

Introducing Splunk Enterprise 6.2

Stefano Radaelli
Senior Sales Engineer



Splunk Company Overview

Company

- Global HQs:
 - San Francisco
 - London
 - Hong Kong
- 1,300 employees globally
- Annual Revenue: \$302.6M (YoY +52%)
- NASDAQ: SPLK

Products

- Free trial to massive scale
- Splunk products:
 - Splunk Enterprise
 - Splunk Cloud
 - Hunk
 - Splunk MINT
 - Premium Apps

Customers

- 7,900+ customers
- Across 100 countries
- Small to large organizations
- 70+ of the Fortune 100
- Largest license:
 - 300+ Terabytes/day



Big Data Comes from Machines

Volume | Velocity | Variety | Variability

GPS,
RFID,
Hypervisor,
Web Servers,
Email, Messaging
Clickstreams, Mobile,
Telephony, IVR, Databases,
Sensors, Telematics, Storage,
Servers, Security Devices, Desktops

What Does Machine Data Look Like?

Sources



ORDER,2013-05-21T14:04:12.484,10098213,569281734,67.17.10.12,43CD1A7B8322,SA-2100

Order Processing



May 21 14:04:12.996 wl-01.acme.com Order 569281734 failed for customer 10098213. Exception follows: weblogic.jdbc.extensions.ConnectionDeadSQLException: weblogic.common.resourcepool.ResourceDeadException: Could not create pool connection. The DBMS driver exception was: [BEA][Oracle JDBC Driver]Error establishing socket to host and port: ACMEDB-01:1521. Reason: Connection refused

Middleware Error

⌋

05/21 16:33:11.238 [CONNEVENT] Ext 1207130 (0192033): Event 20111, CTI Num:ServID:Type 0:19:9, App 0, ANI T7998#1, DNIS 5555685981, SerID 40489a07-7f6e-4251-801a-13ae51a6d092, Trunk T451.16

Care IVR

05/21 16:33:11.242 [SCREENPOPEVENT] SerID 40489a07-7f6e-4251-801a-13ae51a6d092 CUSTID 10098213

05/21 16:37:49.732 [DISCEVENT] SerID 40489a07-7f6e-4251-801a-13ae51a6d092



Twitter

{actor:{displayName:"Go Boys!!",followersCount:1366,friendCount:789,link:"http://dallascowboys.com/",location:{displayName:"Dallas, TX",objectType:"place"},objectType:"person",preferredUsername:"B0ysF@n80",statusesCount:6072},body:"Just bought this POS device from @ACME. Doesn't work! Called, gave up on waiting for them to answer! RT if you hate @ACME!!",objectType:"activity",postedTime:"2013-05-21T16:39:40.647-0600"}

Machine Data Contains Critical Insights

Sources



Order Processing



Middleware Error



Care IVR



Twitter

ORDER,2013-05-21T14:04:12.484, **Customer ID** 10098213, **Order ID** 569281734, 67.17.10.12, 43CD1A7B8322, **Product ID** SA-2100

May 21 14:04:12.996 wl-01.acme.com Order **Order ID** 569281734 failed for customer **Customer ID** 10098213. Exception follows: weblogic.jdbc.extensions.ConnectionDeadSQLException: weblogic.common.resourcepool.ResourceDeadException: Could not create pool **Customer ID**. The DBMS driver exception was: [BEA][Oracle JDBC Driver]Error establishing socket to host and port: ACMEDB-01:1521. Reason: Connection refused

05/21 16:33:11.238 [CONNEVENT] Ext 1207130 (0192033): Event 20111, CTI Num:ServID:Type **Time Waiting On Hold** 98#1, DNIS 5555685981, SerID 40489a07-7f6e-4251-801a-13ae51a6d092, trunk 1451.16

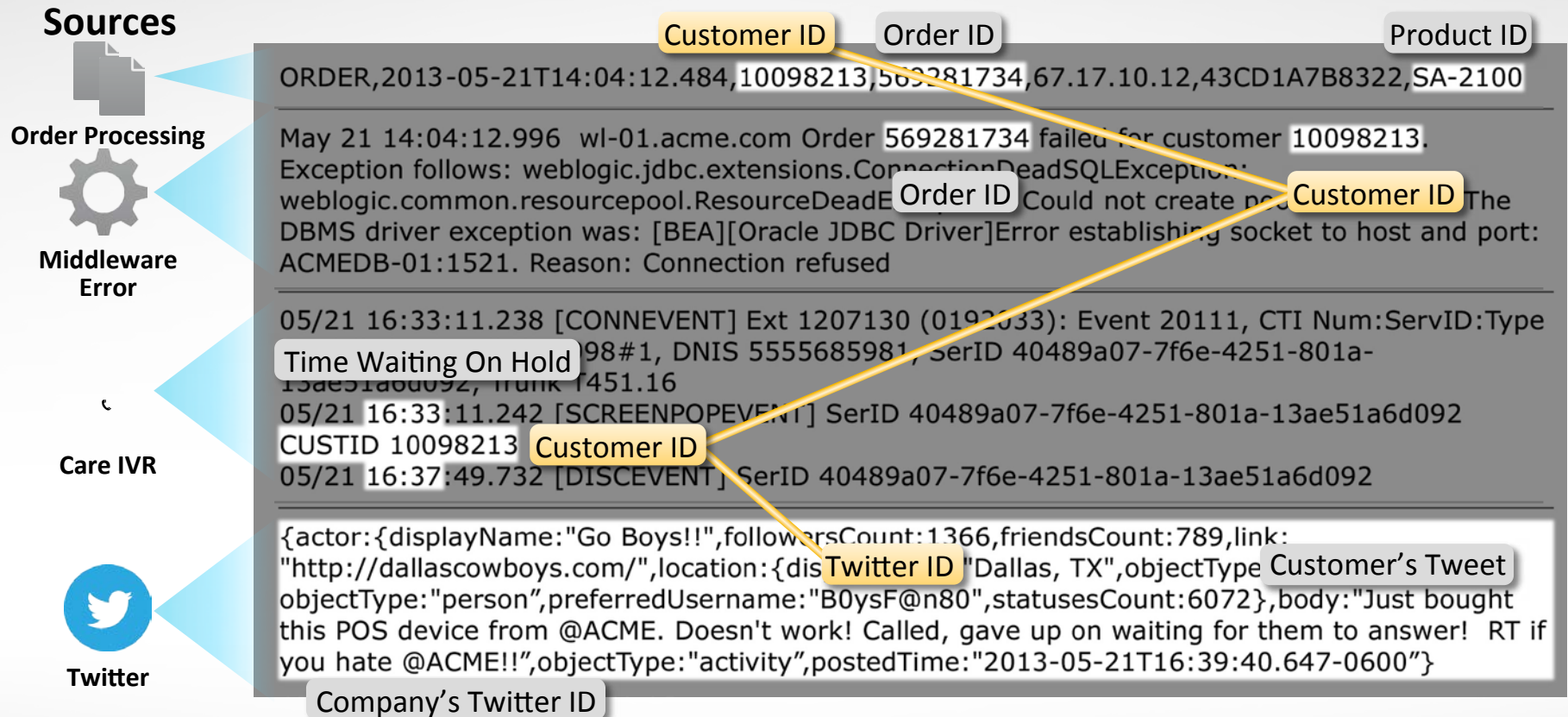
05/21 16:33:11.242 [SCREENPOPEVENT] SerID 40489a07-7f6e-4251-801a-13ae51a6d092 CUSTID 10098213 **Customer ID**

05/21 16:37:49.732 [DISCEVENT] SerID 40489a07-7f6e-4251-801a-13ae51a6d092

```
{actor:{displayName:"Go Boys!!",followersCount:1366,friendsCount:789,link:"http://dallascowboys.com/",location:{disTwitter ID "Dallas, TX",objectType Customer's Tweet objectType:"person",preferredUsername:"B0ysF@n80",statusesCount:6072},body:"Just bought this POS device from @ACME. Doesn't work! Called, gave up on waiting for them to answer! RT if you hate @ACME!!",objectType:"activity",postedTime:"2013-05-21T16:39:40.647-0600"}
```

Company's Twitter ID

Machine Data Contains Critical Insights

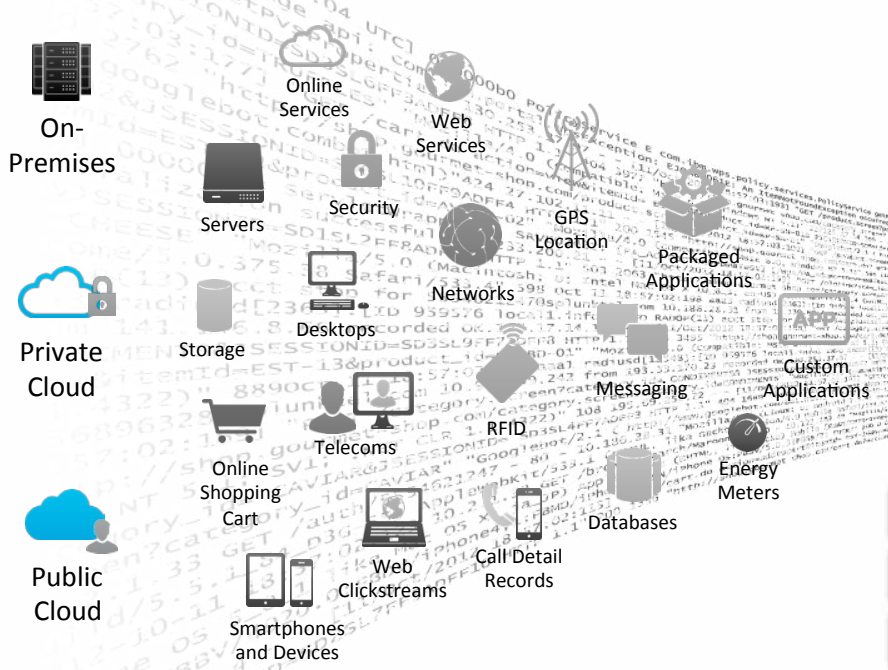


splunk

Make machine data accessible,
usable and valuable to everyone.

Industry Leading Platform For Machine Data

Machine Data: Any Location, Type, Volume



Answer Any Question



Ad hoc search



Monitor and alert



Report and analyze



Custom dashboards



Developer Platform

splunk > enterprise

splunk > cloud

Platform Support (Apps / API / SDKs)

Enterprise Scalability

Universal Indexing

Industry Leading Platform For Machine Data

Machine Data: Any Location, Type, Volume

Answer Any Question

On-Premises

Private Cloud

Public Cloud

Online

Servers

Networks

Desktops

Storage

Smartphones and Devices

Web Services

Packaged Applications

Me

Energy Meters

Databases

Call Detail Records

Web

Shopping Cart

Ad hoc search

Monitor and alert

Report and analyze

Custom dashboards

Developer platform

Any amount, any location, any source

Schema-on-the-fly

Universal indexing

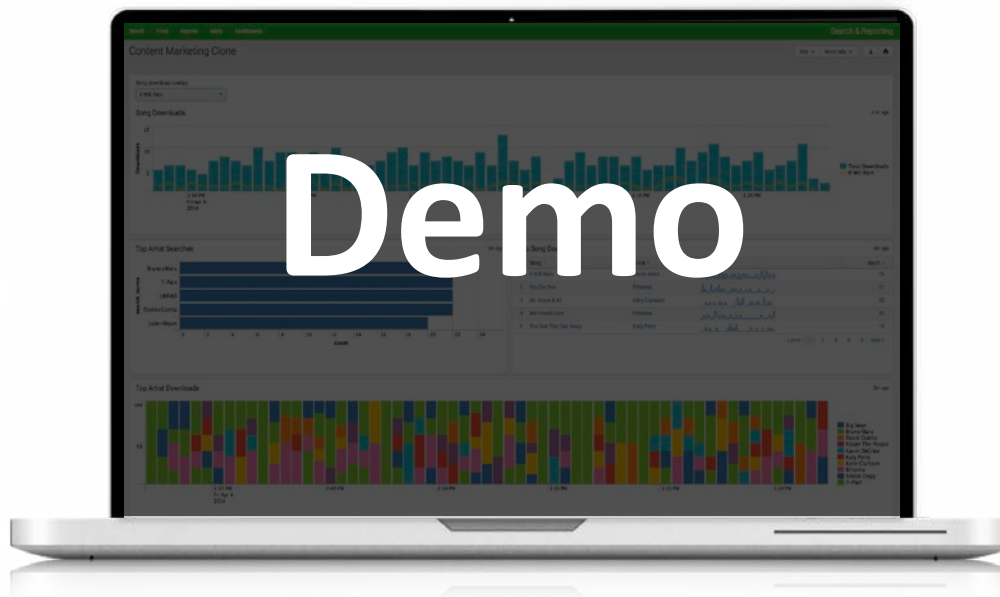
No back-end RDBMS

No need to filter data

Platform Support (Apps / API / SDKs)

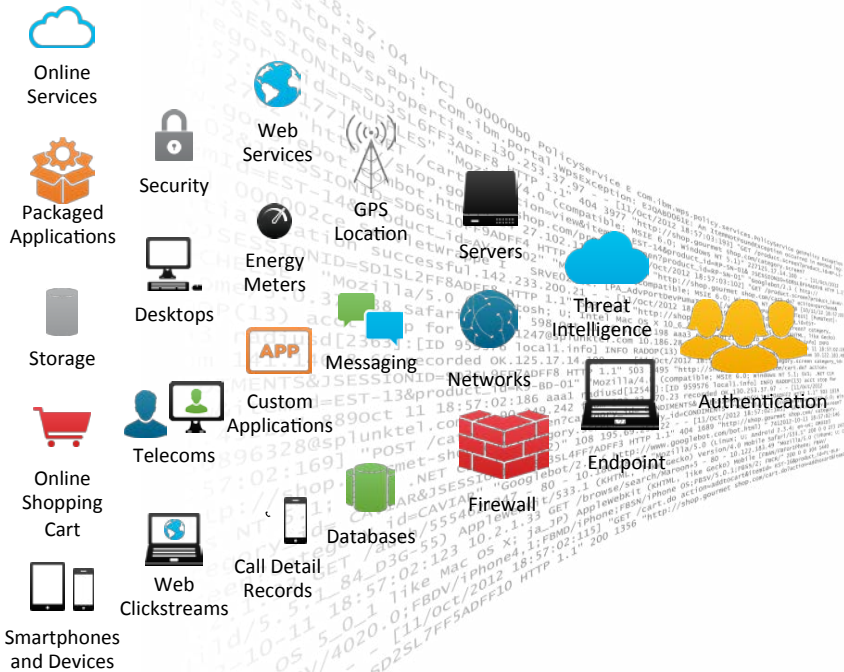
Enterprise Scalability

Universal Indexing



Security Use Case

Security Intelligence



Ad hoc search



Monitor and alert



Report and analyze



Custom dashboards



Developer Platform



External Lookups

Asset & CMDB



Employee Info



Threat Intelligence



Applications



Data Stores



Big Data Platform: Insight for Business Risk




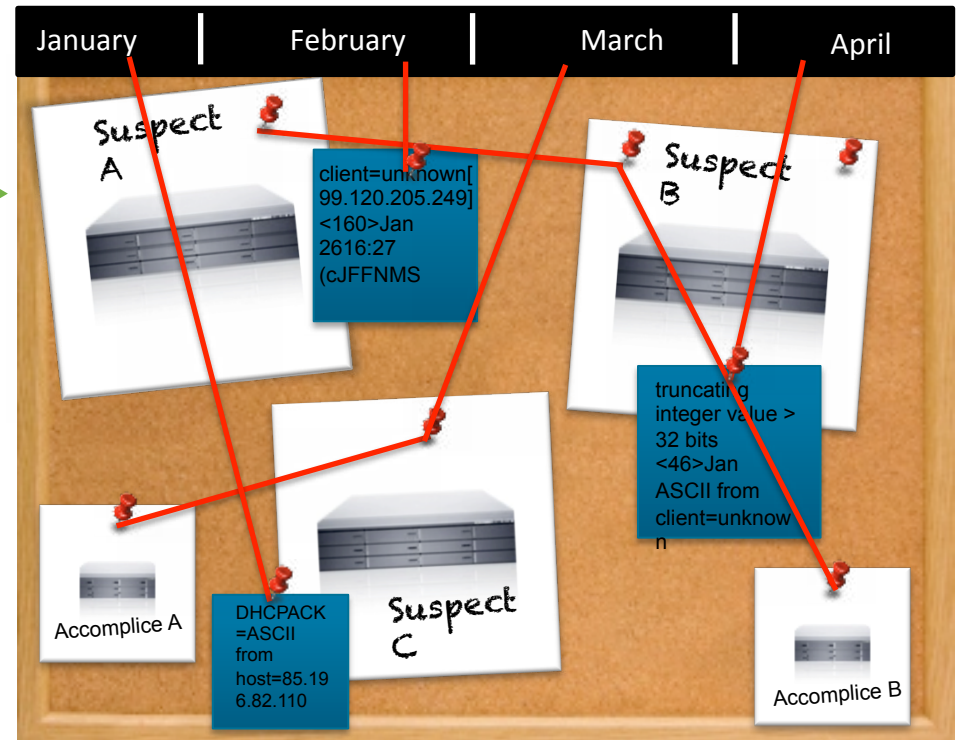
Business Risk and Security

The Business Risk and Security section displays five key Splunk dashboards:

- Security & Compliance:** Shows a world map with red markers indicating security events.
- IT Operations Management:** Displays a list of system health and performance metrics.
- Business Analytics:** Features a line graph showing trends over time.
- Web Intelligence:** Includes pie charts and bar graphs for website performance analysis.
- Application Monitoring:** Shows a bar chart for application performance metrics.

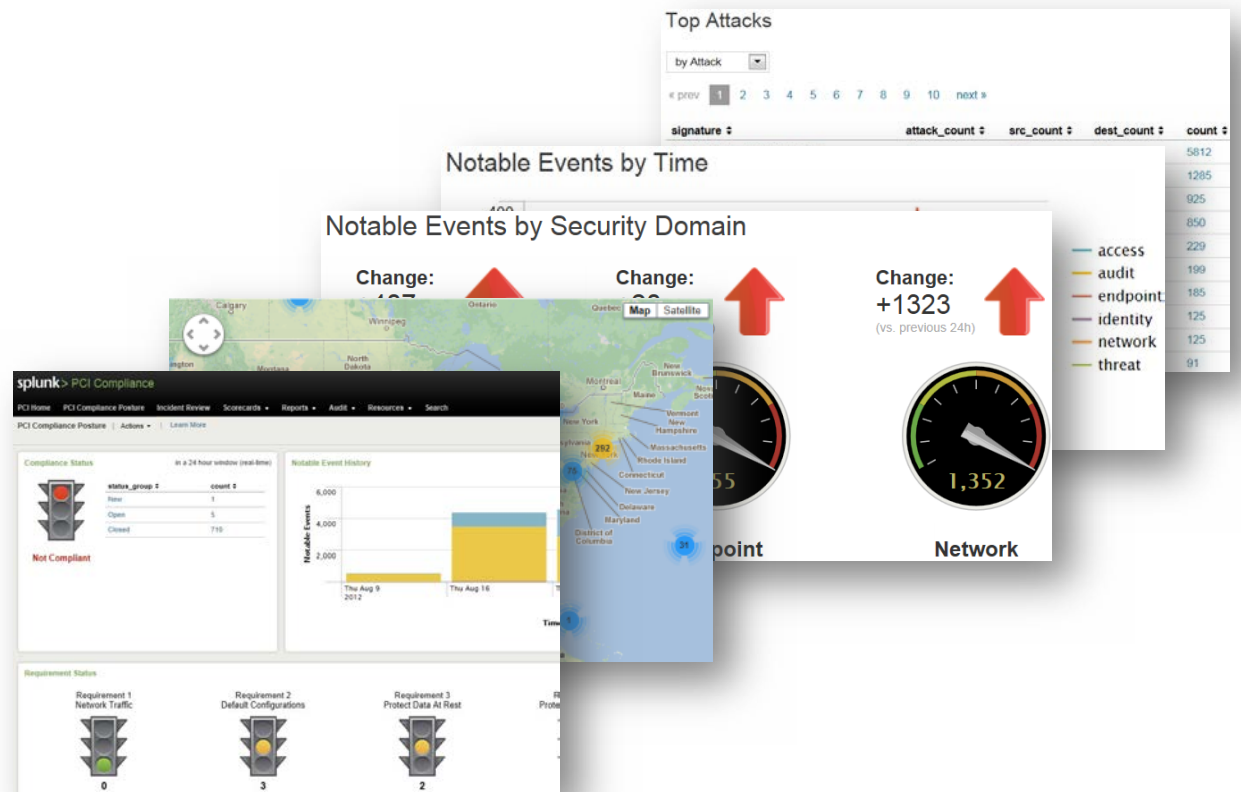
Case #1 - Incident Investigation/Forensics

- Often initiated by alert in another product
- May be a “cold case” investigation requiring machine data going back months 
- Need all the original data in one place and a fast way to search it to answer:
 - What happened and was it a false positive?
 - How did the threat get in, where have they gone, and did they steal any data?
 - Has this occurred elsewhere in the past?
- Take results and turn them into a real-time search/alert if needed



Case #2 – Security/Compliance Reporting

- Many types of visualizations
- Easy to create in Splunk
 - Ad-hoc auditor reports
 - New incident list
 - Historical reports
 - SOC/NOC dashboards
 - Executive/auditor dashboards



Case #3 – Real-time Monitoring of *Known* Threats

Sources

Example Correlation – Data Loss



Windows Authentication

20130806041221.000000Caption=ACME-2975EB Administrator Description=Built-in account for administering the computer/domainDomain=ACME-2975EB InstallDate=NIUULocalAccount = IP 10.11.36.20 TrueName=Administrator SID =S-1-5-21-1 Default Admin Account 15543 50 Source IP Status=Degradedwmi_type=UserAccounts



Endpoint Security

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," Malware Found 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



Intrusion Detection

Aug 08 08:26:54 snort.acmetech.com {TCP} 10.11.36.20:5072 -> 10.11.36.26:443 itsec snort[18774]: [1:100000:3] [Classification: Potential Corp Source IP Correlation] Credit Card Number Detected in Clear Text [Priority: 2]: Data Loss



Time Range

All three occurring within a 24-hour period

Case #4 – Real-time Monitoring of *Unknown* Threats

Sources

Example Correlation - Spearphishing



Email Server

2013-08-09T12:40:25.475Z,,exch-hub-den-01,,exch-mbx-cup-00,,,STOREDRIVER,DELIVERED:79426.<20130809050115.18154.11234@acme.com>,johndoe@acme.com,,685 91,1,,
hacker@neverseenbefore.com , please open this attachment with payroll information,, ,

Rarely seen email domain

User Name



Web Proxy

2013-08-09T12:40:25.475Z 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;) Use John Doe"

Rarely visited web site

User Name



Endpoint
Logs

08/09/2013 16:00:23 User Name ..._nt_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="

Rarely seen service



Time Range

All three occurring within a 24-hour period

Case #4 – More Examples






Attack Phase	What Threat is Doing	What to Look For	Data Source
Lateral movement	Creating new admin accounts	Account creation without corresponding IT service desk ticket	AD/ Service Desk logs
Data gathering	Stealing credentials	For single employee: Badges in at one location, then logs in countries away	Badge/ VPN/ Auth
Data gathering	Gathering confidential data for theft	Employee makes standard deviations more data requests from file server with confidential data than normal	OS
Exfiltration	Exfiltration of info	Standard deviations larger traffic flows (incl DNS) from a host to a given IP	NetFlow

Case #5 – Insider Threat

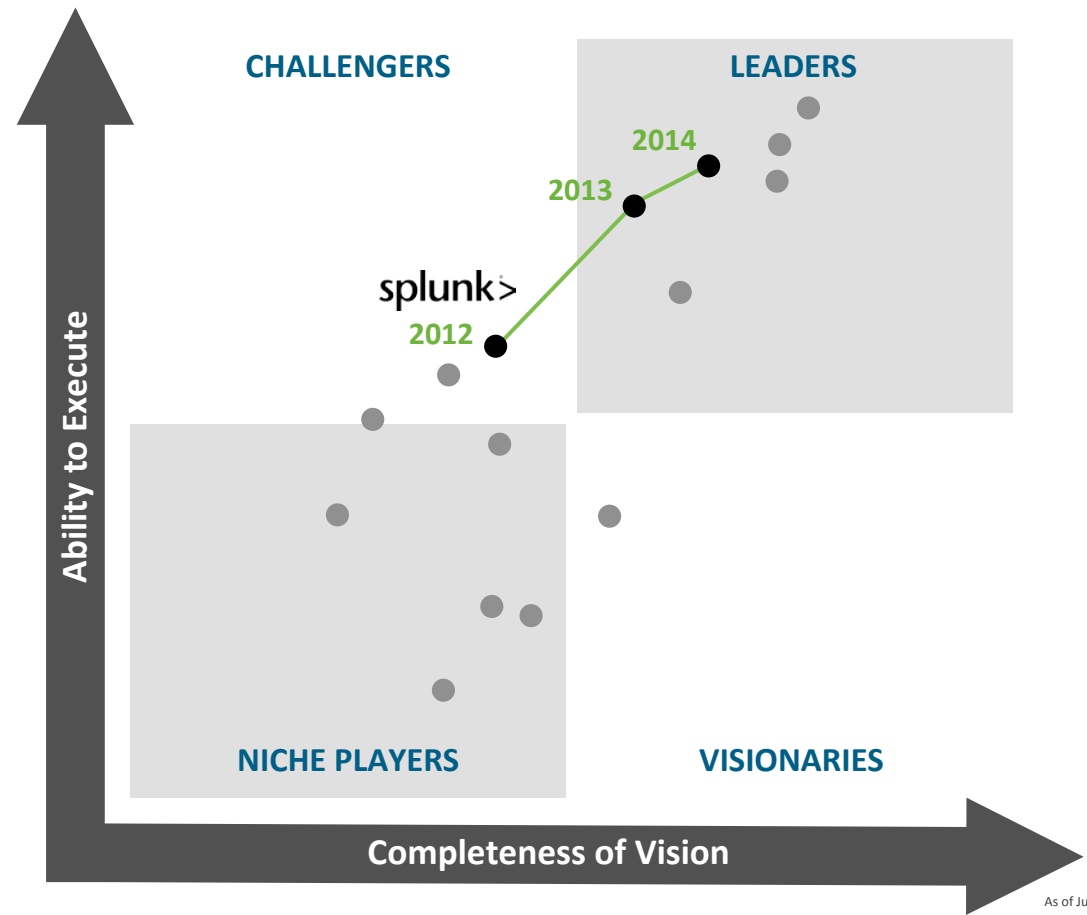
What To Look For	Data Source
Abnormally high number of file transfers to USB or CD/DVD	OS
Abnormally large amount of data going to personal webmail account or uploaded to external file hosting site	Email / web server
Unusual physical access attempts (after hours, accessing unauthorized area, etc)	Physical badge records / AD
Above actions + employee is on an internal watchlist as result of transfer / demotion / poor review / impending layoff	HR systems / above
User name of terminated employee accessing internal system	AD / HR systems

Case #6 – Fraud Detection

Sample Patterns of Fraud in Machine Data:

	Vertical	Type of Fraud	Pattern of fraud
	Financial Services	Account takeover	Many transactions between \$9-10k
	Healthcare	Physician billing	Physician billing for drugs outside their expertise area
	E-tailing	Account takeover	Many accounts accessed from one IP
	Telecom	Roaming abuse	Excessive roaming on partner network by unlimited use customers
	Online education	Student loan fraud	Student IP in “high-risk” country and student absent from classes & assignments

A 3-YEAR JOURNEY



As of June 2014

Industry Accolades



BEST SIEM SOLUTION

SC Magazine Awards, 2013



BEST ENTERPRISE SECURITY SOLUTION

SC Magazine Awards, Europe 2013 & US 2014



BEST SIEM

Information Security Magazine Readers' Choice Awards, 2013

Enterprise Security v3.2.1

“Defense-in-depth” Requires a New Strategy

Two types of analysis to fight today's threats

Traditional Monitoring for Known Events

- In the ‘wild’ but prevalent
- Uses vendor supplied signatures
- Generally caught by IDS/IPS, AV or firewall
- Reported to traditional SIEM

Statistical Analysis for Unknown Events

- Hidden in terabytes of ‘normal’ user activity
- Circumvents perimeter defenses
- Often uses HTTP to communicate
- Much harder to find without advanced analytics

Enterprise Security Content Focus

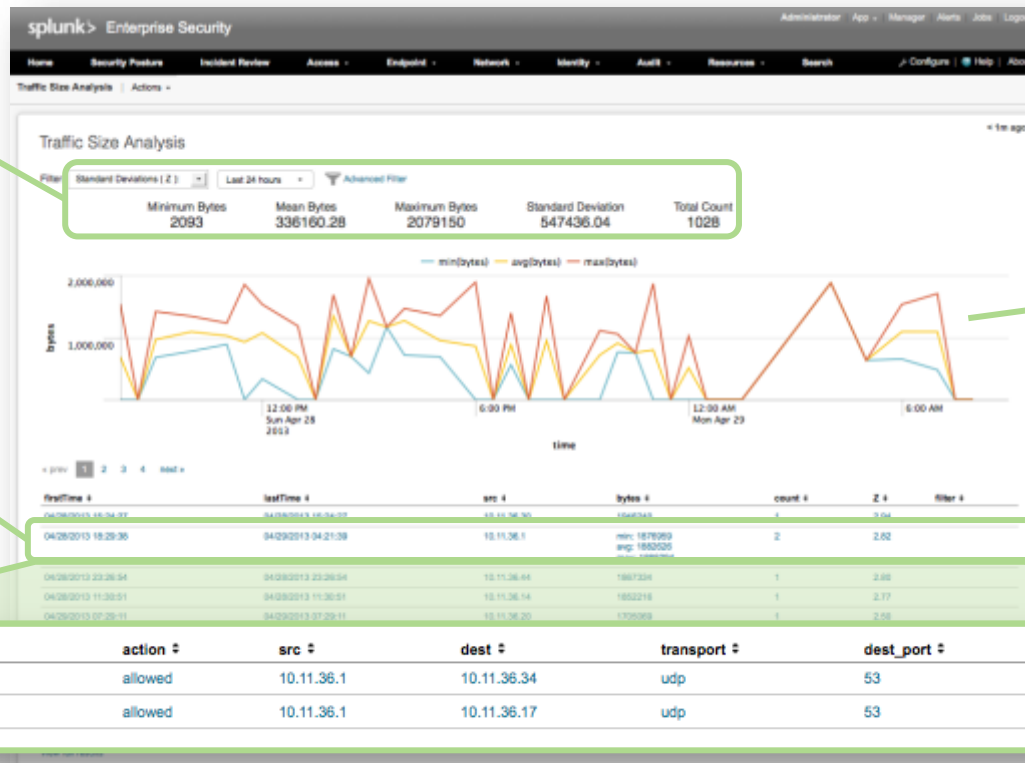
Analysis of real-time and historical data using Splunk statistical analytics to better understand, detect and address unknown threats.

Dashboard: Traffic Size Analysis

Compare traffic data with statistical data to find outliers

Drill-down to look for anomalous source/dest traffic

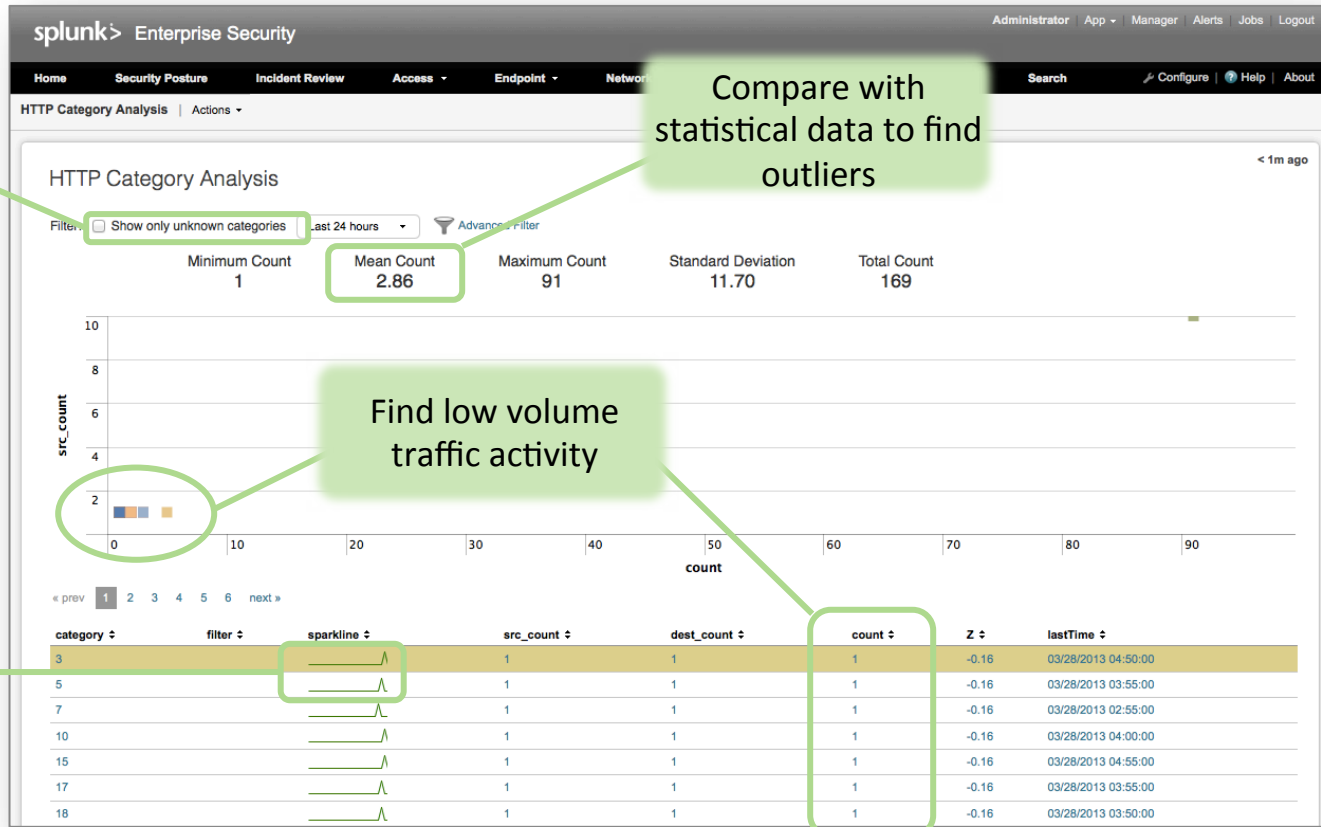
Identify suspicious data exfiltration patterns



Dashboard: HTTP Category Analysis

Investigate 'unknown' HTTP traffic

Compare with statistical data to find outliers



Look for suspicious patterns of activity by category

Find low volume traffic activity

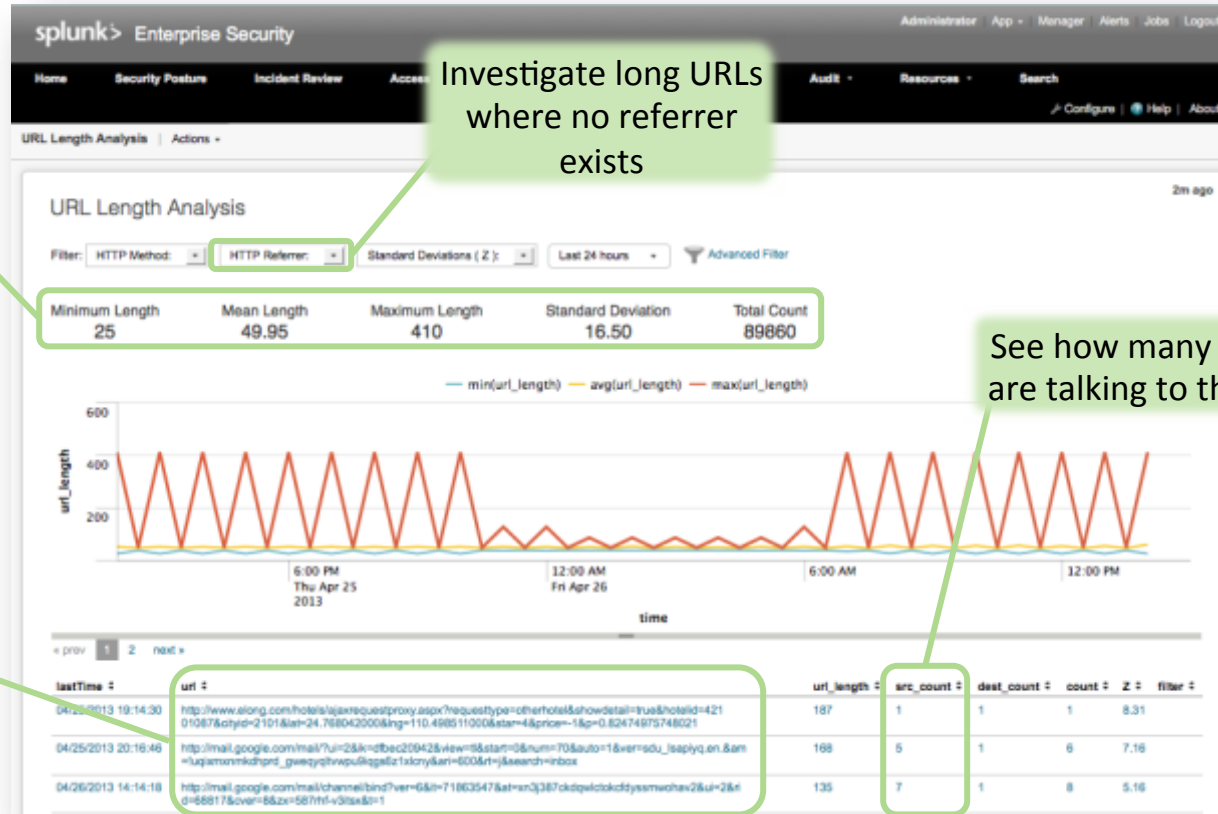
Dashboard: URL Length Analysis

Compare each URL statistically to identify outliers

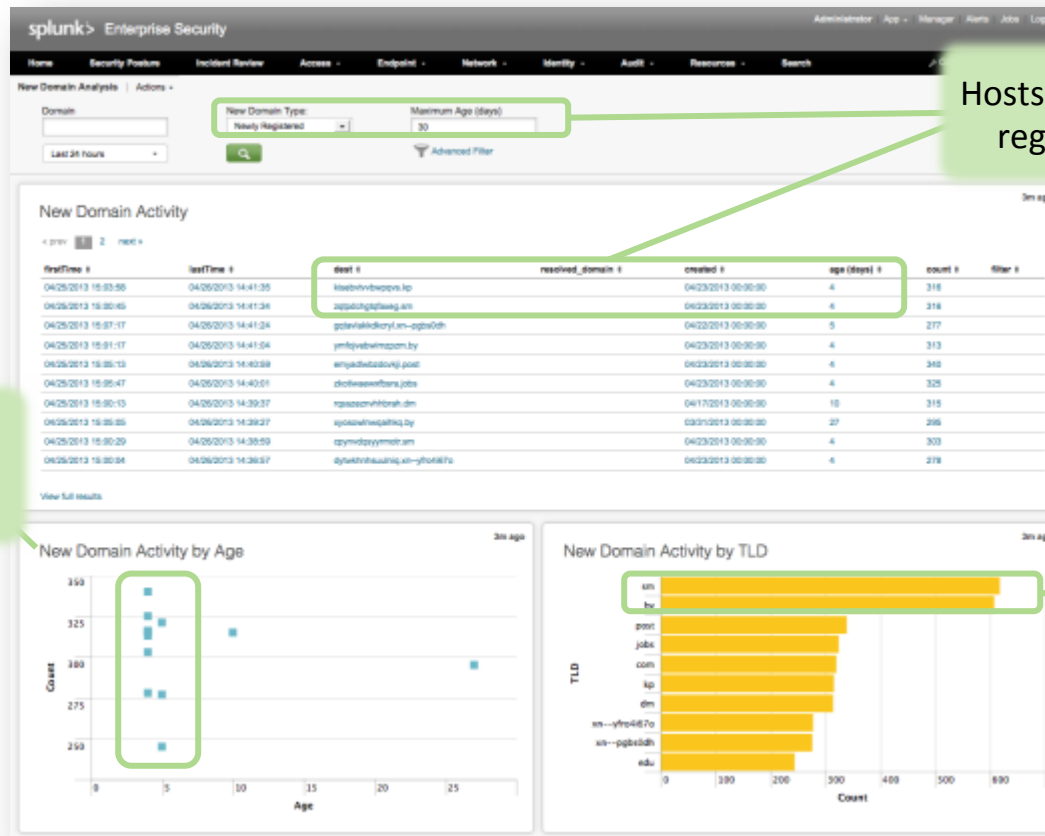
Investigate long URLs where no referrer exists

See how many assets are talking to the URL

Look for long URLs that may include embedded C&C instructions



Dashboard: New Domain Analysis

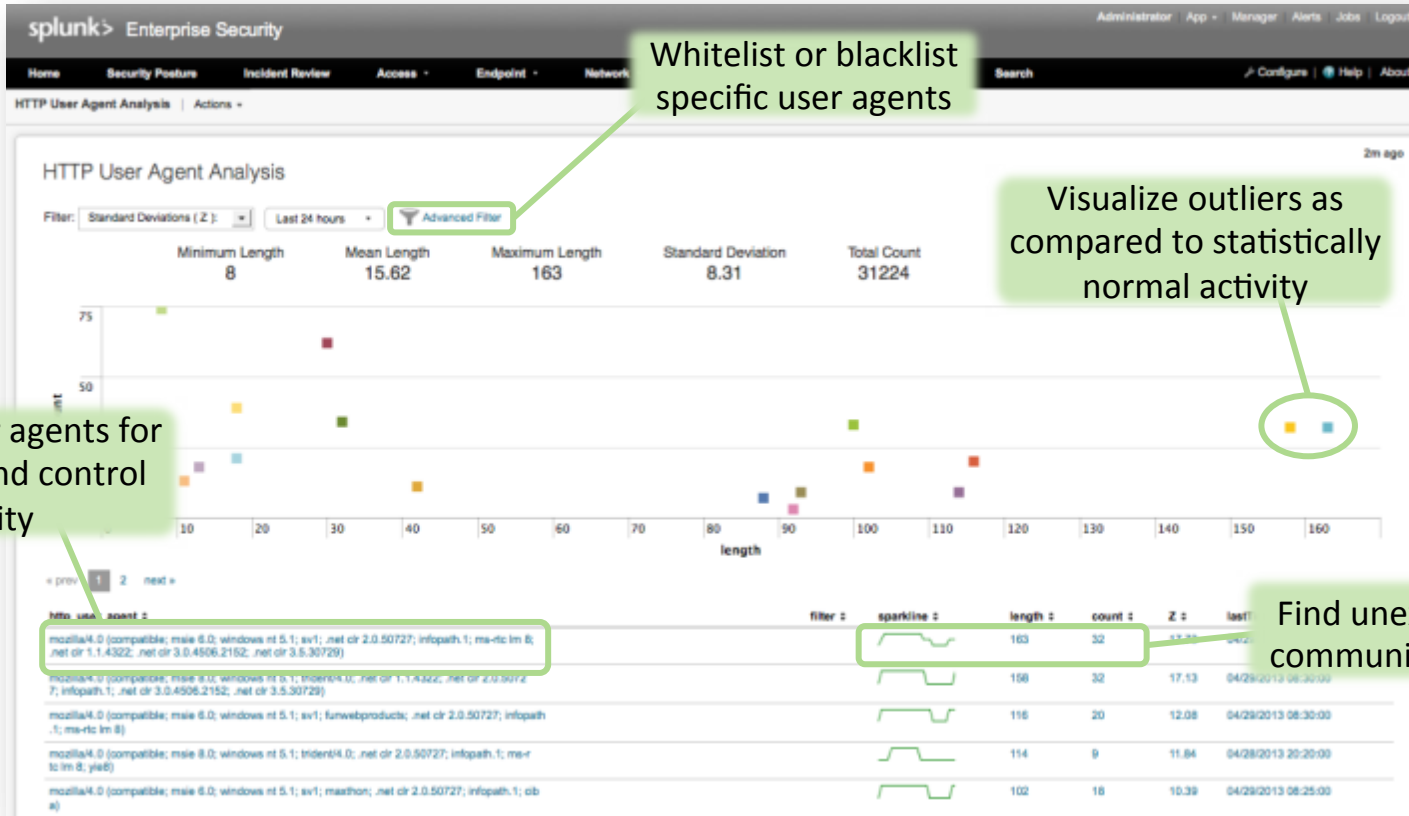


Hosts talking to recently registered domains

Discover outlier activity to newly registered domains

Identify unexpected top level domain activity

Dashboard: HTTP User Agent Analysis



Whitelist or blacklist specific user agents

Visualize outliers as compared to statistically normal activity

Evaluate user agents for command and control activity

Find unexpected HTTP communication activity

Asset and User Identities Lookup Editor

Edit Lookup File

assets.csv

1	ip	mac	nt_host	dns	owner	priority	lat	long	city	country	bunit	category	pc
2	6.0.0.1-9.0.0.0					low	41.040855	28.986183	Istanbul	TR	apac		
3	1.2.3.4	00:15:70:91:df:6c				medium	38.959405	-77.04	Washington D.C.	USA	americas		
4				CORP1.acmetech.com		high	37.694452	-121.894461	Pleasanton	USA	americas	pci cardholder	tr
5	192.168.12.9-192.168.12.9		storefront			critical	32.931277	-96.818167	Dallas	USA	americas	pci	tr
6	2.0.0.0/8					low	50.84436	-0.98451	Havant	UK	emea	pci sox	dr

- More easily edit values in each of the columns
- Color coding for specialized fields for added visual clarity
- Add new rows of data with a single right-click action

Security Threat Indicator Library

- Key Security Indicators (over 100 available)
- The ability to set a threshold for each metric that indicates if the value is acceptable or not
- Change in color (good or bad) based on customer defined threshold
- A description of the trend (increasing or decreasing) depending on whether the an increase or a decrease ought to be interpreted as good or bad)
- Drill-down from the metric to a dashboard that provides more information

Security Posture | Actions ▾

MALWARE INFECTIONS

Total Count

632  **+63**

VULNERABLE HOSTS

Total Count

1452  **-74**

VULNERABILITIES / HOST AVG

Medium Severity Or Higher

1.6  **-0.2**

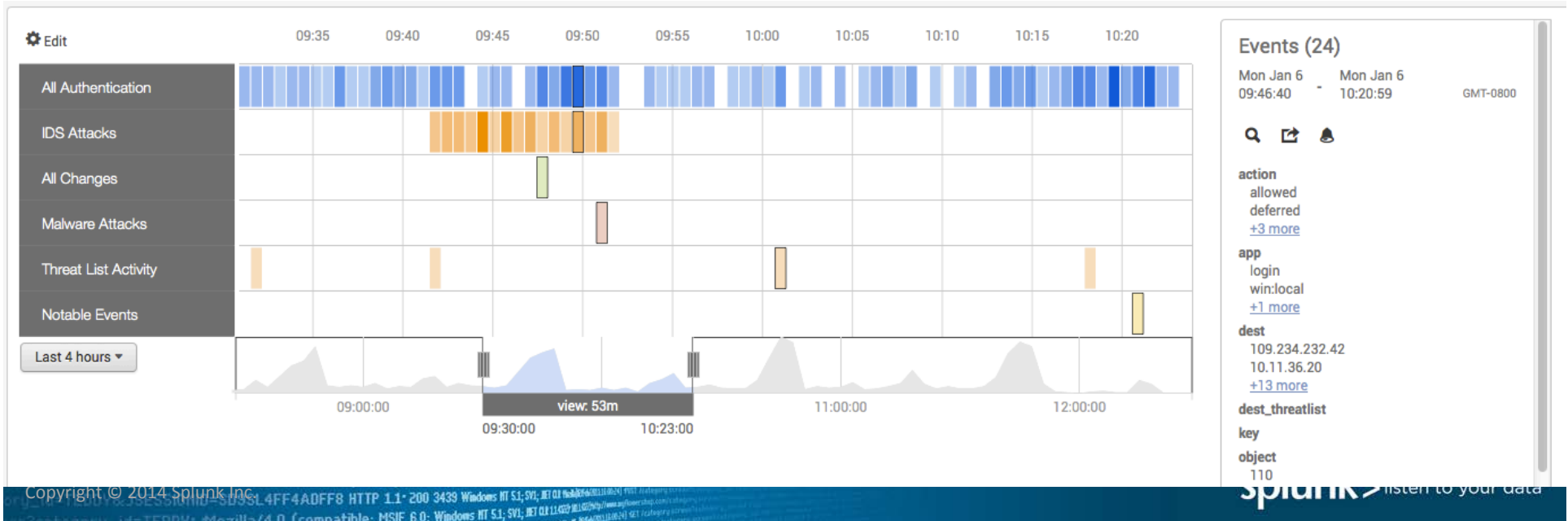
HOSTS FULLY PATCHED

Percent Of Total Hosts

78.3%  **+0.2**

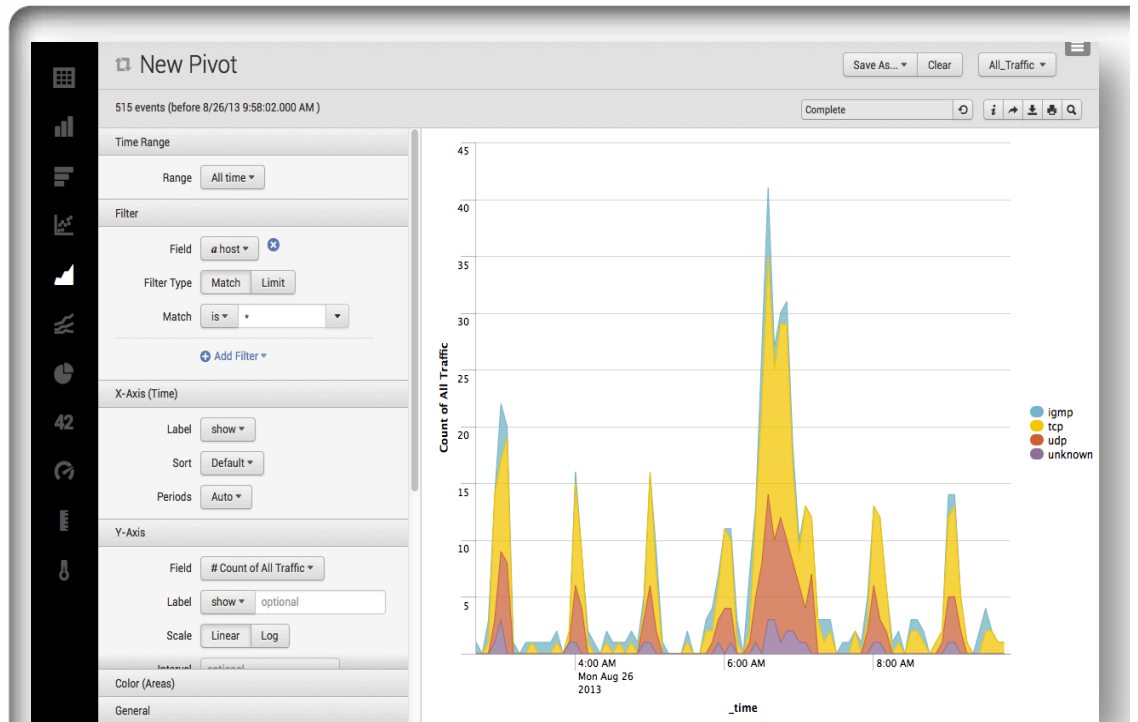
Threat Visualizer

- Search for unusual behavior patterns based on Asset and/or Identity
- Pre-determined (by the customer) events in time-synchronized swim lanes
- Select specific events to create visual correlations across known assets or identities in a single view
- The selections create a “story board” (shown on the right) for investigation

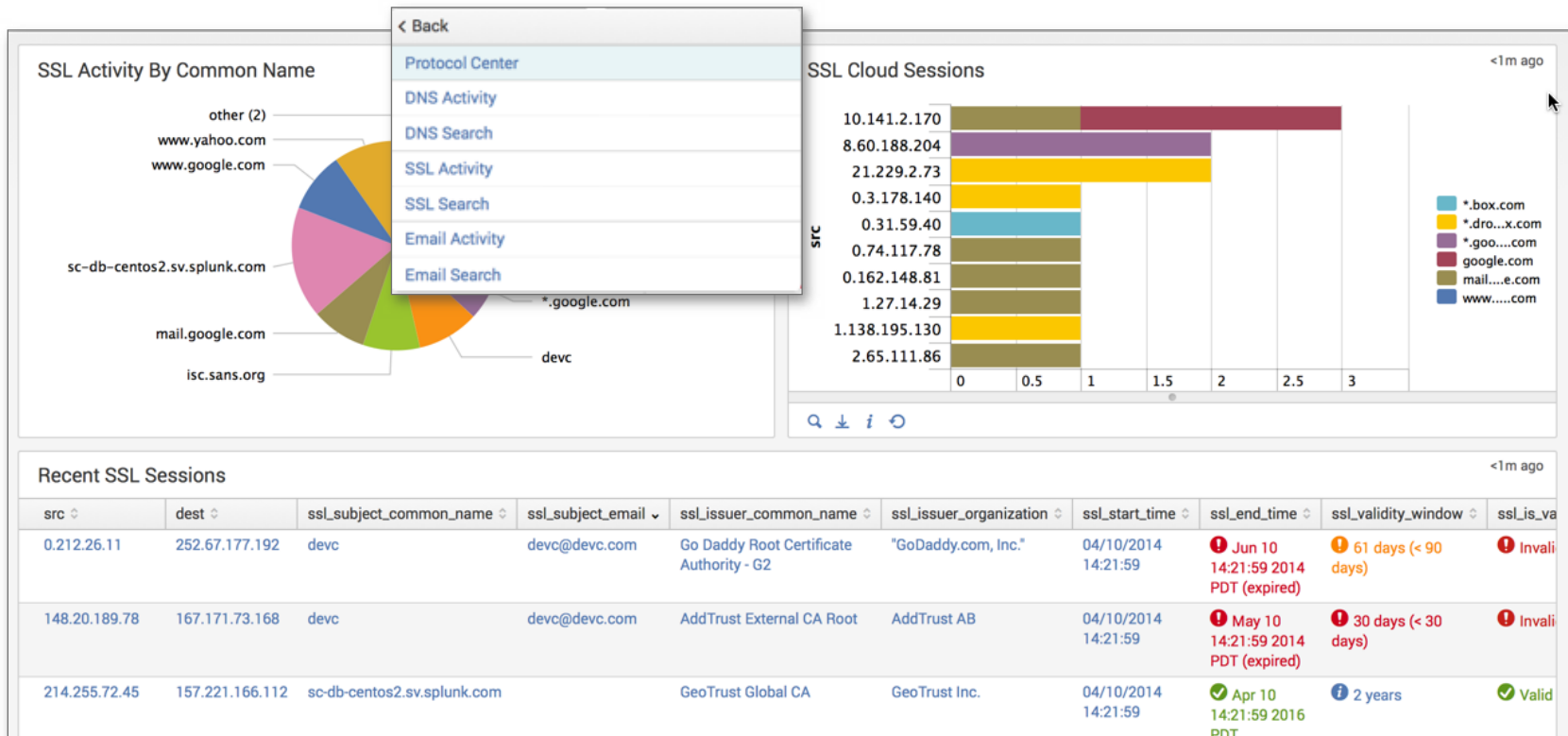


Pivot Tables for Security Reporting

- Driving down report creation complexity
- Create Pivot-based reports
- Customize as needed graph type, color, detail, etc.
- Create and circulate as a report
- Add to or create a dashboard



Protocol Intelligence Reports



Faster Protocol Investigations

Important protocol fields are exposed for fast access

Enter into workflows for investigation

Create new reports or export investigation results

The screenshot displays the Splunk Enterprise Security interface. At the top, there is a navigation bar with 'splunk' and 'App: Enterprise Security'. Below this, a menu bar includes 'Security Posture', 'Incident Review', 'Predictive Analytics', 'Event Investigators', 'Advanced Threat', 'Security Domains', 'Audit', and 'Search'. The main content area is titled 'SSL Search' and features a search form with fields for 'Source', 'Destination', 'Subject/Issuer Common Name' (containing 'google*'), 'Certificate Serial Number', and 'Certificate Hash'. A 'Last 24 hours' filter and a 'Submit' button are also present. Below the search form, a table displays search results with columns for '_time', 'src', 'dest', 'ssl_subject_common_name', 'ssl_issuer_common_name', 'ssl_serial', 'ssl_hash', and 'count'. Two rows of data are visible, both dated '2014-10-30 01:10:58'. Below the table, an event viewer shows details for a specific event, including 'ack_packets_in: 5', 'ack_packets_out: 3', 'bytes_in: 667', 'bytes_out: 3849', and 'client_rtt: 16'. The interface also includes an 'Export PDF' button and a 'Listen to your data' logo in the bottom right corner.

_time	src	dest	ssl_subject_common_name	ssl_issuer_common_name	ssl_serial	ssl_hash	count
2014-10-30 01:10:58	10.141.2.170	206.169.145.222	google.com	Google Internet Authority G2	7324132209463369388	AE435972651BFE75B5E8547BF7A35AC2	4
2014-10-30 01:10:58	10.141.2.170	74.125.224.86	mail.google.com	Google Internet Authority G2	4546184021295660457	A9D74B27453EB0034FFE5F769927D19B	2

```
> 10/30/14 1:10:58.000 AM { [-]
  ack_packets_in: 5
  ack_packets_out: 3
  bytes_in: 667
  bytes_out: 3849
  client_rtt: 16
```

Acquire Wire Data – On Alert or On-The-Fly

Correlation Search

Search Name*

Application Context

Description
Describes what kind of issues this search is intended to detect

Risk Scoring

Create risk modifier

Score*
Indicates how much to adjust the score for the given risk object

Risk object field*
Indicates what field in the results indicates the risk object (such as the system or the user) that t

Risk object type*
Indicates the type of risk object this applies to (usually 'system' or 'user')

Actions

Include in RSS feed

Send email

Run a script

Start Stream capture on for

Malware Search

- Nbtstat 10.11.36.20
- Nslookup 10.11.36.20
- Ping 10.11.36.20
- Stream Capture**
- Traffic Search (as destin
- Traffic Search (as sourc
- Update Search
- Vulnerability Search
- Web Search (as destinat

Create Stream Capture

Initiate a capture using the Splunk App for Stre

Description

Protocols to capture

- All
- HTTP
- DNS
- Email
- SMB & NFS

Over 2800 Global Security Customers



Colorado School of Public Health





splunk > live!

Milano - 24 marzo 2015

Roma - 26 marzo 2015

Oltre 8.400 aziende di tutto il mondo, incluse 70 tra le Fortune 100 usano Splunk® Enterprise per trasformare i dati macchina in preziose informazioni in grado di garantire un rapido ROI e un valore reale per il reparto IT e il business in generale.

Partecipando a SplunkLive! Italia potrai :

- Scoprire la straordinaria rapidità e semplicità delle funzioni di analisi di Splunk Enterprise 6.2
- Imparare come ottenere in modo efficiente, informazioni da data store tipo Hadoop e NoSQL
- Ascoltare casi di successo direttamente dai clienti e capire come hanno ricavato valore dai loro dati grazie a Splunk.
- Assistere a nuovi training che insegnano come massimizzare l'investimento fatto e risolvere nuovi problem di business.

Qualunque sia la tua attività, dallo sviluppo di applicazioni o generazione di analisi a fini aziendali, alla gestione, protezione e verifica in ambito IT, Splunk può aiutarti ad acquisire rapidamente valore dai tuoi dati..

Iscriviti oggi stesso : http://live.splunk.com/italia_2015

A presto,

Il team Splunk

Any question? gmary@splunk.com

Dettagli evento

Milano: 24 marzo 2015, ore 9.30-16.30 presso **NHOW**

Milano - Via Tortona 35

Roma: 26 marzo 2015, ore 9.30-16.30 presso **Westin**

Excelsior - Via Vittorio Veneto 125

Testimonianze clienti Milano

- Cerved Group S.P.A
- Alma Mater Studiorum – Università di Bologna
- Fastweb S.P.A.

Testimonianze clienti Roma

- HBG Connex S.P.A.
- Università La Sapienza
- Poste Italiane



Thank You

Stefano Radaelli
sradaelli@splunk.com

