RSACONFERENCE2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

Good Guys vs. Bad Guys. Using Big Data to Counteract Advanced Threats

SESSION ID: SP03-T08

Joe Goldberg

Chief Security Evangelist
Splunk

Security Presentation Template

= Scare them ✚ Unscare them

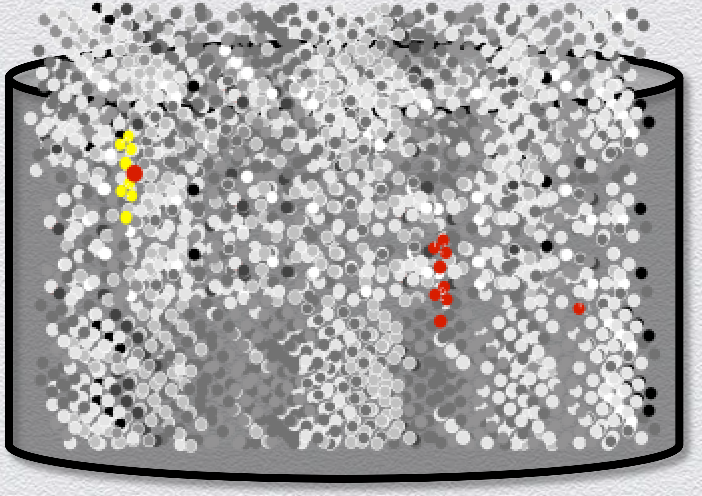
Security Presentation Template

=

Advanced Threats

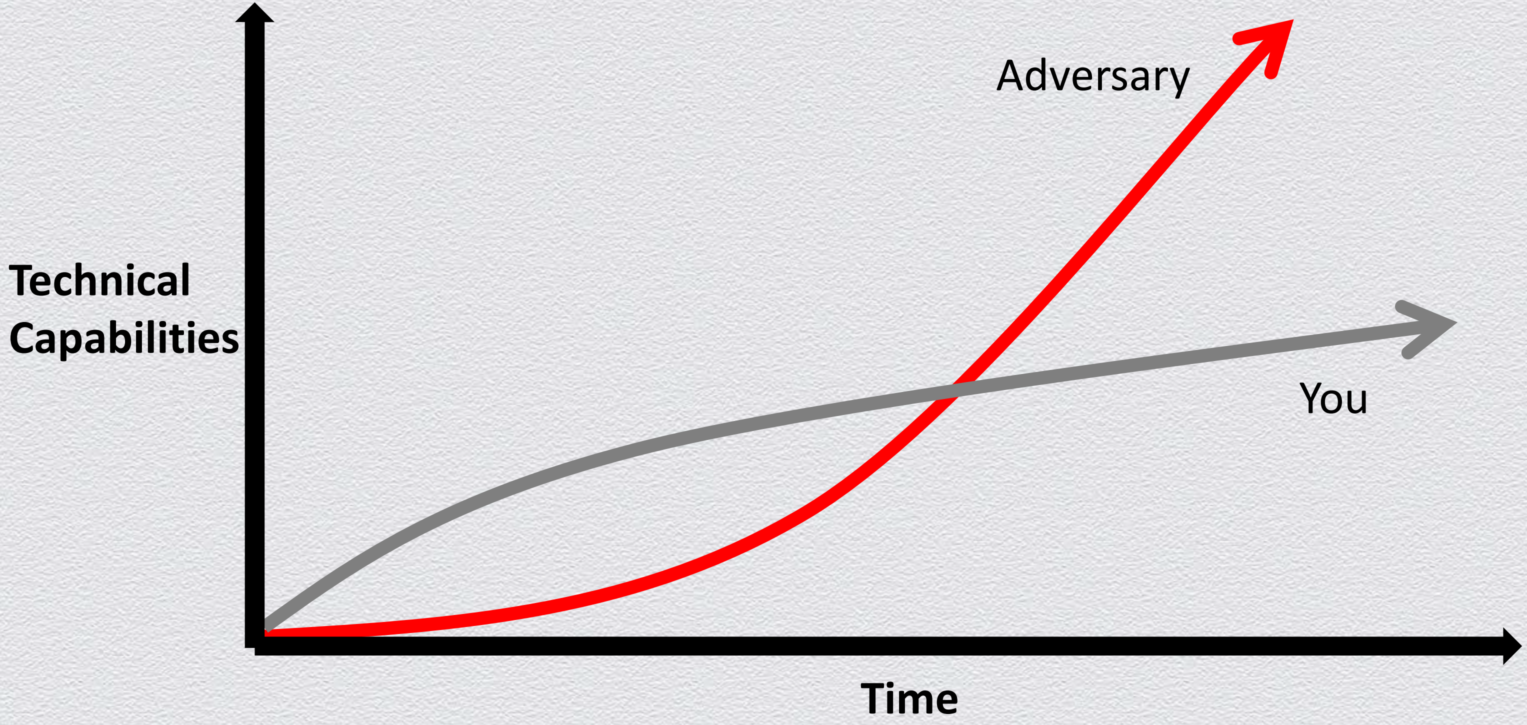
+

Big Data



Here Comes the Scary Part…..

Advanced Threats Outpace the Defenders



splunk>

#RSAC

RSACONFERENCE2014

Advanced Threats Are Hard to Detect

100%

Valid credentials were used

243

Median # of days before detection

40

Average # of systems accessed

63%

Of victims were notified by external entity

Source: Mandiant M-Trends Report 2012 and 2013

Advanced Threat Pattern – Not Signature Based

Infiltration	Back Door	Recon	Data Gathering	Exfiltration
Phishing or web drive-by. Email has attached malware or link to malware	Malware installs remote access toolkit(s)	Malware obtains credentials to key systems and identifies valuable data	Data is acquired and staged for exfiltration	Data is exfiltrated as encrypted files via HTTP/S, FTP, DNS

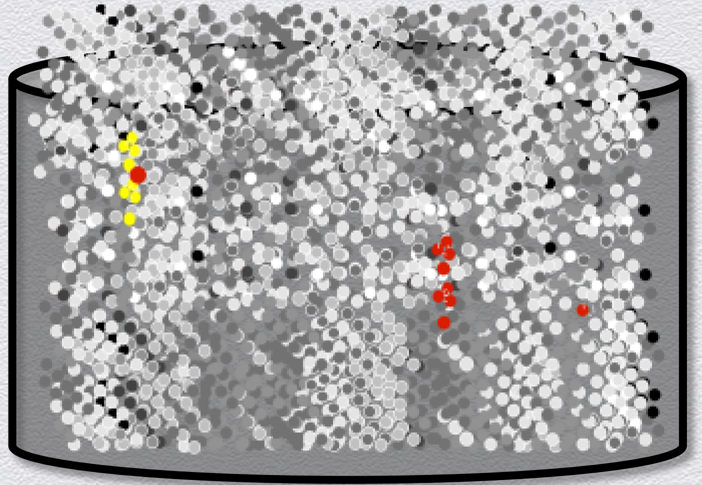
Traditional SIEMs Miss The Threats

- Limited view of security threats. Difficult to collect all data sources. Costly, custom collectors. Datastore w/schema.
- Inflexible search/reporting hampers investigations and threat detection
- Scale/speed issues impede ability to do fast analytics
- Difficult to deploy and manage; often multiple products

Better Defensive Cybersecurity Tools Needed

Here Comes The Solution

Big Data



Big Data is Used Across IT and the Business

App Mgmt	IT Ops	Security	Compliance	Fraud	Business Intelligence

Big Data

“Big Data” Definition

- Wikipedia: Collection of data sets so large and complex that it becomes difficult to process using database management tools
- Gartner: The Three Vs
  - Data volume
  - Data variety
  - Data velocity
- Security has always been a Big Data problem; now it has a solution

Machine Data / Logs are Big Data

Web Proxy

2013-08-09 16:21:38 10.11.36.29 98483 148 TCP_HIT 200 200 0 622 - - OBSERVED GET www.neverbeenseenbefore.com HTTP/1.1 0 "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; InfoPath.1; MS-RTC LM 8; .NET CLR 1.1.4322; .NET CLR 3.0.4506.2152;) User John Doe,"

Endpoint Logs

20130806041221.000000Caption=ACME-2975EB\Administrator Description=Built-in account for administering the computer/domainDomain=ACME-2975EB InstallDate=NULLLocalAccount = IP: 10.11.36.20 TrueName=Administrator SID =S-1-5-21-1715567821-926492609-725345543 500SIDType=1 Status=Degradedwmi_ type=UserAccounts

Authentications

08/09/2013 16:23:51.0128event_status="(0)The operation completed successfully. "pid=1300 process_image="\John Doe\Device\HarddiskVolume1\Windows\System32\neverseenbefore.exe“ registry_type ="CreateKey"key_path="\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ Printers Print\Providers\ John Doe-PC\Printers\{}\ NeverSeenbefore" data_type""

Anti-virus

Aug 08 06:09:13 acmesep01.acmetech.com Aug 09 06:17:24 SymantecServer acmesep01: Virus found,Computer name: ACME-002,Source: Real Time Scan,Risk name: Hackertool.rootkit,Occurrences: 1,C:/Documents and Settings/smithe/Local Settings/Temp/evil.tmp,"""",Actual action: Quarantined,Requested action: Cleaned, time: 2009-01-23 03:19:12,Inserted: 2009-01-23 03:20:12,End: 2009-01-23 03:19:12,Domain: Default,Group: My Company\ACME Remote,Server: acmesep01,User: smithe,Source computer: ,Source IP: 10.11.36.20

Big Data Analytics

"[Security teams need] an analytical engine to sift through massive amounts of real-time and historical data at high speeds to develop trending on user and system activity and reveal anomalies that indicate compromise."

Security for Business Innovation Council report, "When Advanced Persistent Threats Go Mainstream,"

"The core of the most effective [advanced threat] response appears to be a new breed of security analytics that help quickly detect anomalous patterns -- basically power tools in the hands of a new and important sub-category of data scientists: the security analytics expert.."

Chuck Hollis
VP – CTO, EMC Corporation

Step 1: Collect *ALL* The Data in One Location

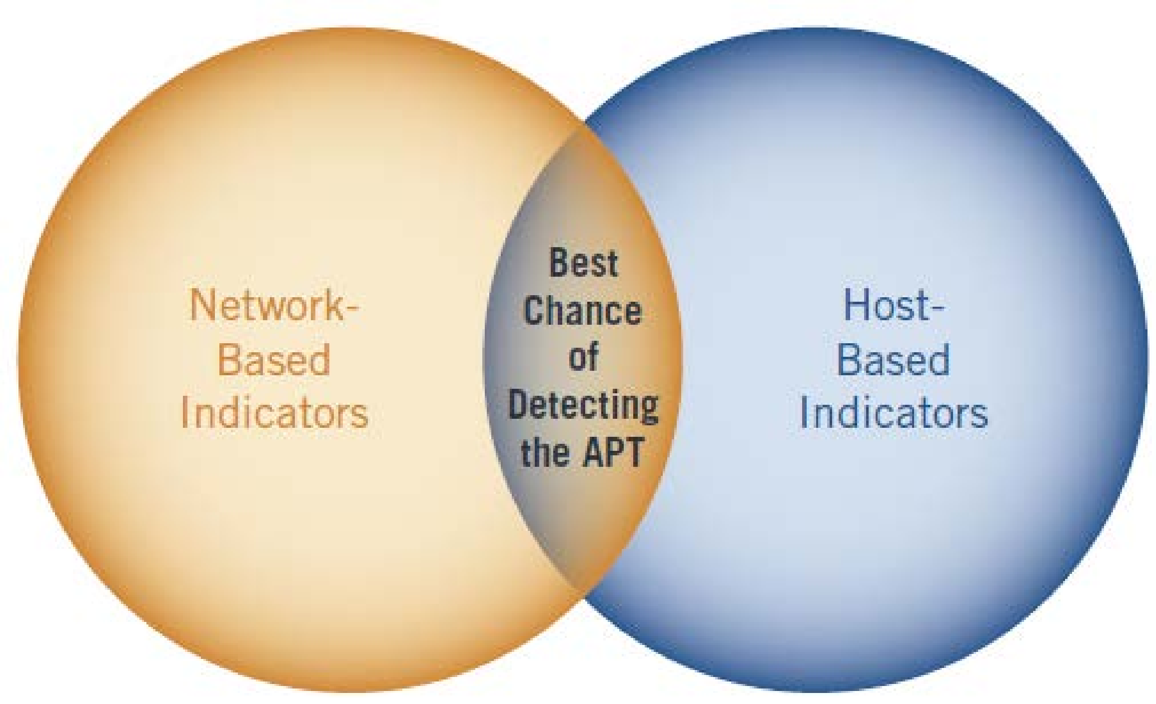
- Databases
- Email
- Web
- Desktops
- Servers
- DHCP/ DNS
- Network Flows
- Hypervisor
- Badges
- Storage
- Mobile
- Custom Apps
- Service Desk
- Industrial Control / HVAC
- Call Records

Traditional SIEM

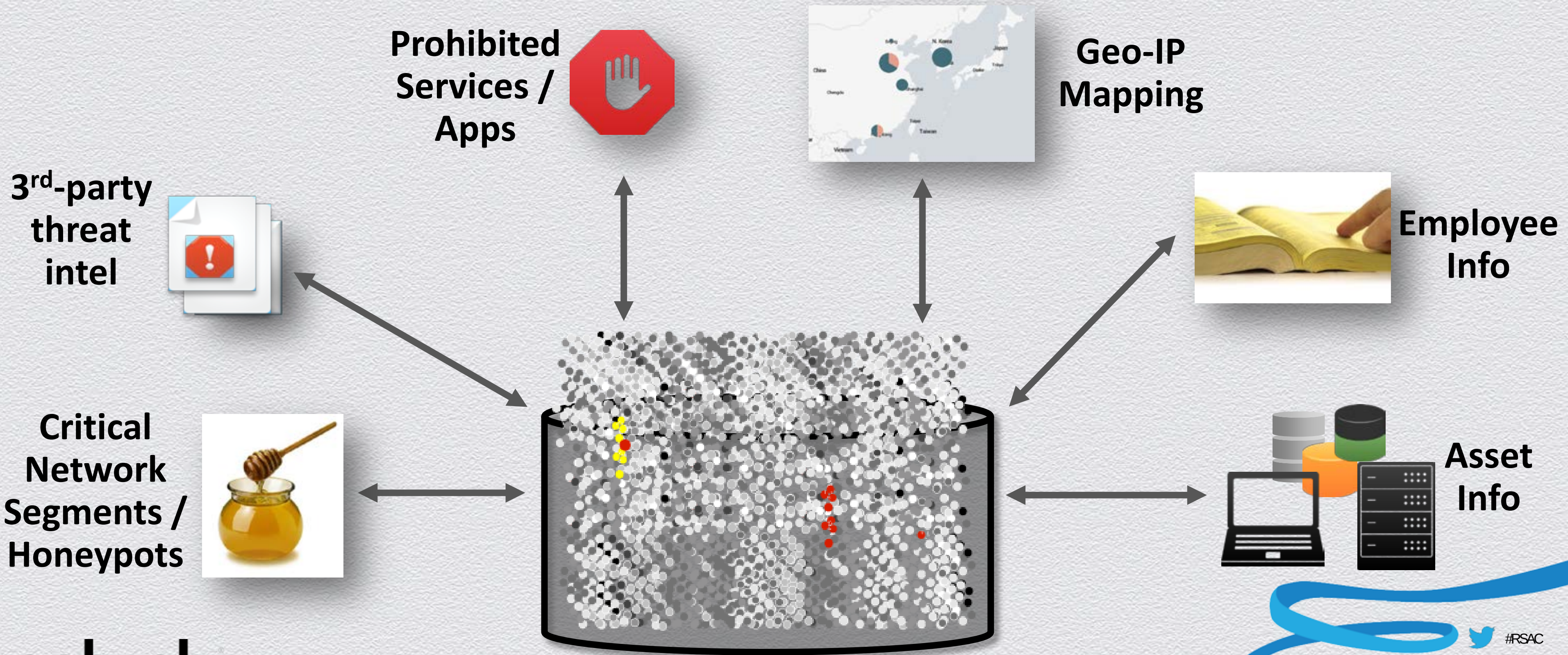
- Firewall
- Authentication
- Vulnerability Scans
- Intrusion Detection
- Data Loss Prevention
- Anti-Malware

Need Both Network and Endpoint

And Inbound/Outbound!



Enrich Indexed Data with External Data / Lookups

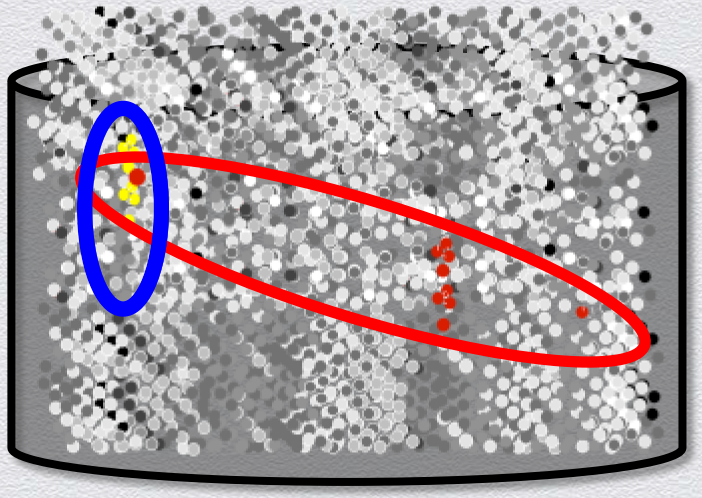


Step 2: Identify Threat Activity

- What's the M.O. of the attacker? (think like a criminal)
- What/who are the most critical assets and employees?
- What minute patterns/correlations in 'normal' IT activities would represent 'abnormal' activity?
- What in my environment is different/new/changed?
- What is rarely seen or standard deviations off the norm?

Big Data Solution

Big Data Architecture



Data Inclusion Model

- ✓ All the original data from any source
- ✓ No database schema to limit investigations/detection
- ✓ Lookups against external data sources
- ✓ Search & reporting flexibility
  - ✓ Advanced correlations
  - ✓ Math/statistics to baseline and find outliers/anomalies
- ✓ Real-time indexing and alerting
- ✓ “Known” and “Unknown” threat detection
- ✓ Scales horizontally to 100 TB+ a day on commodity H/W
- ✓ One product, UI, and datastore

Big Data Solutions

- Flat file datastore (not database), distributed search, commodity H/W
- More than a SIEM; can use outside security/compliance

Incident investigations/forensics, custom reporting, correlations, APT detection, fraud detection

Sample Correlation of *Unknown* Threats

Example Correlation - Spearphishing

Email Server

User Name

2013-08-09T12:40:25.475Z,,exch-hub-den-01,,exch-mbx-cup-00,,,STOREDRIVER,DELIVER,79426,<20130809050115.18154.11234@acme.com>,johndoe@acme.com,,685191,1,,,hacker@neverseenbefore.com, Please open this attachment with payroll information,,,2013-08-09T2

Rarely seen email domain

Web Proxy

Rarely visited web site

20 .36.29 98483 148 TCP_HIT 200 200 0 622 - - OBSERVED GET www.neverbeenseenbefore.com HTTP/1.1 0 "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; InfoPath.1; MS-RTC LM 8;.NET CLR 3.0.4506.2152;) User John Doe,"

User Name

Endpoint Logs

User Name

08/09/2013 16:23:51.0128event_status="(0)The operation completed successfully. "pid=1300 process_image="\John Doe\Device\HarddiskVolume1\Windows\System32\neverseenbefore.exe" registry_type ="CreateKey"key_path="\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ Printers Print\Providers\ John Doe-PC\Printers\{}\ Ne e""

Rarely seen service

All three occurring within a 24-hour period

Fingerprints of an Advanced Threat

What to Look For	Why	Data Source	Attack Phase
Rarely seen registry, service, DLL. Or they fail hash checks.	Malware or remote access toolkit	OS	Back door
Account creation or privilege escalation without corresponding IT service desk ticket	Creating new admin accounts	AD/ Service Desk logs	Lateral movement
A non-IT machine logging directly into multiple servers. Or chained logins.	Threat accessing multiple machines	AD /asset info	Lateral movement
For single employee: Badges in at one location, then logs in countries away	Stealing credentials	Badge/ VPN/ Auth	Data gathering
Employee makes standard deviations more data requests from file server with confidential data than normal	Gathering confidential data for theft	OS	Data gathering
Standard deviations larger traffic flows (incl DNS) from a host to a given IP	Exfiltration of info	NetFlow	Exfiltration

Step 3: Remediate and Automate

- Where else in my environment do I see the "Indicators of Compromise" (IOC)?
- Remediate infected machines
- Fix weaknesses, including employee education
- Turn IOC into a real-time search for future threats

Security Realities…

- Big Data is only as good as the data in it and people behind the UI
- No replacement for capable practitioners
- Put math and statistics to work for you
- Encourage IT Security creativity and thinking outside the box
- Fine tuning needed; always will be false positives

Recap

- **Step 1:** Collect *ALL* The Data in One Location
- **Step 2:** Identify Threat Activity
- **Step 3:** Remediate and Automate

About Splunk

- Big Data platform for ingesting machine data; desktop to 100+ TB/day
- Many use cases within security; also outside security
- Over 6500 customers total; 2800+ security customers
- Free download and tutorial at www.splunk.com

RSA CONFERENCE 2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Questions?

RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Thank You!

jgoldberg@splunk.com