

Decoding Cyber and IT Security Vulnerabilities in the Era of Big Data



HP ESP Global Services
Mike Loginov
Chief Cyber Strategist

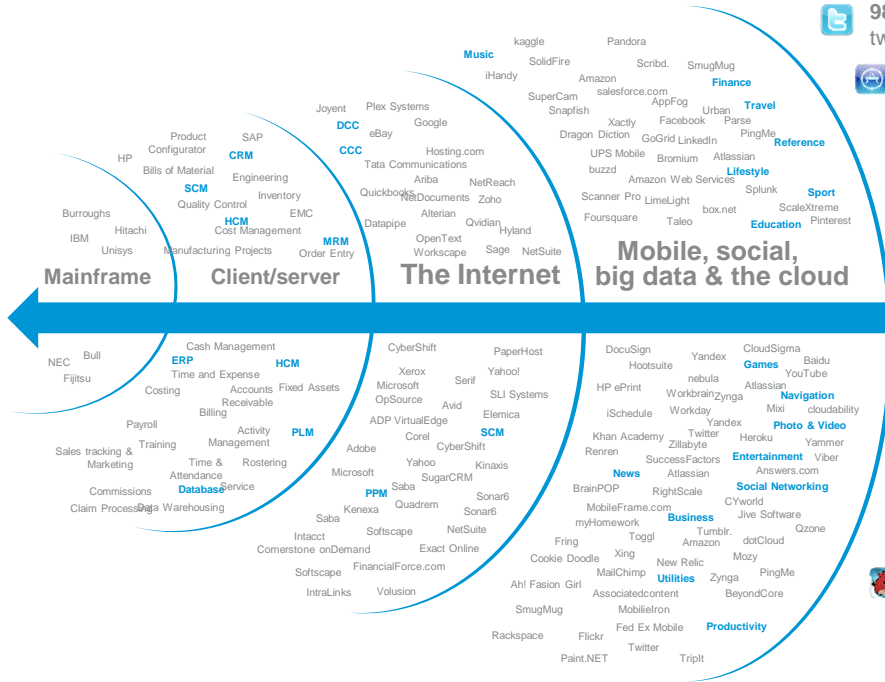
Topics

- **The Human Factor**
- **The Challenges Faced**
- **What Data Analytics Offers**
- **Exploitable Vulnerabilities**
- **Converting Analytics into Actionable Results**
- **Conclusion**





What is big data?



 98,000 tweets

 23,148 apps downloaded


 400,710 ad requests


Every 60 seconds

Data sets too large to analyze with relational database technology

Requires large or distributed processing power

 2000 lyrics played on Tunewiki

 1500 pings sent on PingMe

 34,597 people using Zinio

 208,333 minutes of Angry Birds played

Incorporates many sources (depth and breadth)



Growing Persistent Threat Vectors

- Hackers,
- Crackers,
- Criminals,
- Hacktavists,
- Idealists,
- Terrorists,
- Thieves,
- Disgruntled Employees,
- Spies,
- Social Engineers
- Nation States
- People in general.....!



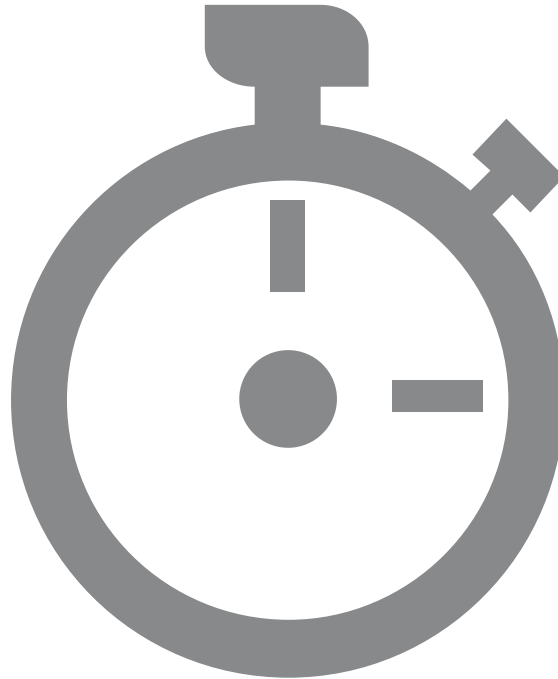
The Security Industry Is Not Catching Enough Bad Guys

Most enterprises remain challenged with missing critical breaches.

229 Days

is the median duration of how long breaches were present before discovery in 2013

(M-Trends Report)



100%

of business networks have traffic going to known malware hosting websites

(Cisco 2014 Annual Security Report)



Why Is This So Hard?

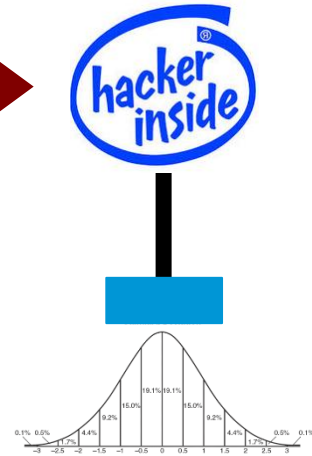
Bad guys know how to stay inside the bell curve.

Known: Easier to detect

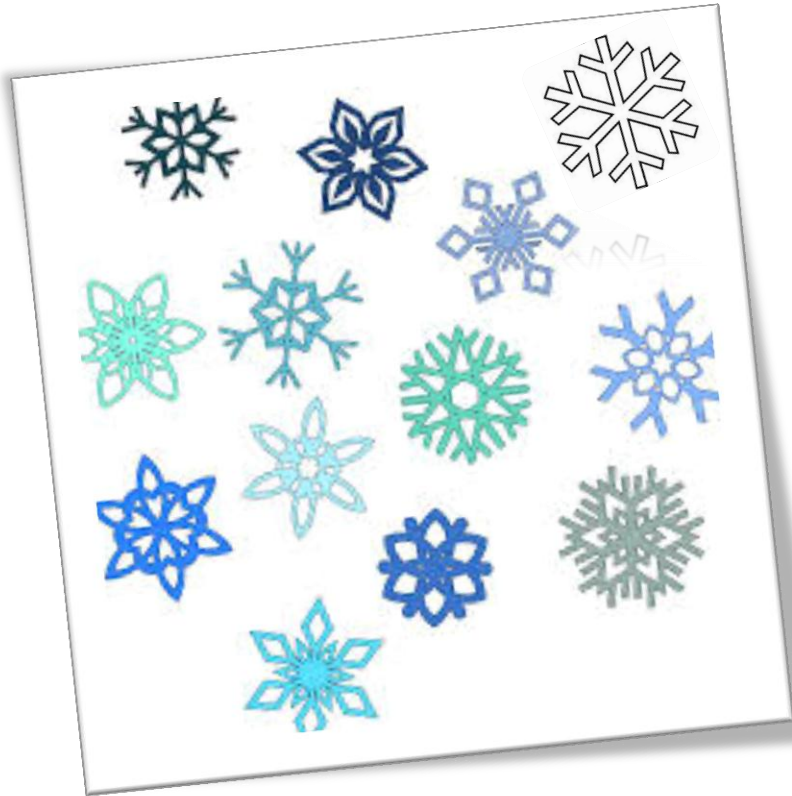
- Matches a signature
- Goes to a bad place
- Works in the clear
- Unauthorized Use
- Outside of baseline
- Within monitored infrastructure

Unknown: Harder to detect

- New behavior
- Goes to an approved place
- Works encrypted
- Authorized Use
- Inside of baseline
- Outside monitored infrastructure



Haystacks, Needles and Snow Flakes



UK is the No. 1 target for Advanced Persistent Threat cyber attacks

A report published by leading security specialist Firefly has discovered that the UK is the number one target for Advanced Persistent Threats. Taking data from the first half of 2014 the report looked at the cyber threat landscape across Europe, the Middle East and Asia (EMEA).



They're in there! Let's find them.

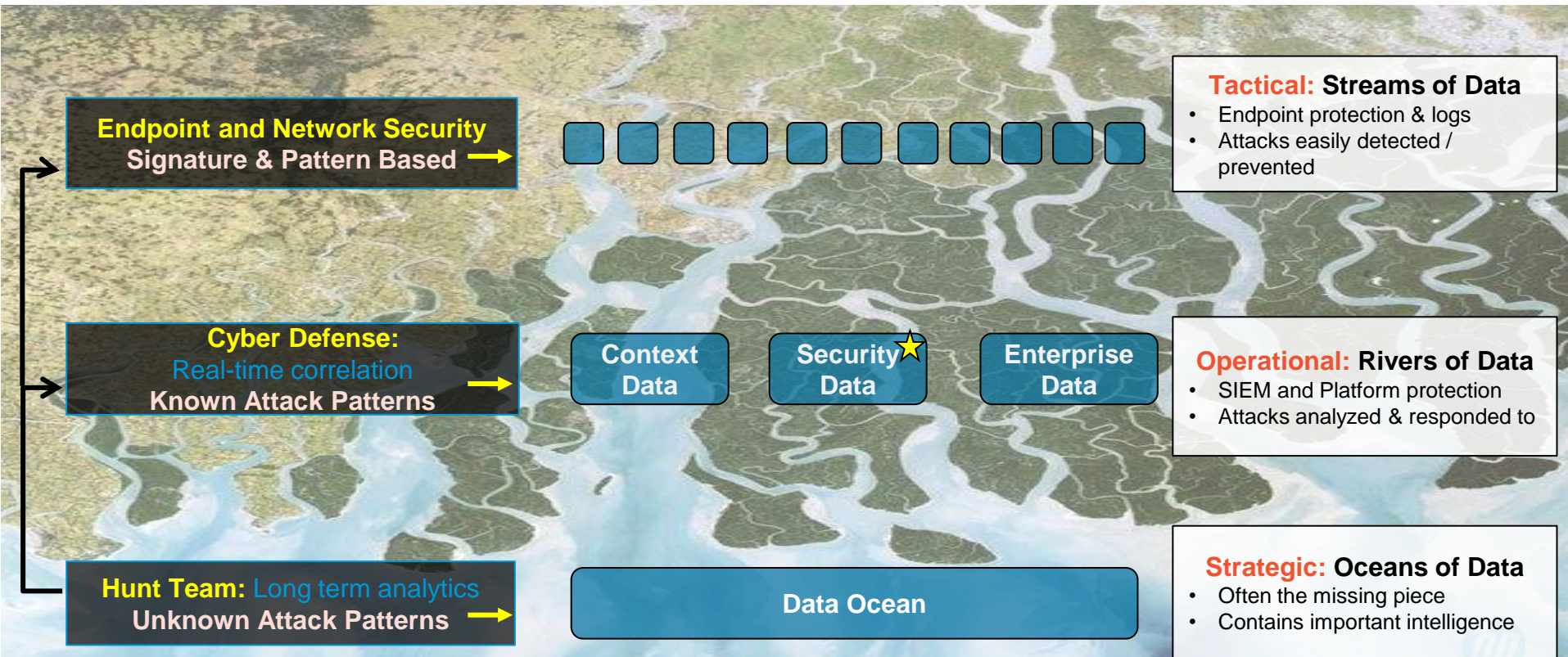


What Stopped Us From This Kind Of Analysis?



The Geography Of Security Detection Has Changed

Data flows in many ways – where should we catch and analyze it?



Visualization Of Big Data – Affinity Group

This example reveals a command and control infrastructure

Business Statement

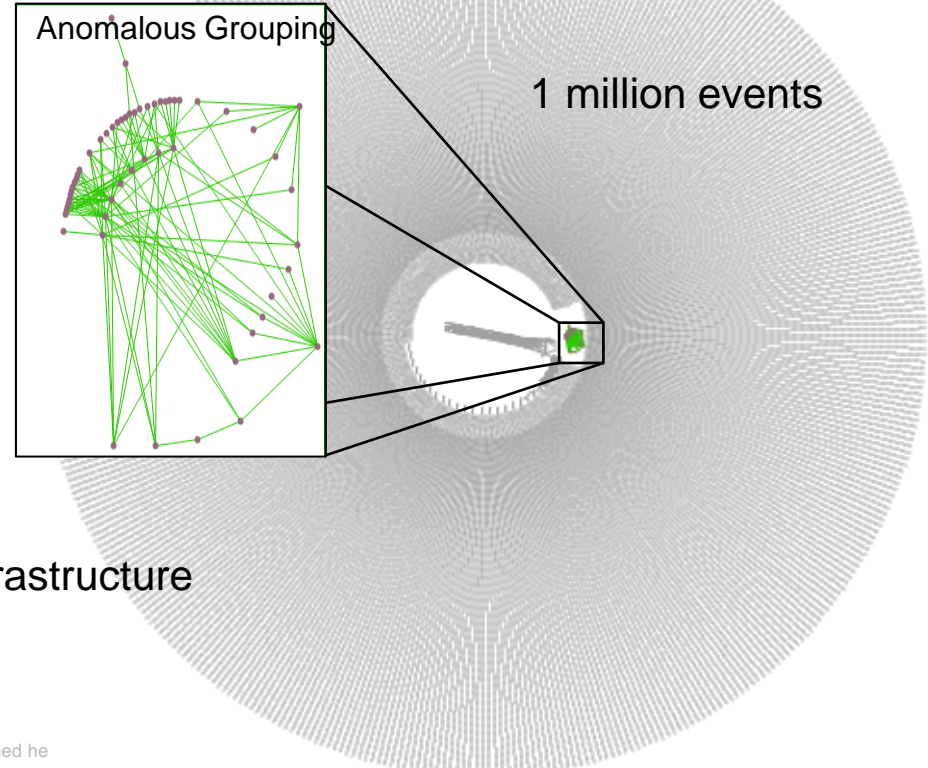
- Find **command and control infrastructure** in your enterprise

Analytics Statement

- Identify **affinity groups**
- Investigate anomalous groupings

Findings from Visualization

- Hierarchical, highly-resilient C&C infrastructure



Visualization Of Big Data – Scatterplot

This example reveals a low and slow scan

Business Statement

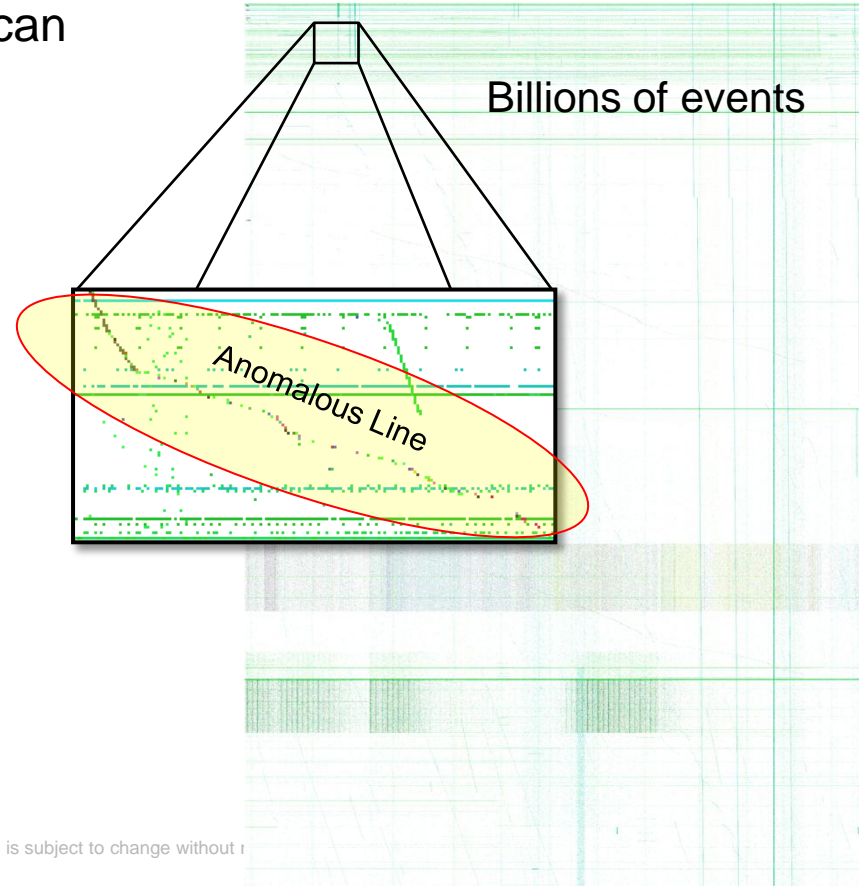
- Find sophisticated port scan activity (distributed, randomized)

Analytics Statement

- Plot multiple months of data on one scatterplot

Findings from Visualization

- Single multi-week scan from distributed, internal sources indicates advanced attacker



Visualization Of Big Data – Anomaly Chart

This example reveals inappropriate communication (**bottom 10 phenomenon**)

Business Statement

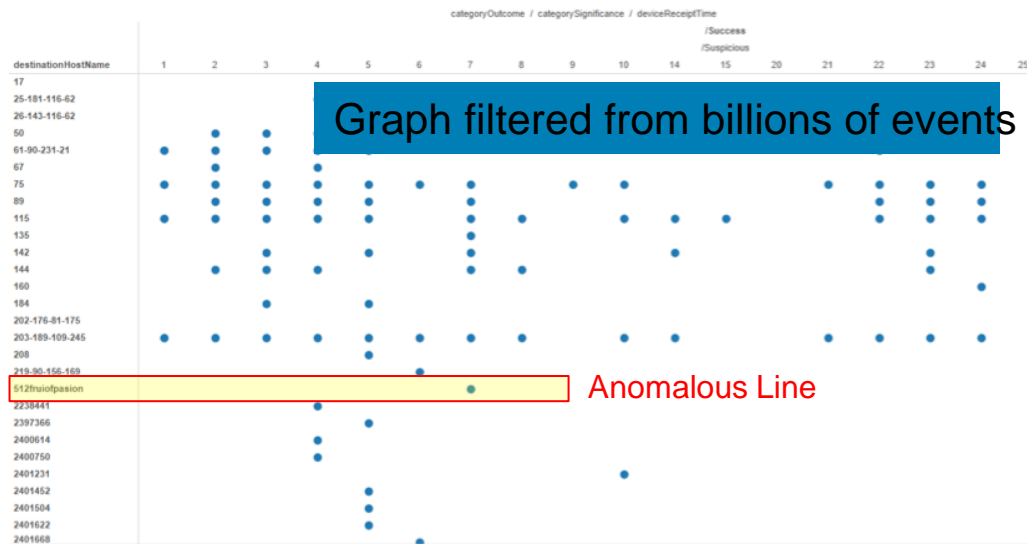
- Find servers talking to suspicious hosts outside the network

Analytics Statement

- Plot all suspicious successful communications and review

Findings from Visualization

- A host communicated w/ suspicious external website
- Unique in that no other host in the environment has ever talked to this external website



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)

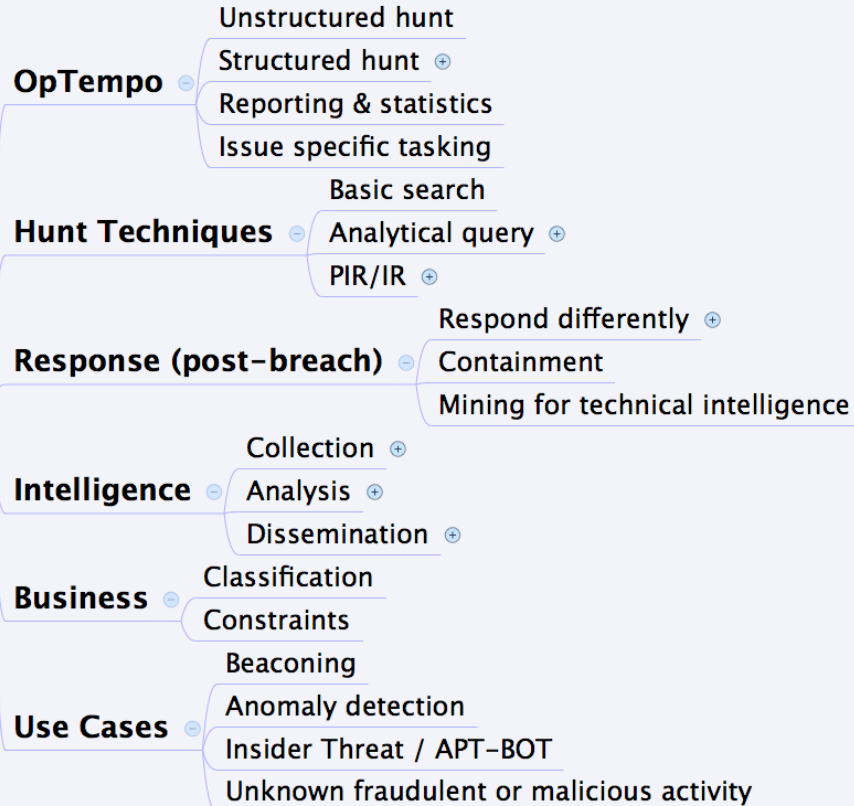
A new market adversary



Research → Infiltration → Discovery → Capture → Exfiltration

Hunt Team - The Way To Operationalize Analytics

Process



Your Hunt Team Needs A 2-Sided Skill Set

Roles and Personas

Security Specialist:

- The “go to” person to get to the bottom of any major security incidents and would be responsible for actively hunting for indicators of breach
- This person understand and researched hyper-current attacker tactics, techniques and procedures

Data Scientist:

- Knowledgeable to run specialized queries. Tasked to regularly find interesting anomalies or affinities in the data to review with the security specialist.
- This person optimizes tooling/searches, finding patterns that can increase risk probability factors and finding common patterns in attacks.

Security



Data Science



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 insider threats

Viewer

IDOL
 Social Media Threats
 Presales Engineers - Recent Activity
 Social Media Threats
 Correlated
 Last 5 Minutes

Active Channel: Social Media Threats Total Events

Start Time: 14 Feb 2013 06:47:00 PST Very High
End Time: 14 Feb 2013 07:48:00 PST High
Filter: (Type = "Correlation" And (Name StartsWith "Social" Or Name StartsWith "Potential" Or Name StartsWith "IDOL")) Medium
Low
Very Low

Inline Filter: No Filter

Radar

End Time	Device Product	Name	Sentiment	Social Media Website
14 Feb 2013 07:47:41 PST	ArcSight	Social Media - Hacktivist (DDOS) Threat	Negative	http://twitter.com/hakdplnt/statuses/301054906566066177
14 Feb 2013 07:47:41 PST	ArcSight	Social Media - Insider Threat	Negative	http://www.glassdoor.com/Reviews/Employee-Review-ArcSight-RVW2360458
14 Feb 2013 07:47:41 PST	ArcSight	Social Media - Hacktivist Threat	Negative	http://twitter.com/hakdplnt/statuses/301085122676002816
14 Feb 2013 07:47:41 PST	ArcSight	Social Media - Hacktivist Threat	Negative	http://twitter.com/hakdplnt/statuses/301061389127122945
14 Feb 2013 07:47:41 PST	ArcSight	Social Media - Hacktivist Threat	Negative	http://twitter.com/hakdplnt/statuses/301054906566066177
14 Feb 2013 07:47:41 PST	ArcSight	Social Media - Hacktivist Threat	Negative	http://twitter.com/YourAnonNews/statuses/299182747463872512
14 Feb 2013 07:47:41 PST	ArcSight	Social Media - Hacktivist Threat	Negative	http://twitter.com/YourAnonNews/statuses/299159456149815296



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

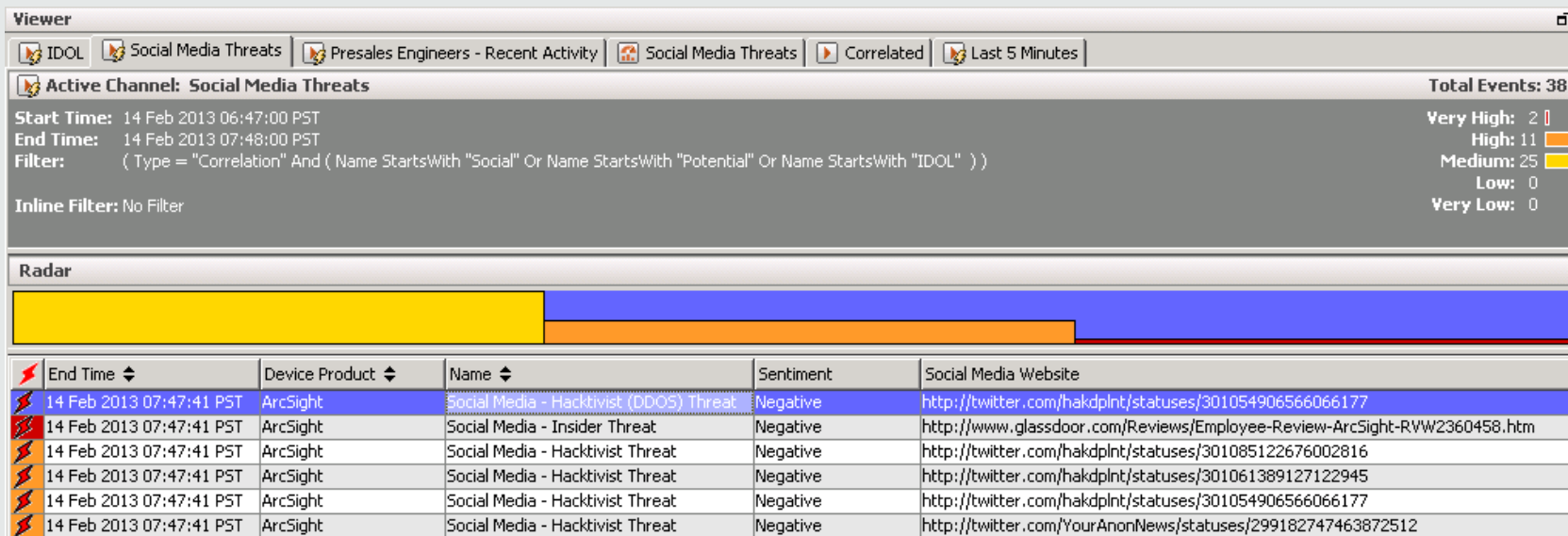
 Follow

Found a JS/iframe/vulnerable server at 10.10.10.120

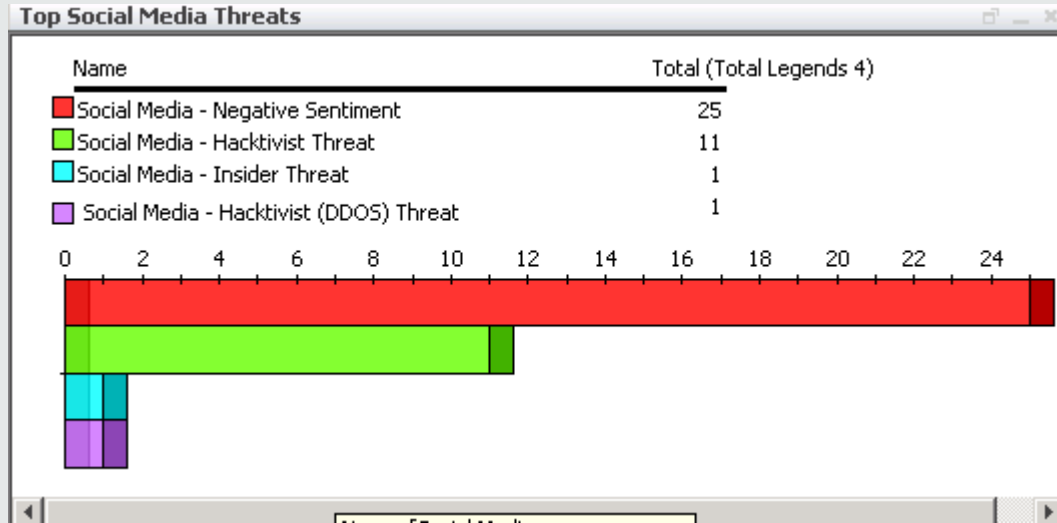
 Reply  Retweet  Favorite  More



Social media monitoring for hacktivist threats



Social media monitoring for hacktivist threats



Data loss monitoring in-action (Internal Threats)

Viewer

Potential Data Loss Correlations MS Exchange Events IDOL CEF Events Data Loss Dashboard

Active Channel: Potential Data Loss Correlations

Start Time: 2 Sep 2012 15:00:00 PDT

End Time: 5 Sep 2012 07:00:00 PDT

Filter: (Type = "Correlation" And Name StartsWith "IDOL")

Inline Filter: No Filter

Radar

Manager Receipt Time ↑ 1	Name ↓	Source User Name	Destination User Name	Message Id
2 Sep 2012 15:29:30 PDT	IDOL - Potential loss of Mergers data - Proximity: 57.02	Jameson Jones	peter.chambliss@gmail.com ...	347122d0de8c9a953cb2b8f877eea7d7
2 Sep 2012 15:29:30 PDT	IDOL - Potential loss of Research data - Proximity: 51.15	Jameson Jones	peter.chambliss@gmail.com ...	347122d0de8c9a953cb2b8f877eea7d7
2 Sep 2012 15:29:30 PDT	IDOL - Potential loss of HR data - Proximity: 60.08	Jameson Jones	peter.chambliss@gmail.com ...	c21aa08652ecad0b616f8a07f8b2c5fc



Conclusions

- Big Data Analytics coming to a SOC near you!
- Will enhance (but not replace) SIEM technology
- Will be leveraged for network, user, and fraud monitoring
- Will become more real time and predictive
- Will increase need to hire resources trained in data analytics & discovery

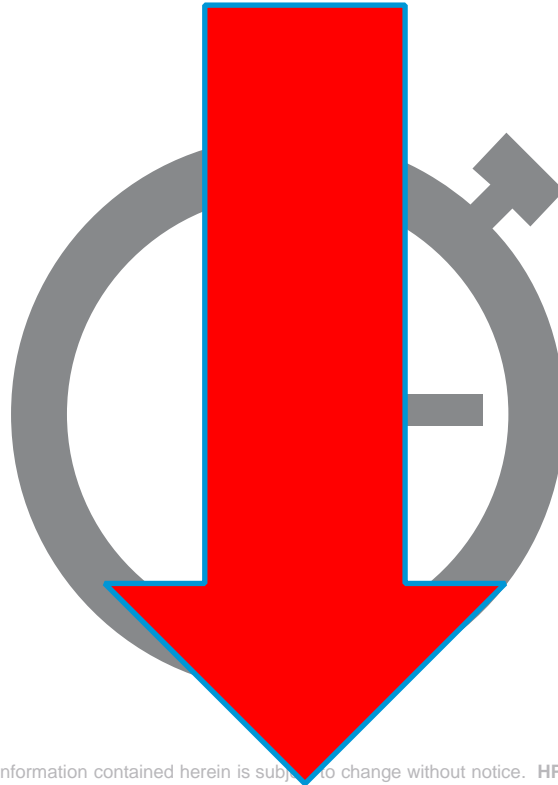
The Security Industry Is Not Catching Enough Bad Guys

Most enterprises remain challenged with missing critical breaches.

229 Days

is the median duration of
how long breaches were
present before discovery in
2013

(M-Trends Report)



100%

of business networks
have traffic going to
known malware hosting
websites

(Cisco 2014 Annual Security Report)



Blended Capability



ENTERPRISE SECURITY

Universal Log Management



Insider Threat



Data Privacy & Data Loss Monitoring



Perimeter & Network Security



Advanced Persistent Threat



Application & Transaction Monitoring



Software Security Assurance (SSA)



Compliance & Risk Management



Thank you!



Mike.loginov@hp.com

