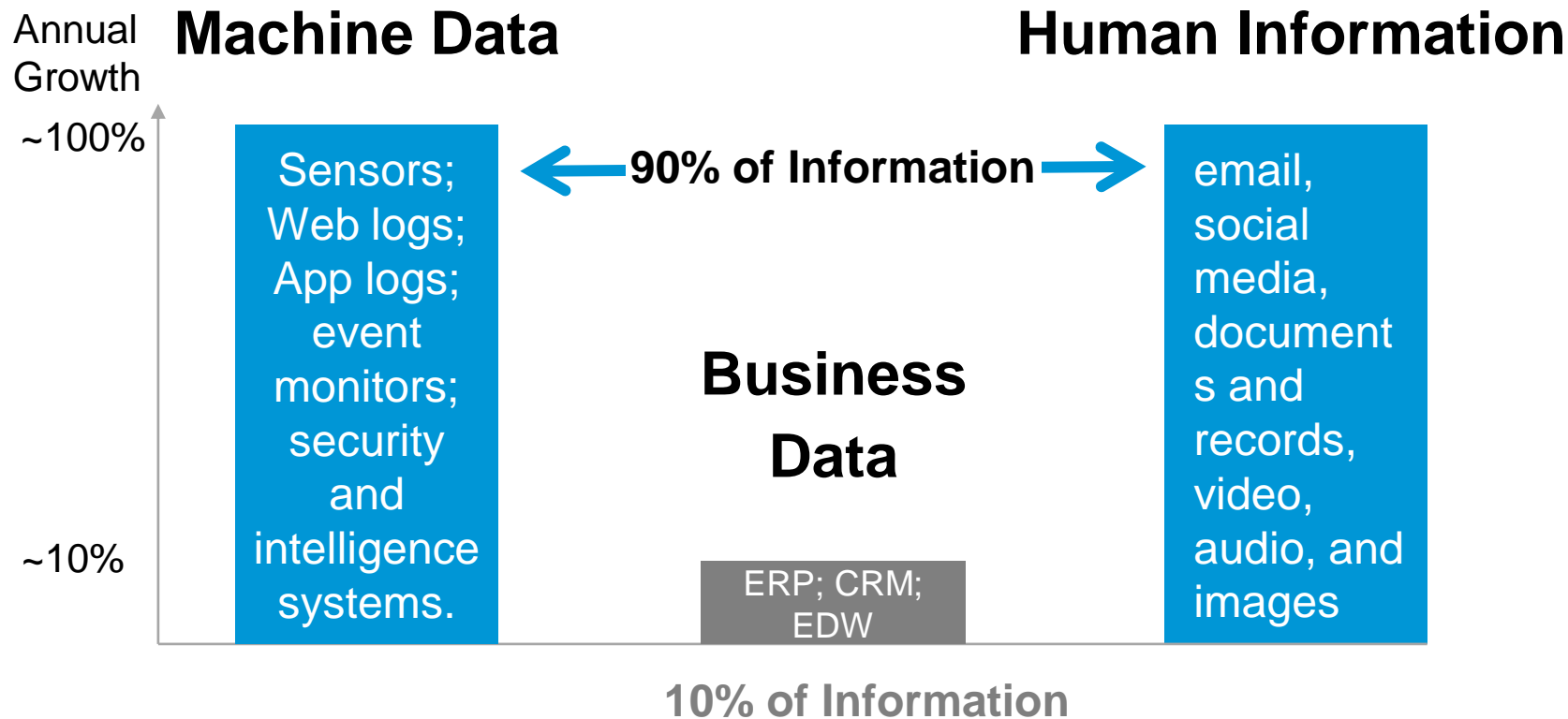
**Intelligence-driven models
are necessary**



„You're already a walking sensor platform“ – CIA CTO



Big Data landscape



HP HAVE_n



Big Data needs a unified approach

One platform for structured, semi, and unstructured to profit from 100% of data.

Enable me to:

on

100% of Data

- **Capture**
- **Store**
- **Manage**
- **Analyze**
- **Optimize**

Structured warehouses

CRM, transactions, sales, marketing...

Universal log management

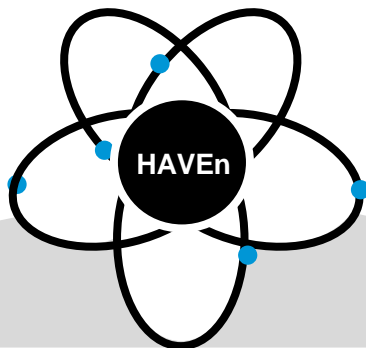
IT logs, security logs, social, tweets, JSON's

Unstructured

Audio, Video, emails, sentiments, threat ...



HAVEn – Big Data Platform



Hadoop/
HDFS

Catalog massive
volumes of
distributed data



Social media



Video



Audio



Email



Texts



Mobile



Transactional
data



Documents



IT/OT



Search engine



Images

— **A**utonomy
IDOL

Process and
index all
information

— **V**ertica

Analyze at
extreme scale
in real-time

— **E**nterprise
Security

Collect & unify
machine data

— **n** Apps

Powering
HP Software
+ **your** apps



HP ArcSight ESM and Autonomy IDOL

Unstructured data



- Email, files
- Social Media, Chat Sessions
- Websites, Audio/Video



CEF

CEF

HTTPS

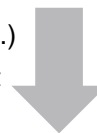
Alerts ESM to targeted negative
sentiment communications and threat
intelligence

IDOL provides additional business
context for suspicious communications

Display to analyst the full content of
communications and threat intelligence

Structured data

- Security Devices (FW, IDS, etc.)
- Identity & Access Management
- Applications



HP ArcSight
ESM

API query

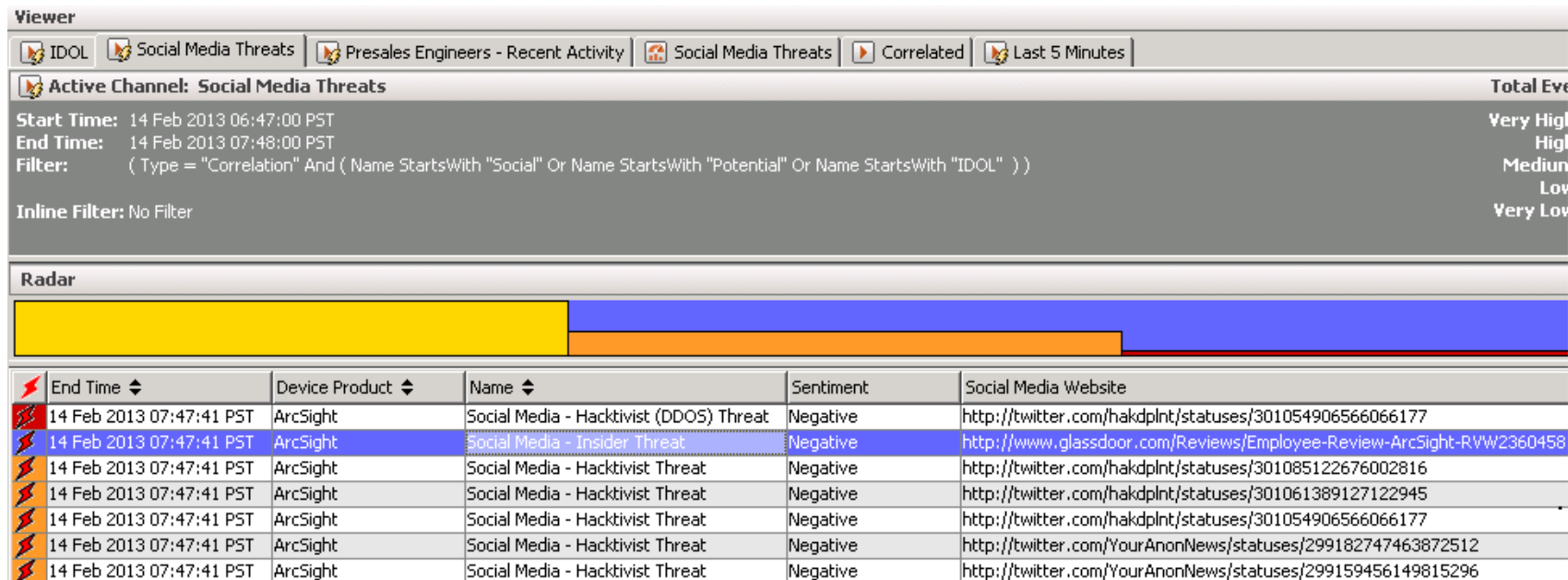
HTTP
S



HP ArcSight ESM & Autonomy IDOL in action



Social media monitoring for insider threats



Social media monitoring for insider threats

Kobalt Systems not what it used to be”

★★★★☆ Current Presales Engineer in Washington, DC – Reviewed Feb 11, 2013

Pros – The company is full of smart people and excellent technology. The benefits are very good and so are the perks (snacks, drinks, happy hour, etc.).

Cons – Excessively political. The ability to get something completed is based on who you know in the company. The training program is inadequate to successfully prepare one to be successful. I'm a presales engineer in the east and have been neglected by my management. I am strongly considering working for a competitor.

Advice to Senior Management – Focus more on people development and less on politics. Too often people are promoted based on personal relationships and not industry expertise.



Social media monitoring for insider threats

Active Channel: Presales Engineers - Recent Activity







Start Time: 14 Feb 2013 05:54:00 PST

End Time: 14 Feb 2013 07:55:00 PST

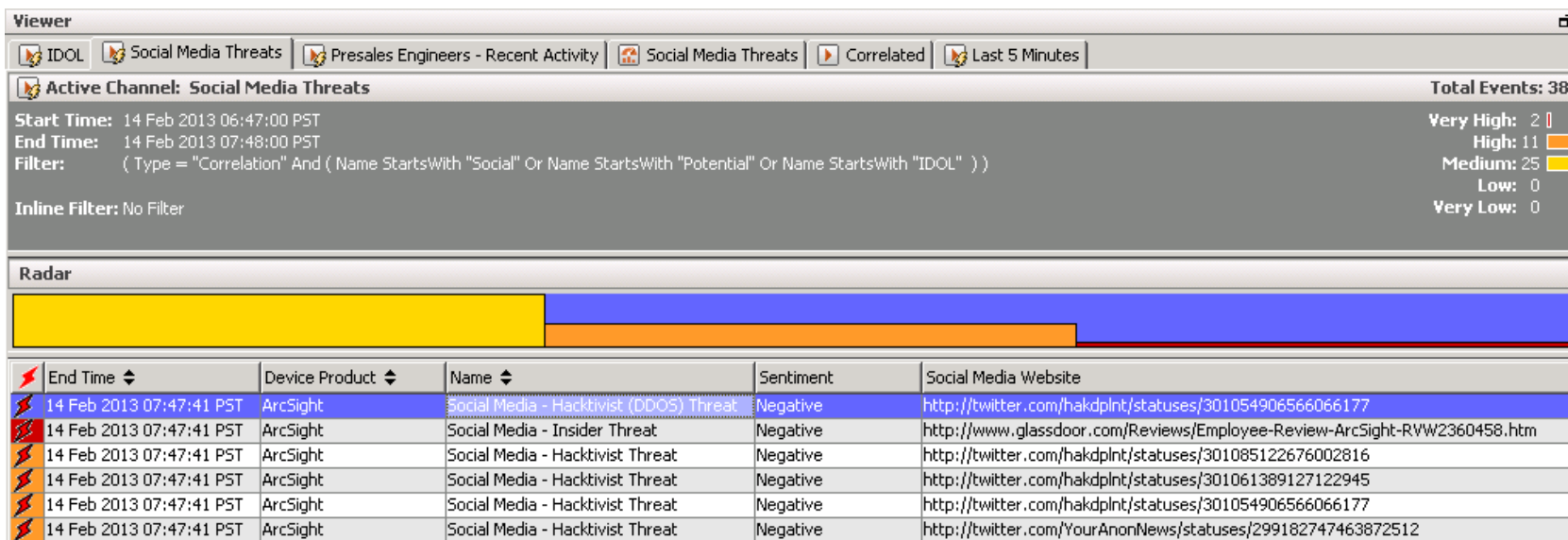
Filter: GetGroup.groupname = "Presales Engineer"

Inline Filter: No Filter

Radar

	End Time 		1	Name 	Device Vendor 	Device Product 	Attacker User Name	Destination User Name	GetGroup.groupname
	14 Feb 2013 07:47:42 PST			Logon	Microsoft	Windows	amaloney		Presales Engineer
	14 Feb 2013 07:47:42 PST			Logon	Microsoft	Windows	amaloney		Presales Engineer
	14 Feb 2013 07:47:42 PST			GET	Squid	Proxy	jsmith@kobaltsystems....		Presales Engineer
	14 Feb 2013 07:47:42 PST			GET	Squid	Proxy	jsmith@kobaltsystems....		Presales Engineer
	14 Feb 2013 07:47:42 PST			GET	Squid	Proxy	jsmith@kobaltsystems....		Presales Engineer
	14 Feb 2013 07:47:42 PST			Logon	Microsoft	Windows	aharvey		Presales Engineer
	14 Feb 2013 07:47:42 PST			Logon	Microsoft	Windows	aharvey		Presales Engineer
	14 Feb 2013 07:47:42 PST			email	Microsoft	Exchange	jsmith@kobaltsystems....	jeffreysmith@gmail.com	Presales Engineer

Social media monitoring for hacktivist threats



Social media monitoring for hacktivist threats



Joe Schmopped

@hakdpint



Follow

Kobalt Systems is infringing upon their employees' rights by monitoring every action on the network. We should teach them a lesson: DDOS

← Reply ↺ Retweet ★ Favorite ⋮ More



Joe Schmopped

@hakdpint

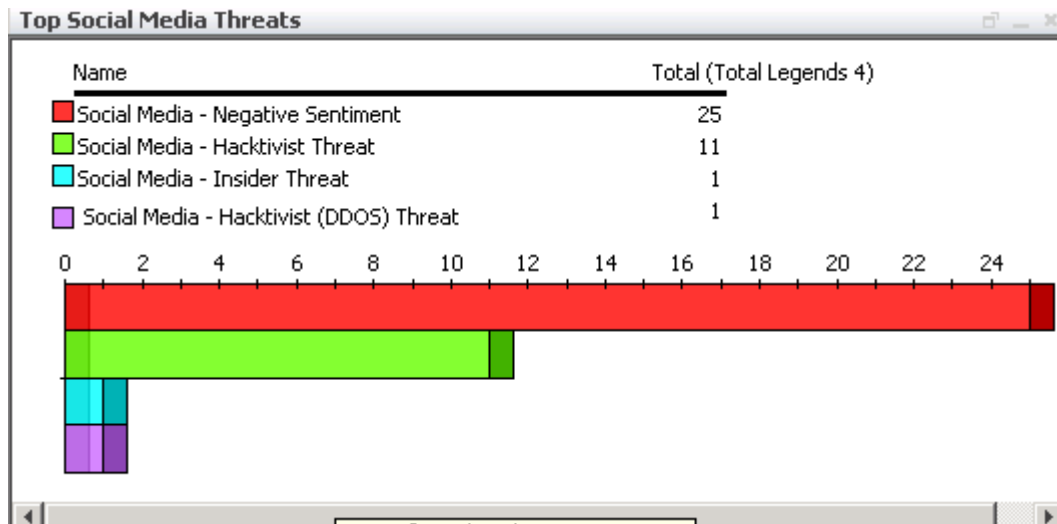


Follow

Found a JS/iframe ref vulnerable server at 10.10.10.120

← Reply ↺ Retweet ★ Favorite ⋮ More

Social media monitoring for hacktivist threats



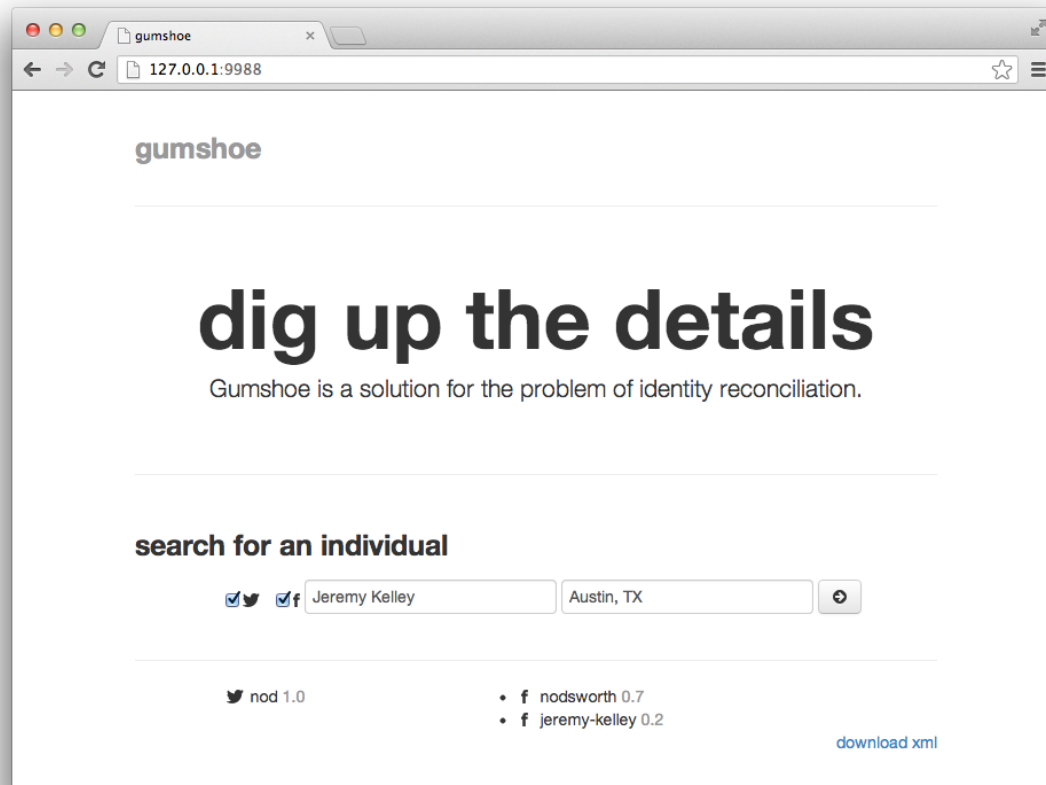
Social Identity Reconciliation

Gumshoe

How do you know that
John Doe is really @jdoe?

Finds social profiles via
simple heuristics.

Can easily be extended to
further refine results.



Just a bit more...



We're just getting started.

Google self-driving cars ~1Gb/s per vehicle

Jet turbines generate ~12 exabytes a day on commercial flights

7 billion people with Nike+, fitbit, Google Glass and the next thing...



Impact to Enterprise Security?

More data constantly generated.

More data to monitor.

More sources to monitor.

More signal to analyze.

**More Noise.
More Work.**



Ďakujem za pozornosť

peter.mikeska@hp.com

