How to Use Splunk to Detect and Defeat Fraud, Theft, and Abuse

Joe Goldberg

Product Marketing, Splunk

jgoldberg@splunk.com

Gleb Esman

Product Management, Splunk

gesman@splunk.com

Disclaimer

During the course of this presentation, we may make forward looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not, be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

Personal introduction

- Joe Goldberg
  - Product marketing for anti-fraud, cybersecurity, compliance
  - 4.5 years at Splunk
  - Previously Symantec Data Loss Prevention (Vontu)

- Gleb Esman
  - Product management for anti-fraud
  - 1 year at Splunk
  - Formerly anti-fraud consultant using Splunk at Morgan Stanley

Questions for You—Show of Hands

- Which of you has fraud or risk in your title/department?
- Which of you spends over 1/3 of your time on anti-fraud?
- Who works in the financial services industry? Retail?
- Who uses software (not Excel) to fight fraud?

Agenda

- Fraud, Theft, & Abuse 101
- Example fraud patterns and data sources
- Splunk technologies/Apps to help
- Demo

Splunk for Anti-Fraud, Theft, Abuse (“fraud”)

Why You Should Care: Fraud is Costly

Business Moving Online Has Increased Fraud

Data breaches

No boundaries

Credential theft

More sophistication

Machine Data Contains Critical Fraud Insights

Sources

Card Payment System

[2013-09-04-14.45.54.608000] proc_source="B24A", tmst_target="2013-09-04-14.45.54.724000", serv_id="ISS", proc_input="MAST", proc_target="[illegible] acq="BNET_1", interface_iss="02008", cod_msg="1110", oper_[illegible]="090448764439", card_id="526430VS350Y2992", oper_amount="000000008000", oper_curre[illegible]r_country="380", term_id="00599307", circuito="", sett_merc="4722", bin_acq="002111", id_merc="329017246168", [illegible]rcode="003000", action_code="000", approval_code ="H8H766", oper_mod_input="1", channel="O", flag_dupl="Y", [illegible] auth_rout_dst="INTFHI93", auth_rout_id="HISO_AUTH", msg_subst="", [illegible]ndg="0000000078507391", station_acq="STA-BNET-MI1", acceptor =" TRAWEL SPA\\MILANO\ 380", tmst_ins="2013-09-04-14.48.56.277466", lpar="B"

Card ID

Amount

Merchant ID

Client ID

Web Proxy

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

Source IP

Referring URL

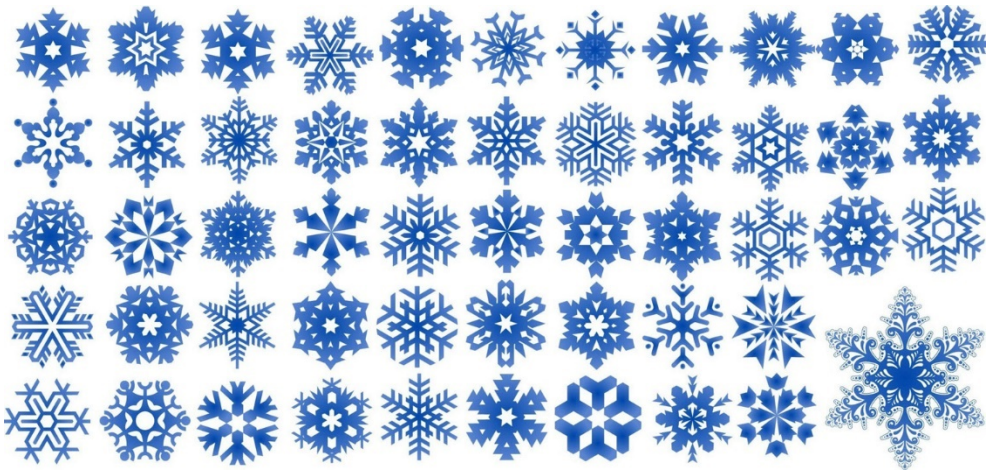
Authentication

20130806041221.000000 Caption=ACME-2975EB\JohnDoe Description=User account Built-in account for administering the computer/domainDo\n[illegible] NULLLocalAccount = IP: 10.11.36.20 TrueName=Administrator SID =S-1-5-21-1[illegible]45543 500SIDType=1 Status=Degradedwmi_ type=UserAccounts

User Name

Source IP

Hundreds of Ways to Commit Fraud



- Not all are a good fit for Splunk – bribery, corruption, financial statements, etc.

Example Patterns of Fraud in Machine Data

Industry	Type of Fraud	Pattern of Fraud
Financial Services	Account takeover	Abnormally high $ or velocity of transactions
E-Tailing	Account takeover	Many accounts accessed from one IP/browser
Health Care	Physician billing	Physician billing for drugs outside their expertise area
Online education	Student loan fraud	Student w/loan has IP in “high-risk” country and is absent from classes and assignments

Example Patterns of Fraud in Machine Data

Industry	Type of Fraud	Employee Pattern of Fraud	Data Sources
All	Internal Fraud	On PTO but logging into critical systems	HR app, auth systems
		On payroll but never badging/logging in	HR app, badging systems
		Cashier: Abnormally high $ of cash voids or no-receipt returns	POS terminals
		Finance: Skipping approval/workflow steps for vendor payments	Payment system, workflow app

Sample Fraud Indicators in Appendix

Over 50 more examples for financial services, ecommerce, health care, online education

Also In Appendix

How to catch a killer…and in-store shoplifters

Why Splunk for Fraud Detection?

Existing Fraud Tools

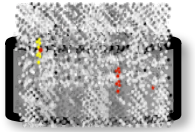
RIGID AND INFLEXIBLE

NARROW VIEW OF FRAUD

SCALE AND SPEED ISSUES

DIFFICULT TO DEPLOY;
LIMITED ROI

Splunk for Fraud



FLEXIBLE

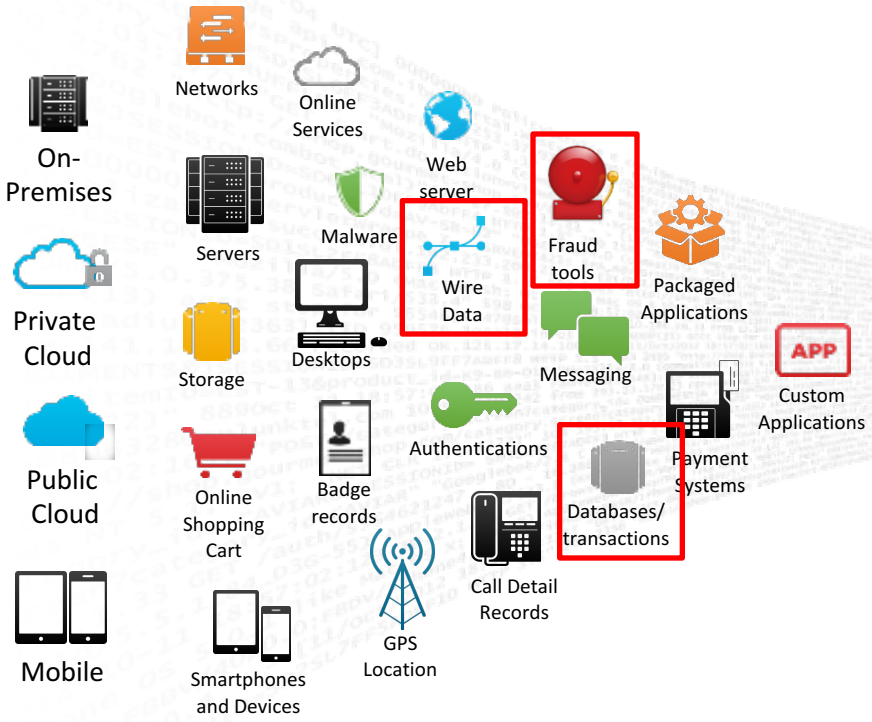
BROAD VIEW

SCALE & SPEED

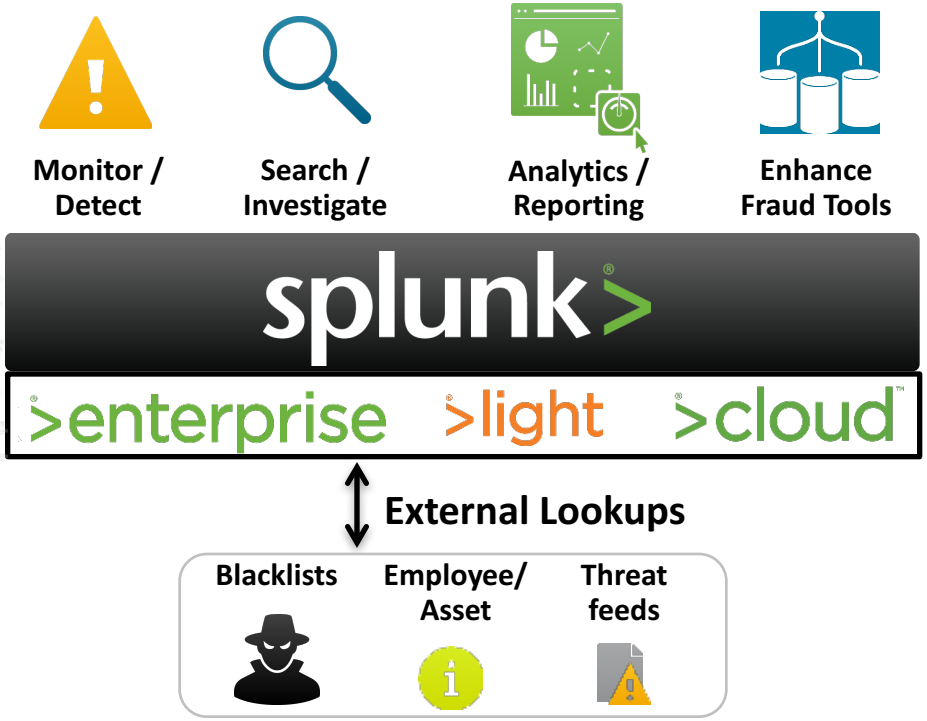
FAST VALUE;
COMPELLING ROI

Splunk: Machine Data Platform For Fraud Use Cases

Machine Data: Any Location, Type, Volume



Anti-Fraud Use Cases

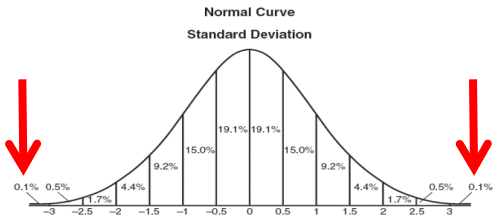


Use Case 1: Fraud Monitoring and Detection

1. Correlations/patterns

A AND B AND C NOT D = FRAUD

2. Anomalies/outliers off baseline



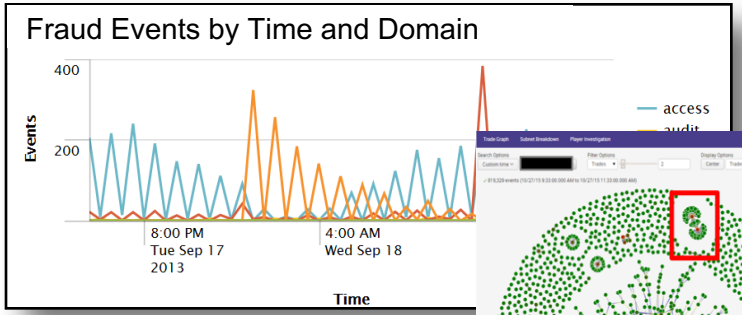
3. Risk scoring

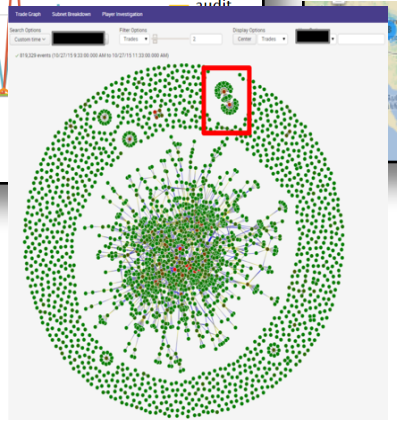
Web Site Session Activity						
Customer	New IP Address	New Browser	Changed Email Address	Changed Shipping Address	Order has Multiple #s of Same Item	Total
John Doe	5	0	0	0	0	**5**
Mike Smith	5	5	15	15	15	**55**
Jane Green	0	0	0	15	0	**15**

- Combine 1-3; use Key-Value Store for scale & maintaining state
- Alerts; Optionally can initiate automated remediation

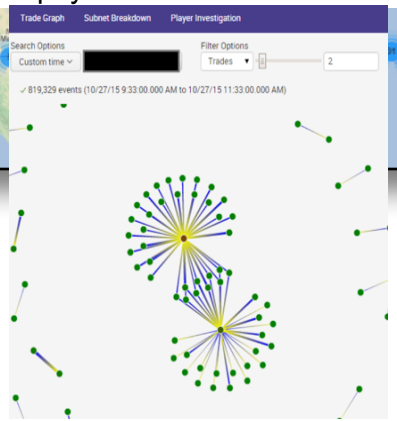
Use Case #3 – Fraud Analytics and Reporting

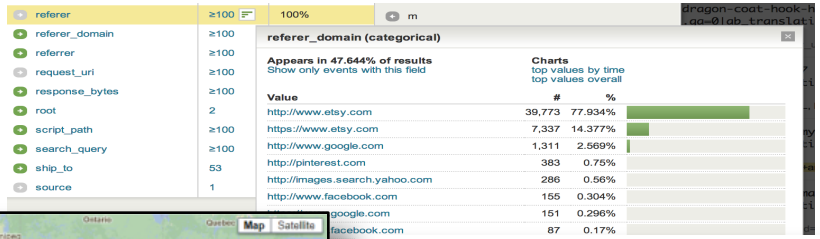
- Many types of visualizations to measure and manage fraud risk
- Easy to create in Splunk

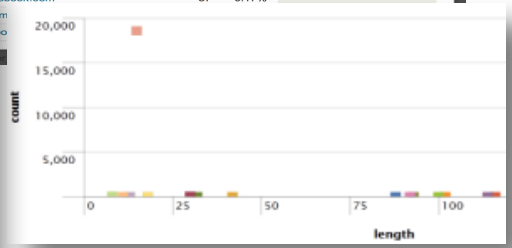




Suspicious physician transactions





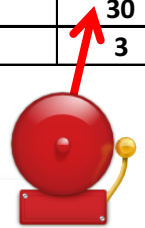


Use Case #4: Enhance Existing Fraud Tools

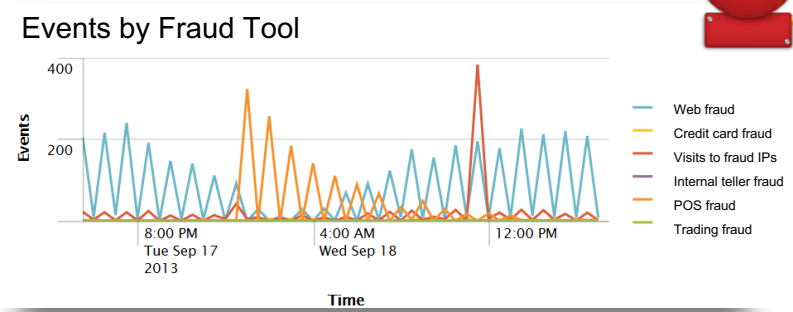
Collect data from existing, point fraud tools to:

- Give single transaction/event aggregate risk score

Web Site Session Activity				
Session ID	Web fraud risk score	Credit card risk score	Threat Intel risk score	Splunk Total
1234567	0	2	0	**2**
7654321	6	9	15	**30**
1231789	1	2	0	**3**



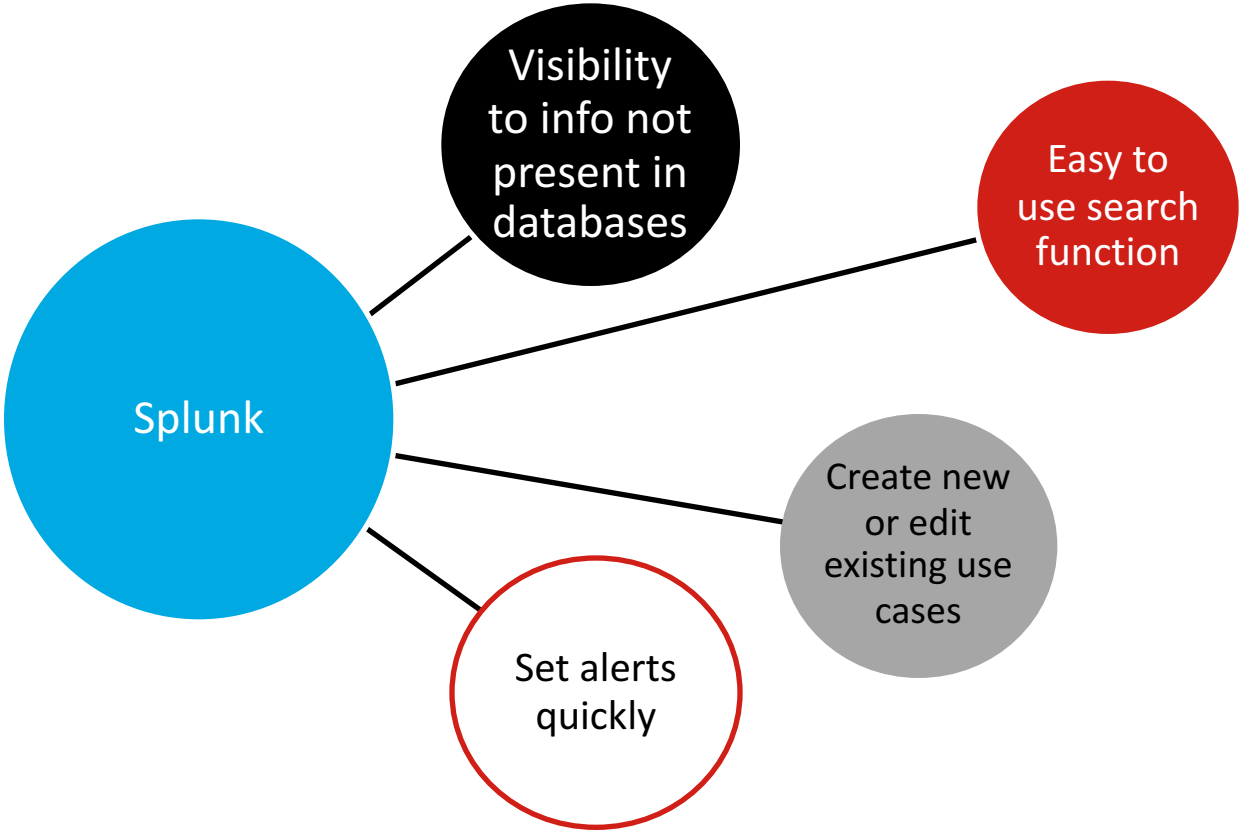
- Consolidated risk reporting to see overall risk posture and trends



Splunk Product Offering

- No anti-fraud App
- Build content on Splunk Enterprise/Light
- Apps/TAs can help

Leading Wire Transfer Co: Advantages of Splunk



Finding Value With Splunk

- Helped with significant savings due to its ability to target behavior of known fraud rings
- Prevented more fraud losses in 2015 than past 2 years combined
- Double-digit year over year fraud loss decreases from 2014 to 2015

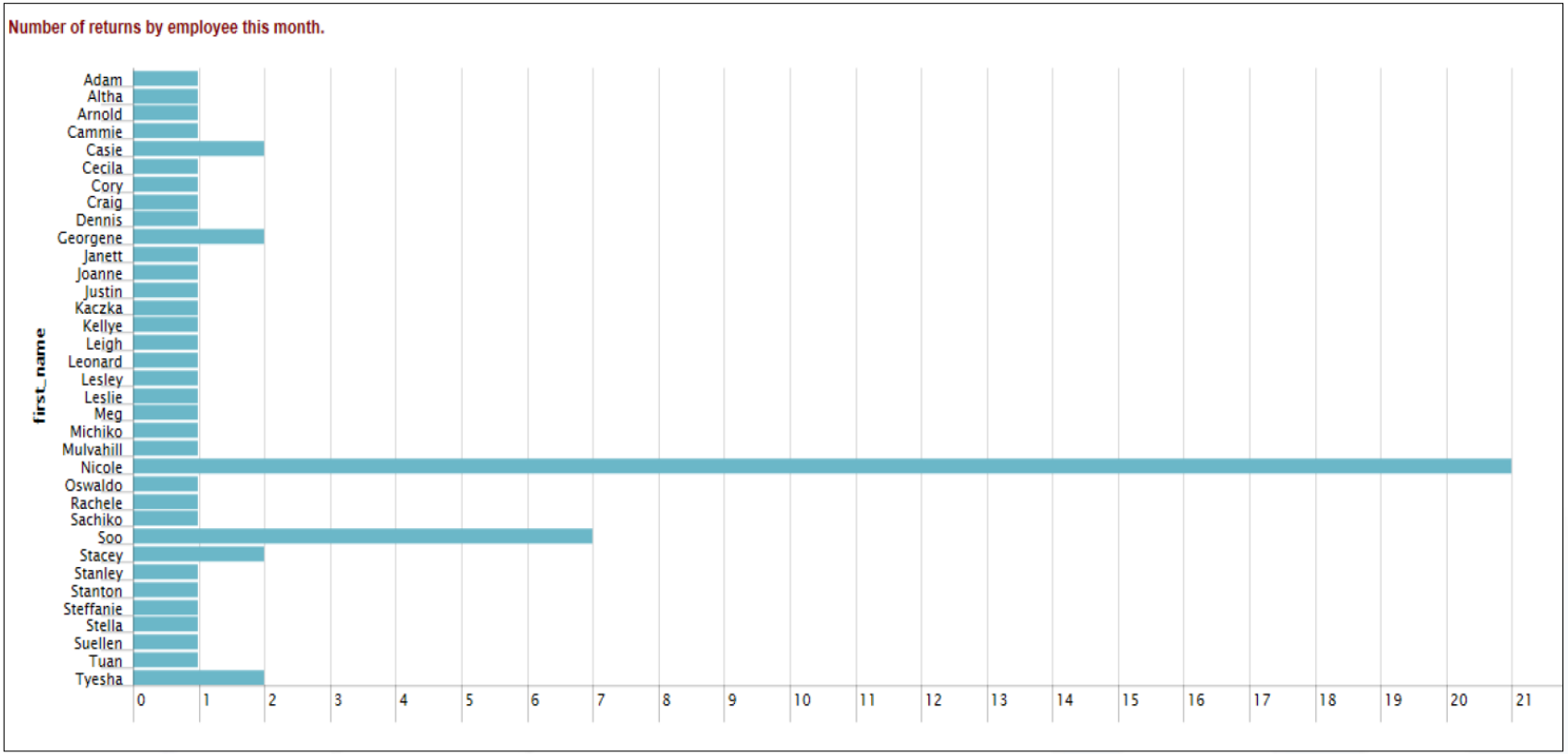
Top Takeaways

Start with one type of fraud and expand from there

Challenge yourself to discover an unknown trend or pattern

Reliant—Loss Prevention at Retail Stores

Splunk Use Case: Employee Returns Analysis



Case Studies in Appendix

In Appendix have over 15 customer success slides.

Also case studies online: Online Retailer, Orrstown Bank, PostFinance, Surescripts

Splunk Technologies / Apps To Help

Advanced Technologies

- Splunk DB Connect
- Splunk App for Stream
- Splunk Machine Learning Toolkit

Splunk DB Connect

- Working with data from traditional databases
- Supports:
  DB2/Linux, Informix, MemSQL, MySQL, AWS Aurora, Microsoft SQL Server, Oracle, PostgreSQL, AWS RedShift, SAP SQL Anywhere, Sybase ASE, Sybase IQ, Teradata
- Get it here:
  https://splunkbase.splunk.com/app/2686/

Use cases for structured data in Splunk

Index structured data from databases, such as sales records

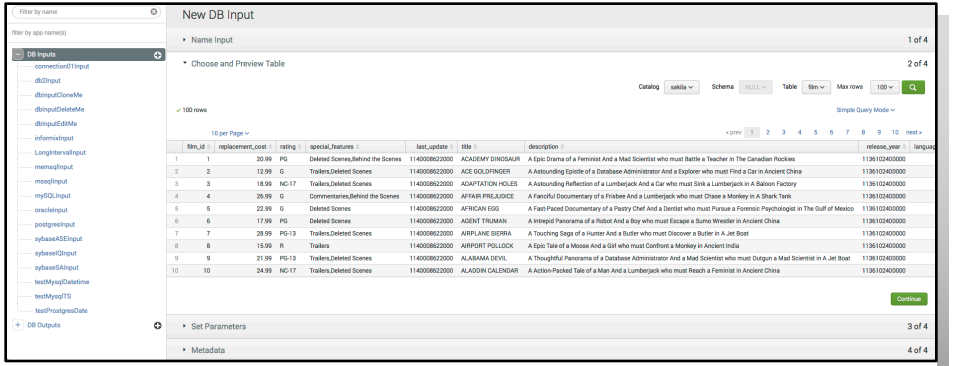
Enrich machine data in Splunk with database records

Update structured databases with Splunk info, such as risk scores

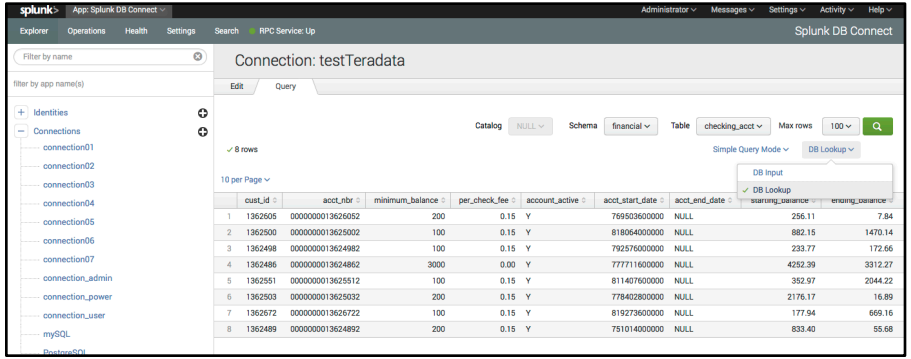
Interactively browse structured and unstructured data from Splunk reports

Splunk DB Connect

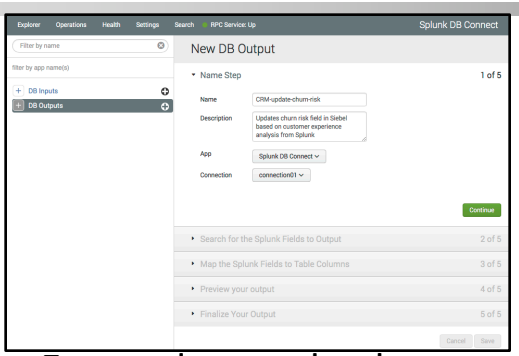
Add-on that uses JDBC to enable structured data use cases



Index data from databases



Use databases as lookups



Export data to databases

Report on structured data

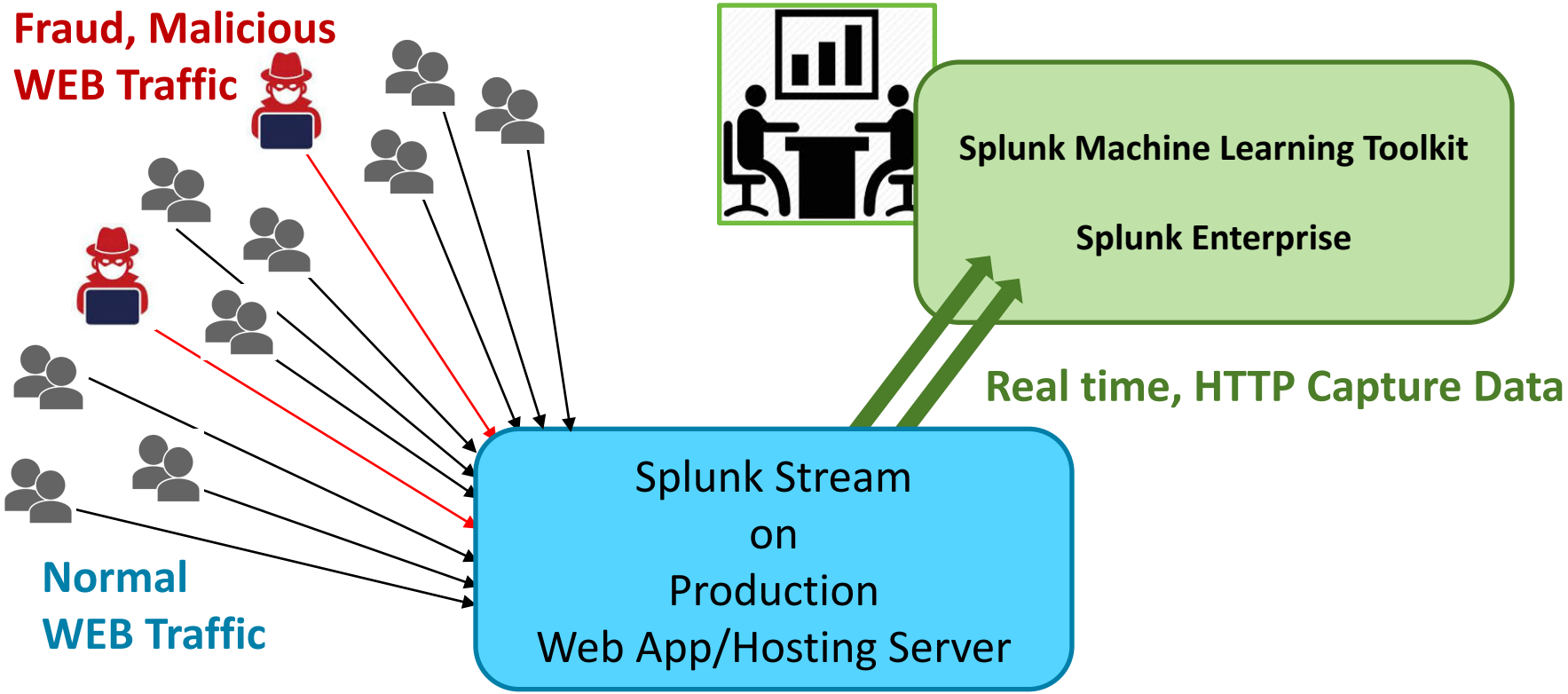
Splunk App for Stream

- Captures real-time streaming wire data from anywhere in your datacenter or from any public Cloud infrastructure.
- Capture only relevant data for analytics, through filters and aggregation rules.
- Correlate other data such as logs, events and metrics with wire data to gain valuable insights.
- Decrypt SSL-encrypted traffic.
- Manage data volumes with filtering.
- Get it here: https://splunkbase.splunk.com/app/1809/

Splunk Machine Learning Toolkit

- Delivers custom visualizations, assistants, and examples to explore a variety of machine learning concepts + custom SPL commands.
- Ability to apply the visualizations and SPL commands to your own data.
- Assistants allows to visually generate SPL to cluster numeric events.
- Allows to detect unknown unknowns for Fraud and Security cases.
- Get it here: https://splunkbase.splunk.com/app/2890/

Architecture of Fraud and Threat Detection



List ⌄ Format ⌄ 20 Per Page ⌄

‹ Hide Fields All Fields

Selected Fields
- City 27
- Country 23
- host 1
- Region 26
- source 1
- sourcetype 1

Interesting Fields
- accept 3
- accept_language 3
- action 2
- app 1
- # bytes 100+
- # bytes_in 90
- # bytes_out 100+
- # canceled 1
- cookie 41
- cs_cache_control 2
- # cs_content_length 28
- cs_content_type 1
- cs_version{} 2
- # date_hour 24
- # date_mday 2
- # date_minute 56
- date_month 1
- # date_second 58
- date_wday 2
- # date_year 1
- # date_zone 1
- dest 2
- dest_headers 79
- dest_ip 2
- dest_mac 1
- # dest_port 1
- # duration 100+
- endtime 100+
- eventtype 2
- form_data 100+
- http_comment 5
- # http_content_length 2
- http_content_type 3
- http_method 1
- http_referrer 10
- http_user_agent 10
- index 1

i		Time	Event
>	1	9/14/16 2:13:31.647 PM	


```
{ [-]
   bytes: 6478
   bytes_in: 285
   bytes_out: 6193
   canceled: 1
   connection_type: close
   cs_content_length: 34
   cs_content_type: application/x-www-form-urlencoded
   cs_version: [ [+]
   ]
   dest_headers: HTTP/1.1 200 OK
Date: Wed, 14 Sep 2016 21:13:31 GMT
Server: Apache
X-Frame-Options: SAMEORIGIN
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Set-Cookie: wordpress_test_cookie=WP+Cookie+check; path=/
Set-Cookie: PHPSESSID=955be39214c87e4920f51d42def6bcdf; path=/
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8


   dest_ip: 158.69.124.164
   dest_mac: 0C:C4:7A:7B:97:A4
   dest_port: 80
   endtime: 2016-09-14T21:13:31.647474Z
   form_data: pwd=test&wp-submit=Login&log=admin
   http_comment: HTTP/1.1 200 OK
   http_content_type: text/html; charset=UTF-8
   http_method: POST
   http_user_agent: Mozilla/5.0 (X11; U; Linux i686) Gecko/20071127 Firefox/2.0.0.11
   request: POST /wp-login.php HTTP/1.1
   server: Apache
   set_cookie: [ [+]
   ]
   site: www.presentlove.com
   src_content: pwd=test&wp-submit=Login&log=admin
   src_headers: POST /wp-login.php HTTP/1.1
Accept-Encoding: identity
Content-Length: 34
Host: www.presentlove.com
Content-Type: application/x-www-form-urlencoded
Connection: close
User-Agent: Mozilla/5.0 (X11; U; Linux i686) Gecko/20071127 Firefox/2.0.0.11


   src_ip: 69.28.199.70
   src_mac: 00:FF:FF:FF:FF:FD
   src_port: 55167
   status: 200
   time_taken: 320552
   timestamp: 2016-09-14T21:13:31.353515Z
   transfer_encoding: chunked
   transport: tcp
   uri: /wp-login.php
   uri_path: /wp-login.php
}
```


Show as raw text

City = Chatham | Country = Canada | Region = Ontario | host = ns522056.ip-158-69-124.net | source = strean

Stream data formatted

SPL:

source=stream:stream_http

splunk> .conf2016

4/12/16
3:35:00.000 AM

```
{ [-]
    bytes: 1703
    bytes_in: 662
    bytes_out: 1041
    cached: 0
    cookie: external_no_cache=1; frontend_cid=871912058; frontend=67520080632
    dest_headers: HTTP/1.1 302 Found
  Date: Sun, 06 Sep 2015 12:17:03 GMT
  Server: Apache/2.4.7 (Ubuntu)
  X-Powered-By: PHP/5.5.9-1ubuntu4.11
  Expires: Thu, 19 Nov 1981 08:52:00 GMT
  Cache-Control: no-store, no-cache, mus revalidate, post-check=0, pre-check=0
  Set-Cookie: frontend=6752008063289; expires=Sun, 06-Sep-2015 13:17:03 GMT; Max-Age=3600, magento; domain=52.74.170.211
  Set-Cookie: frontend=deleted; expir =Thu, 01-Jan-1970 00:00:01 GMT; 0; path=/magento; domain=52.74.170.211; http
  Set-Cookie: frontend=3979981608454; expires=Sun, 06-Sep-2015 13 =3600; path=/magento; domain=52.74.170.2
  Set-Cookie: persistent_shopping_car deleted; expires=Thu, 01 Max-Age=0; path=/magento; domain=52.7
  X-Frame-Options: SAMEORIGIN
  Location: https://52.74.170.211/magento/checkout/onepage/i
  Content-Length: 0
  Keep-Alive: timeout=5, max=100
  Connection: Keep-Alive
  Content-Type: text/html; charset=UTF-8

    dest_ip: 172.31.19.68
    dest_mac: 06:B8:1 58:0B:D3
    dest_port: 443
    form_data: login%5Busername%5D=CameronJohnston% 0olschar.de&form_key=Iy4fBlRhjeVJZjdC&s d=&login%5Bpassword%5D=XXXXXXXX2864
    http_comme t: Found
    http_content_length: 0
    http_content_type: text/html; charset=UTF-8
    http_method: POST
    http_referrer: https://52.74.170.211/magento/customer/account/login/
    http_user_agent: Mozilla/5.0 (X11; Linux i686; rv:2.0b3pre) Gecko/20100731 Firefox/4.0b3pre
    location: https://52.74.170.211/magento/checkout/onepage/index/
    login_failure_direct:
    login_post_message:
    login_success_direct:
    request: POST /magento/customer/account/loginPost/ HTTP/1.1
```

Sessionize

Decrypted

- Headers
- Args
- Cookies
- Content

Form Fields
- **Username**
- **password**

splunk> App: Search & Reporting

Administrator | Messages | Settings | Activity | Help | Find

Search | Pivot | Reports | Alerts | Dashboards | Search & Reporting

New Search

```
index=str source=stream:stream_http http_method=POST wp-login pwd | iplocation src_ip
| rex field=form_data "log=(?<username>[^&]+)"  | eval username=urldecode(username)
| rex field=form_data "pwd=(?<password>[^&]+)" | fillnull value="" password
| table _time, src_ip, site, username, password, Country http_user_agent
```

✓ 186 events (before 9/14/16 3:31:09.000 PM) No Event Sampling

Events (186) | Patterns | Statistics (186) | Visualization

100 Per Page | Format | Preview

< Prev 1 2 Next >

_time	src_ip	site	username	password	Country	http_user_agent
2016-09-14 14:13:31.647	69.28.199.70	www[redacted]ove.com	admin	test	Canada	Mozilla/5.0 (X11; U; Linux i686) Gecko/20071127 Firefox/2.0.0.11
2016-09-14 12:50:58.426	50.63.197.168	berti[redacted]ng.com	jnelson	password	United States	Mozilla/5.0 (X11; U; Linux i686) Gecko/20071127 Firefox/2.0.0.11
2016-09-14 12:40:10.184	178.74.243.246	berti[redacted]ng.com	admin	1	Ukraine	Opera/9.80 (Windows NT 6.1; U; ru) Presto/2.8.131 Version/11.10
2016-09-14 12:22:16.958	82.115.130.152	surp[redacted]ure.ca	swadmin	password	Sweden	Mozilla/5.0 (X11; U; Linux i686) Gecko/20071127 Firefox/2.0.0.11
2016-09-14 12:04:51.719	50.62.177.238	www[redacted]actory.ca	jnelson	password	United States	Mozilla/5.0 (X11; U; Linux i686) Gecko/20071127 Firefox/2.0.0.11
2016-09-14 11:26:18.924	91.200.12.93	www[redacted]com	gadmin	root	Ukraine	Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 6.1; 125LA; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)
2016-09-14 11:26:18.505	91.200.12.93	www[redacted]com	gadmin	pass	Ukraine	Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 6.1; 125LA; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)
2016-09-14 11:26:17.962	91.200.12.93	www[redacted]com	gadmin	adminpass	Ukraine	Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 6.1; 125LA; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)
2016-09-14 11:26:17.417	91.200.12.93	www[redacted]com	gadmin	adminpwd	Ukraine	Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 6.1; 125LA; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)
2016-09-14 11:26:16.858	91.200.12.93	www[redacted]com	gadmin	adminpw	Ukraine	Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 6.1; 125LA; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)
2016-09-14 11:26:16.312	91.200.12.93	www[redacted]com	gadmin	admin	Ukraine	Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 6.1; 125LA; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)
2016-09-14 11:19:04.555	50.62.177.107	www[redacted]des.com	admin	admin	United States	Mozilla/5.0 (X11; U; Linux i686) Gecko/20071127 Firefox/2.0.0.11
2016-09-14 10:17:36.837	178.74.243.246	berti[redacted]ng.com	admin	123	Ukraine	Opera/9.80 (Windows NT 6.1; U; ru) Presto/2.8.131 Version/11.10
2016-09-14 09:33:05.383	46.17.57.181	surp[redacted]ure.ca	swadmin	14121987	United Kingdom	Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/36.0.1985.125 Safari/537.36
2016-09-14 07:59:36.736	83.143.240.4	berti[redacted]ng.com	admin	123123	Czech Republic	Opera/9.80 (Windows NT 6.1; U; ru) Presto/2.8.131 Version/11.10
2016-09-14 07:30:28.096	46.17.57.181	vanit[redacted]m	gadmin	14121987	United Kingdom	Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/36.0.1985.125 Safari/537.36
2016-09-14 07:22:55.158	192.169.200.204	www[redacted]t.com	admin	password	United States	Mozilla/5.0 (X11; U; Linux i686) Gecko/20071127 Firefox/2.0.0.11
2016-09-14 07:11:00.561	91.200.12.65	www[redacted]com	gadmin	root	Ukraine	Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 6.1; 125LA; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)

Leverage Stream data to find account takeover attacks on multiple user accounts. See all attempted passwords

Get sample of data to build ML models

splunk> App: ML Toolkit and Showcase | Administrator | Messages | Settings | Activity | Help | Find

Search | Showcase | Assistants | Scheduled Jobs | Docs | ML Toolkit and Showcase

Cluster Numeric Events

Partition events with multiple numeric fields into clusters.

Create New Cluster | Load Existing Settings

Enter a search

```
index=bank_summ eventcount>3 | head 2500 | fields sum* eventcount duration | fillnull
```

All time

✓ 2,500 events (6/25/16 10:54:45.000 PM to 9/14/16 4:07:33.000 PM)

Job | Smart Mode

Preprocess (optional)

Fields to preprocess

duration, eventcount, sum_bytes_in, sum_bytes_in_get, sum_bytes_in_post, sum_bytes_out, sum_bytes_out_get, sum_bytes_out_post

Select method(s) to use

Apply StandardScaler

Apply PCA to reduce dimensionality to 3 fields

Preprocess

Cluster

Algorithm: DBSCAN

Fields to use for clustering: PC_1, PC_2, PC_3

eps (radius of neighborhood): 0.75

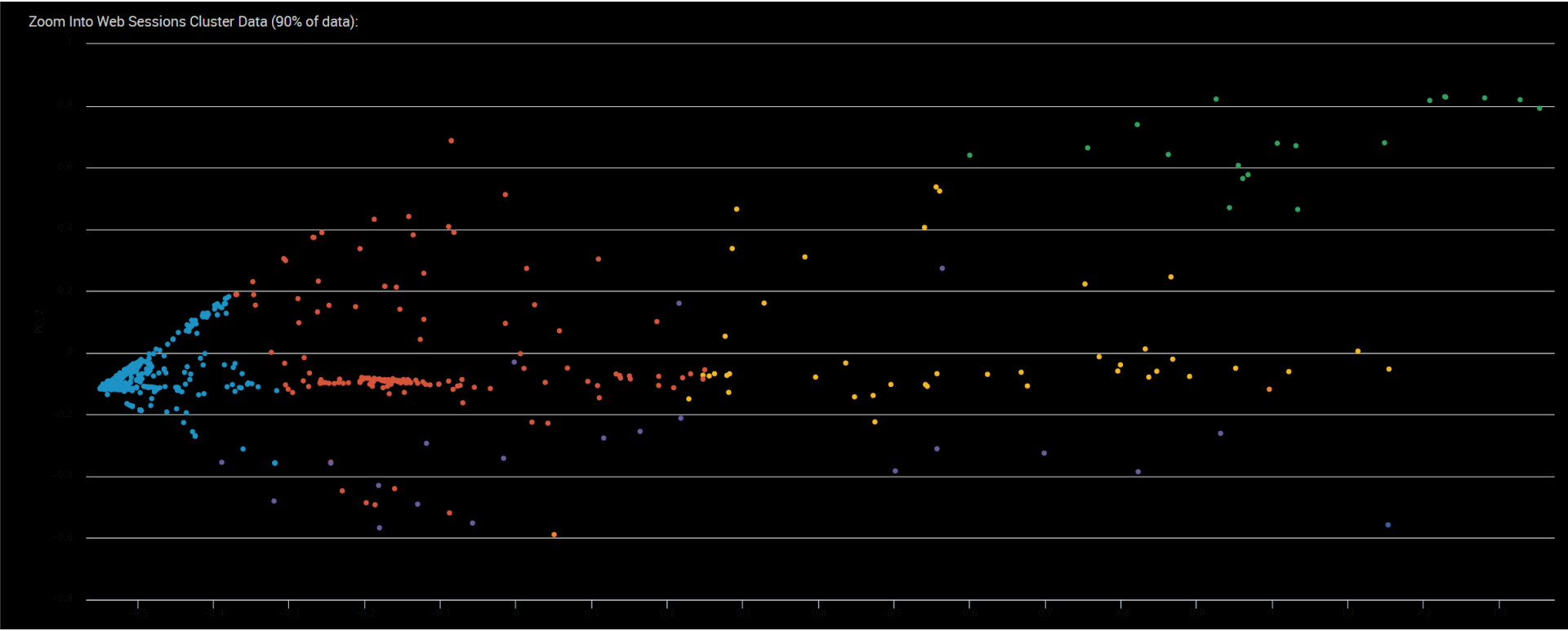
Cluster

index=bank_summ eventcount>3 | head 2500 | fields sum* eventcount duration | fillnull

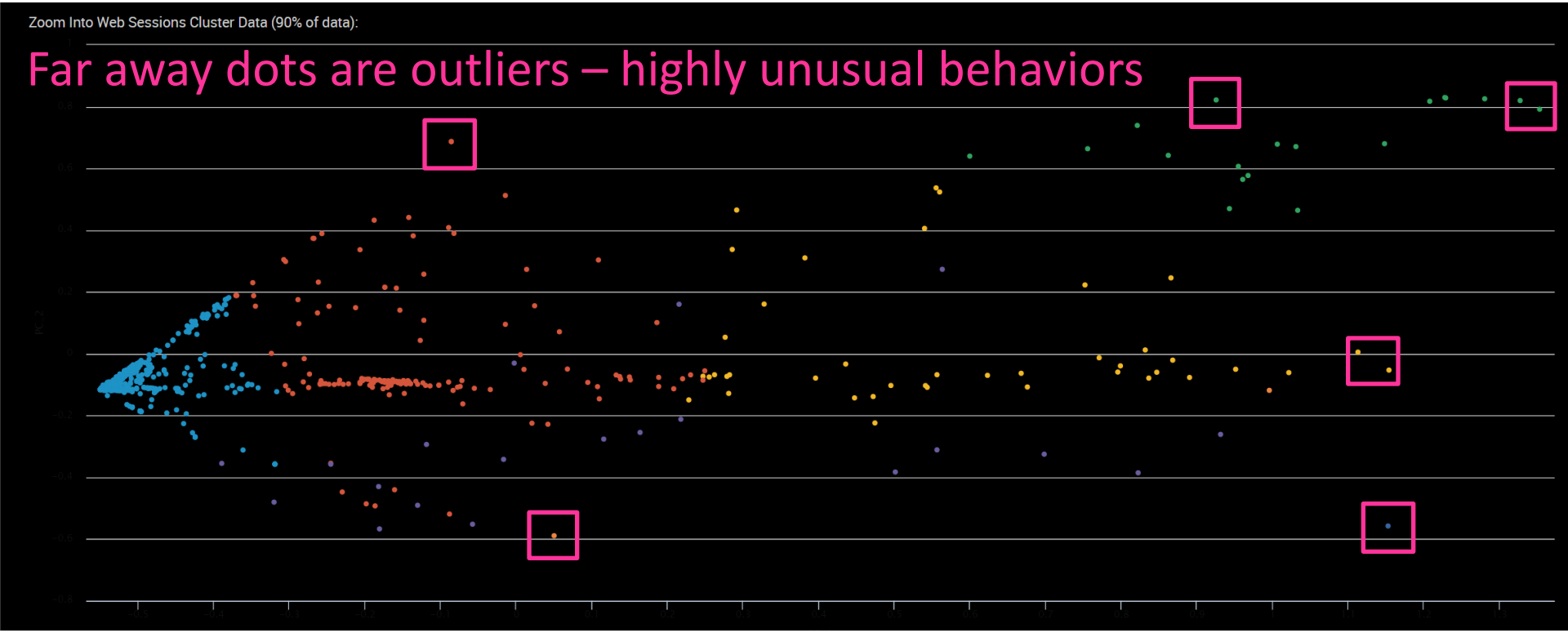
Preview Clusters within data

Generated clusters of data visually shows the majority of user sessions as well as outliers and anomalies

Clustering WEB Sessions to detect outliers



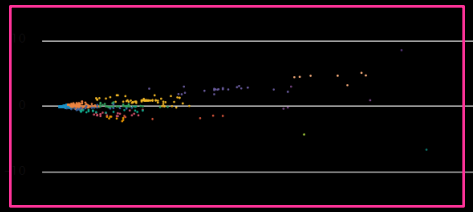
Clustering WEB Sessions to detect outliers



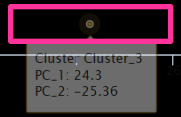
Global View: Complete Set of Cluster Data (100% of data):

Detected anomaly pointed to highly suspicious file:

Main Cluster of Web Sessions



Far away outlier by behavior



Detected Anomalies:

_out_get_total	bytes_out_post_total	bytes_out_total	phpsessid	src_ip	Country	Region	City	uri_path	status	http_user_agent	http_referrer
502872	135231	638103	162.195.134.248-c9...	162.195.134.248	United States	Texas	Fort Worth	[redacted]	200	Mozilla/5....fari/601.1	[redacted]
0	41583	41583	116.227.60.152-a85...	116.227.60.152	China	Shanghai Shi	Shanghai	... /xmlrpc.php	200	Mozilla/5....efox/3.6.8	-
420801	83975	504776	209.90.145.141-130...	209.90.145.141	Canada			... dPfTJewedV.php	404	Mozilla/5.....0.2130.32	-
19832006	0	19832006	174.114.59.66-8047...	174.114.59.66	Canada	Ontario	Toronto	... loween-013.jpg	200	Mozilla/5....ari/537.36	[redacted]
3357496	107193	3464689	204.107.141.240-12...	204.107.141.240	United States	California	San Francisco	... 474511831.6919	200	Mozilla/5....ari/537.36	[redacted]
2238426	0	2238426	92.193.57.39-a73da...	92.193.57.39	Germany			... onopono.js.php	200	Mozilla/5....ari/537.36	http://liebe-das-ganze.blogspot.de/
1507623	0	1507623	190.141.4.181-dbea...	190.141.4.181	Panama	Provincia de Panama	Panama City	... itcoin_16x.png	200	Mozilla/5....1.4.589.15	http://thedaedalusreport.com/wp-admin/admin.php?page=pretty-link
1359001	0	1359001	66.249.69.106-af26...	66.249.69.106	United States	California	Mountain View	... VE/w25-api.php	200	Mozilla/5..../bot.html)	http://www.freigeist-forum-tuebingen.de/2013/10/die-wahre-aufgabe-der-bienen-beim.html

Tracking Anomaly to Fraudsters/Attackers

1

Find events with suspicious file

New Search

```
index=str source=stream:stream_http YauCdPfTJewedV.php
```

✓ 1 event

```
uri: /wp-content/plugins/wp-symposium/server/php/YauCdPfTJewedV.php
uri_path: /wp-content/plugins/wp-symposium/server/php/YauCdPfTJewedV.php
```

2

Find events with ***wp-symposium***

New Search

```
index=str source=stream:stream_http wp-symposium/server
```

✓ 56 ever

src_content field only provided by Splunk Stream:

```
Obfuscation provided by FOPO - Free Online PHP Obfuscator: http://www.fopo.com.ar/
This code was created on Wednesday, May 11th, 2016 at 6:10 UTC from IP 203.66.57.176
Content-Disposition: form-data; name="files[]"; filename="assLkPxI.php"
```

Tracking Anomaly to Fraudsters/Attackers

Search | Pivot | Reports | Alerts | Dashboards | Anomaly Research

New Search

Save As | Close

```
index=str source=stream:stream_http
[search index=str source=stream:stream_http
  [search index=str source=stream:stream_http Obfuscator
    | rex field=src_content "filename=\"(?<malware>.*\.php)" | stats values(malware) as malware | eval search = mvjoin(malware, " OR ") | fields search
    ]
  | dedup src_ip | table src_ip
  ]
| iplocation src_ip | timechart c span="1h" by src_ip
```

All time

✓ 357 events (before 9/23/16 8:33:17.000 PM) No Event Sampling

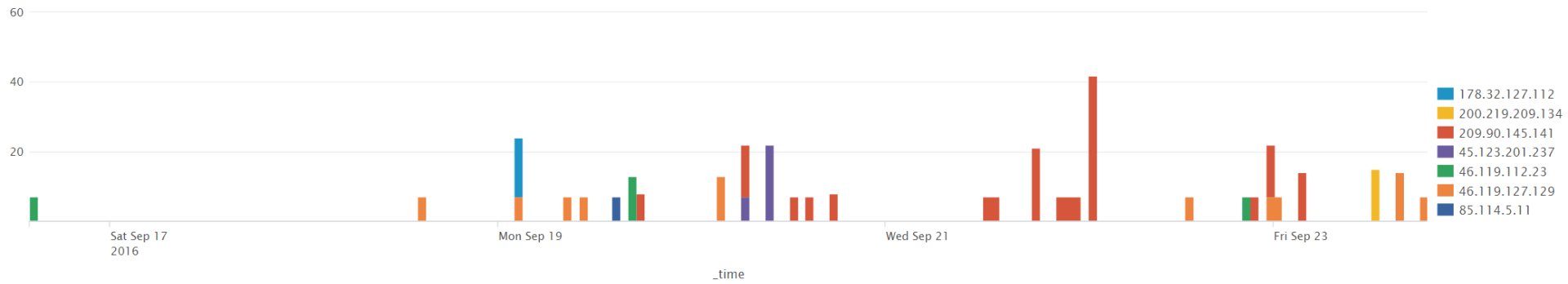
Job | Verbose Mode

Events (357) | Patterns | Statistics (173) | Visualization

3

Find IP addresses of all attackers and show me their activity across timeline

Column Chart | Format



Tracking Anomaly to Fraudsters/Attackers

Search | Pivot | Reports | Alerts | Dashboards — Anomaly Research

New Search — Save As — Close

```
index=str source=stream:stream_http
[search index=str source=stream:stream_http
  [search index=str source=stream:stream_http Obfuscator | rex field=src_content "filename=\"(?<malware>.*\.php)" | stats values(malware) as malware | eval search = mvjoin(malware, " OR ")
    | fields search ]
  | dedup src_ip | table src_ip ]
| iplocation src_ip | table _time, src_ip, Country, site, uri_path, http_method, status, http_user_agent
```

All time

✓ 21 events (before 9/23/16 9:18:15.000 PM) No Event Sampling

Events (21) | Patterns | Statistics (21) | Visualization

20 Per Page | Format | Preview

4

Show me origins of all attackers as well as every possible resource and customer they touched and when. So I can immediately protect my customers, resources and accounts.

_time	src_ip	Country	site	uri_path	http_method	status	http_user_agent
2016-09-23 18:27:42.556	46.119.127.129	Ukraine	www.******.com	/	POST	301	Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/49.0.2623.75 Safari/537.36 OPR/36.0.2130.32
2016-09-23 18:27:42.435	46.119.127.129	Ukraine	www.******.com	/	POST	301	Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/49.0.2623.75 Safari/537.36 OPR/36.0.2130.32
2016-09-23 18:27:42.312	46.119.127.129	Ukraine	www.******.com	/wp-content/plugins/revslider/temp/update_extract/revslider/db.php	GET	404	Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/49.0.2623.75 Safari/537.36 OPR/36.0.2130.32
2016-09-23 12:12:29.023	200.219.209.134	Brazil	www.******.ca	/wp-content/plugins/wp-symposium/server/php/SlHskDassLkPxl.php	GET		Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/49.0.2623.75 Safari/537.36 OPR/36.0.2130.32
2016-09-23 12:10:57.277	200.219.209.134	Brazil	www.******.ca	/wp-content/plugins/wp-symposium/server/php/index.php	POST	404	Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/49.0.2623.75 Safari/537.36 OPR/36.0.2130.32
2016-09-23 12:10:55.268	200.219.209.134	Brazil	www.******.ca	/etc/passwd	GET	301	Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/49.0.2623.75 Safari/537.36 OPR/36.0.2130.32
2016-09-23 03:45:47.186	209.90.145.141	Canada				404	
2016-09-23 03:45:46.407	209.90.145.141	Canada	www.******.com	/wp-content/plugins/wp-symposium/server/php/index.php	POST	404	Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/49.0.2623.75 Safari/537.36 OPR/36.0.2130.32
2016-09-23 03:45:44.720	209.90.145.141	Canada	www.******.com	/wp-content/plugins/revslider/temp/update_extract/revslider/db.php	GET	404	Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/49.0.2623.75 Safari/537.36 OPR/36.0.2130.32
2016-09-22 20:37:47.746	46.119.112.23	Ukraine	www.******.com	/	POST	200	Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/49.0.2623.75 Safari/537.36 OPR/36.0.2130.32
2016-09-22 20:37:46.102	46.119.112.23	Ukraine	www.******.com	/	POST	200	Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/49.0.2623.75 Safari/537.36 OPR/36.0.2130.32
2016-09-22 20:37:44.729	46.119.112.23	Ukraine	www.******.com	/wp-content/plugins/revslider/temp/update_extract/revslider/db.php	GET	404	Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/49.0.2623.75 Safari/537.36 OPR/36.0.2130.32
2016-09-20 09:33:42.403	45.123.201.237	Macao	www.******.com	/wp-content/plugins/wp-symposium/server/php/cbgsjchddQgKlx.php	GET	404	Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/49.0.2623.75 Safari/537.36 OPR/36.0.2130.32
2016-09-20 09:33:41.401	45.123.201.237	Macao	www.******.com	/wp-content/plugins/wp-symposium/server/php/index.php	POST	404	Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/49.0.2623.75 Safari/537.36 OPR/36.0.2130.32
2016-09-20 09:33:37.361	45.123.201.237	Macao	www.******.com	/wp-content/plugins/revslider/temp/update_extract/revslider/db.php	GET	404	Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/49.0.2623.75 Safari/537.36 OPR/36.0.2130.32
2016-09-19 14:08:16.381	85.114.5.11	Russia	******.com	/wp-content/plugins/wp-symposium/server/php/LcXJcHVDWsklli.php	GET	301	Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/49.0.2623.75 Safari/537.36 OPR/36.0.2130.32
2016-09-19 14:08:15.895	85.114.5.11	Russia	******.com	/wp-content/plugins/wp-symposium/server/php/index.php	POST	404	Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/49.0.2623.75 Safari/537.36 OPR/36.0.2130.32
2016-09-19 14:08:13.807	85.114.5.11	Russia	******.com	/wp-content/plugins/revslider/temp/update_extract/revslider/db.php	GET	301	Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/49.0.2623.75 Safari/537.36 OPR/36.0.2130.32

Demo

Popular Anti-Fraud Search

- *Detect account takeovers;* 1 IP logging into > 5 accounts in 1 day
- Detail at Splunk.com > Solutions > Security, Compliance & Fraud > Security and Fraud Use Cases

1. Index appropriate data

```
04/14/2016 06:53,123088,Failure,Mindy Barber,92.42.49.101
04/14/2016 10:15,123098,Success,Douglas Lambert,216.214.255.255
04/14/2016 13:51,123108,Success,John Doe,69.147.76.15
```

Popular Anti-Fraud Search cont…

2. Do Field Extractions

New Search

index=fraud_demo sourcetype=web_site_logs

✓ 484 events (4/7/16 1:00:00.000 PM to 4/14/16 1:52:14.000 PM)

Events (484) | Statistics | Visualization

Format Timeline | – Zoom Out | + Zoom to Selection | × Deselect

List | Format | 20 Per Page

< Hide Fields | All Fields

Selected Fields
- a Acct_Name_Logged_Into 20
- a Auth_Status 2
- a host 10
- # Session_ID 98
- a source 1
- a Source_IP 20
- a sourcetype 1

Interesting Fields
- # date_hour 24
- # date_mday 8
- # date_minute 60
- a date_month 1
- a date_wday 7
- # date_year 1
- a date_zone 1
- a index 1
- # linecount 1
- a punct 1
- a splunk_server 1

i	Time	Event
⌄	4/14/16 1:51:00.000 PM	04/14/2016 13:51,123108,Success,John Doe,69.147.76.15
>	4/14/16 1:29:00.000 PM	04/14/2016 13:29,123107,Success,Douglas Lambert,216.214.255.255 Acct_Name_Logged_Into = Douglas Lambert | Auth_Status = Success | Session_ID = 123107
>	4/14/16 1:08:00.000 PM	04/14/2016 13:08,123106,Success,Godfrey Conte,150.202.0.0 Acct_Name_Logged_Into = Godfrey Conte | Auth_Status = Success | Session_ID = 123106

Event Actions

Type	Field	Value	Actions
Selected	Acct_Name_Logged_Into	John Doe	
	Auth_Status	Success	
	Session_ID	123108	
	Source_IP	69.147.76.15	
	host	webserver_004	
	source	web_site_logs_master_xls.csv	
	sourcetype	web_site_logs	
Event	index	fraud_demo	
	linecount	1	
	splunk_server	JGOLDBERG-XPS	
Time	_time	2016-04-14T13:51:00.000-07:00	
Default	punct	//_:,[]=&...	

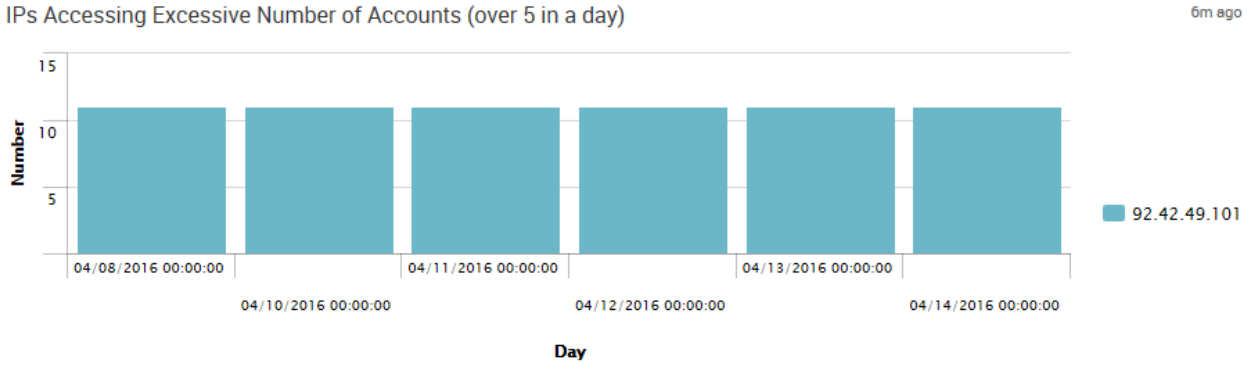
Popular Anti-Fraud Search cont…

3. Search

```
|index=fraud_demo sourcetype=web_site_logs Auth_Status=Success
| bucket _time span=1d
| stats dc(Acct_Name_Logged_Into) as num_accts by _time,Source_IP
| where num_accts >= 5
```

4. Visualize

```
| convert ctime(_time) as day
| xyseries day Source_IP num_accts
```



Takeaways

- Patterns of fraud are in machine data
- Splunk can harness machine data and structured data to detect, investigate, and report on a wide range of fraud
- Advanced Splunk technologies can address the more demanding anti-fraud use cases

What Now?

- App Showcase: “Splunk for Compliance & Anti-Fraud” booth
- Session: “Advanced Techniques for Detecting Fraud Using Splunk”, Thurs, 10:15-11:00 AM
- Web site: Information, Solution Guide, Case Study, Video
  - Splunk.com > Solutions > Security, Compliance and Fraud > Fraud
- Contact sales team at Splunk.com > Contact Us
  - May be eligible for free, onsite Fraud Workshop

Q&A

THANK YOU

Joe Goldberg

Product Marketing, Splunk

jgoldberg@splunk.com

Gleb Esman

Product Management, Splunk

gesman@splunk.com

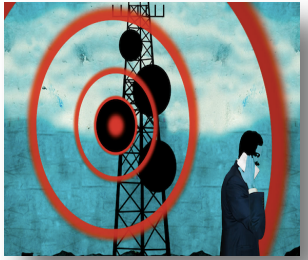
.conf2016

splunk>

Appendix

Splunk For Fraud Detection Across Verticals

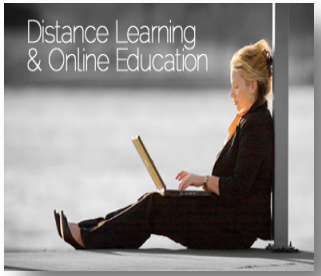
Financial Services



Mobile / Telecom

eCommerce

Health Care



Online Education

Government

Ecommerce/web site: Sample Fraud Indicators

- One referrer string or IP logging into multiple user accounts
- Single IP excessively selecting the “I forgot my password” option for several accounts
- Single IP excessively failing logins using different credentials
- Abnormally large purchases, or very high velocity of purchases, from a single account
- User traffic coming from “rent a VM”, cloud-based services (AWS, Rackspace, etc)
- Brute force password guessing that is too fast to be human
- Customer info that should be stable changing often: email/physical address, payment card, etc
- Geographic mismatch between a user IP, billing address, and/or shipping address
- Multiple purchases with different credit cards going to the same mailing address
- Buyer IP address being international but shipping address being in the U.S
- Single IP creating multiple new accounts in a short time period
- User navigating through site too fast to be human
- User IP coming from high-risk country/region, a known bad IP, or a proxy server
- User using a browser in a language indicative of a high-risk region
- User using a mobile device
- User scraping the full contents of the web site

Internal fraud:

- Store employee: conducting transactions out of normal hours, applying discounts outside of acceptable %s, ringing up their own purchases, processing an excessively large $ amount of returns

Financial Services: Sample Fraud Indicators

- Near-simultaneous ATM withdrawals from 3 or more ATMs involving a single account
- Single account having daily withdrawals in excess of normal limits
- Based off a customer baseline, abnormally large $ wire transfers, or large # of transactions in set time period
- Wire transfers going to high-risk countries/regions or financial institutions associated with fraud
- Multiple wire transfers from single account in the $9500-$9999 range over X number of days
- Financial transaction that skips the normal steps/process
- Securing multiple mortgage loans that exceed the value of the property
- Dishonest appraisals resulting in inflated home values

Internal fraud:

- Bank teller conducting transactions out of normal hours, processing their own transactions
- IT or developer logging into an application to conduct trades
- Trader using credentials that do not match with the owner of the physical workstation
- Financial transaction not following the correct business processes or order of steps

Health Care: Sample Fraud Indicators

- Multiple patients sharing the same phone number, address, email, etc
- Doctor prescribing prescriptions outside of their area of expertise
- Physicians that are many standard deviations off the norm for what an average physician for a given specialty in a given region bills Medicare/Medicaid every month in terms of number of procedures or $
- Doctor receive payments at an address that is geographically distant from their office address

Online Education: Sample Fraud Indicators

- Student IP in “high-risk” country and student absent from classes & assignments
- Student who has taken out a loan not appearing in any online classrooms or forums
- Student enrolling multiple times with slightly different variations on name, address, etc.
- Multiple students logging into online classes from a single IP address
- Students opening multiple virtual classrooms simultaneously

Leading Online Retailer

- **Challenge:** Fraud investigations were too slow with no unified logging.
  - Investigation took 12 hours using ten resources

- **Enter big data:** Big data, flexible platform to accelerate investigations
  - Unites all context around possible fraud on single dashboard
  - Investigation takes 0.2 hours using two resources
  - Consolidated fraud reporting from multiple fraud tools
  - Use the big data solution for fraud, security, compliance, IT Ops, and App Mgmt

Reliant—Loss Prevention at Retail Stores

Splunk Use Case: Transactions Outside Of Normal Hours

Transactions that were performed outside normal working hours of 10AM-6PM

« prev 1 2 3 4 next »

	time	store	date	amount	tran_type	first_name	last_name	employee_no	tender	entry_type
1	7:48:00	3	22-Oct	750	sale	Nicole	Velarde	100242	cash	
2	7:33:00	3	22-Oct	200	x-read	Nicole	Velarde	100242		
3	7:19:00	3	22-Oct	200	count	Nicole	Velarde	100242		
4	7:04:00	3	22-Oct		float in	Nicole	Velarde	100242		
5	7:03:00	3	22-Oct		opening	Nicole	Velarde	100242		
6	7:02:00	3	22-Oct		clockin	Nicole	Velarde	100242		
7	8:57:00	3	22-Oct	180	empsale	Nicole	Velarde	100242	cash	
8	8:52:00	1	22-Oct		clockin	Nicole	Velarde	100242		
9	8:38:00	3	22-Oct	-1500	return-nv	Nicole	Velarde	100242	visa	keyed
10	8:25:00	3	22-Oct	350	sale	Stacey	Warrick	100241	amex	swiped

11/7/12 8:38:00.203 AM

```
3,22-Oct,8:38:00,2030,100242,return-nv,-1500,,visa,keyed,
store=3
```

Leading Device Insurance Co - Improving Fraud Detection

- Challenge
  - False Claims → Insurance fraud → ($$$$)
  - Fraudsters financially motivated and always trying new things

- Solution – Analysis of known bad behavior
  - Multiple claims/phones shipped to same address
  - Anomalous claim durations – impossibly short claim durations
  - Web request origin → account information → shipment correlation
  - Find repeat offenders - extract attributes from bad claims, detect/prevent similar activities

To Catch A Killer…..

From: se <se-bounces@splunk.com> on behalf of Omid Krabbe <okrabbe@splunk.com>
Date: Friday, June 17, 2016 at 9:56 AM
To: se <se@splunk.com>
Subject: [se] Splunk used to find homicide suspects…

This is from a financial services customer -

The Fraud Team uses Splunk to comply with subpoenas from Law Enforcement to monitor certain accounts.
In May, the information provided in real time from Splunk led to the arrest of a homicide suspect in Texas.

&#8226 Timeline – hotel reservation lead to arrests:
&#8226 5/18 12:45: Dallas PD request monitoring on 2 accounts used by homicide suspects
&#8226 5/18 13:52: Splunk alert for KFC in Dallas, TX; advise PD
&#8226 5/18 18:09: Splunk alert for DS TRUCK STOP in Belton, TX; advise PD
&#8226 5/18 18:21: Splunk alert for PLN*PRICELINE HOTELS; advise PD
&#8226 5/18 20:32: Splunk alert for MC DONALDS in Dallas, TX; advise PD
&#8226 5/20 02:30: Splunk alert for UBER TECHNOLOGIES INC; advise PD
&#8226 5/20 02:41: Splunk alert for UBER TECHNOLOGIES INC; advise PD
&#8226 5/20 10:31: Dallas PD advises suspects in custody, state "**We could not have found them without your help.**"

It might not make sense to use your credit card after you murder someone…

Omid

To Catch Shoplifters…..

From: se [mailto:se-bounces@splunk.com] **On Behalf Of** Joe Goldberg
Sent: Friday, June 17, 2016 11:19 AM
To: Michael Wilde <mwilde@splunk.com>; Tolga Tohumcu <ttohumcu@splunk.com>; Omid Krabbe <okrabbe@splunk.com>; se <se@splunk.com>
Subject: Re: [se] Splunk used to find homicide suspects...

Speaking of interesting "real-time, law enforcement-related" use cases, below is another one…..although with lower stakes then catching a killer! It is from last year & is courtesy of James Brodsky. Customer is a big box retailer I anonymized.

==

I did hear, in person today at our Retail talk, a cool physical theft case from XXXXXX, solved via use of Splunk. In a nutshell…

They had a group of thieves visiting XXXXXX stores in a geographic area. One thief would pick a cheap product in a large box, and stealthily remove the product. The others would go around the store and pick up small, high value items, and place them in the box which would then get resealed. Yeah – they were good enough to avoid the security cameras. Then, they used a copied membership card to buy the single box with cash. They did this in multiple stores.

How did they find the culprits?

They are splunking their transactions so they know which member account numbers are used at which times in each store. The thieves always used the same copied membership card. However, they didn't turn off their phone wifi, and they have all of the MAC addresses from members' phones in each store, coming in from the access points (probably something like this – I didn't ask: https://meraki.cisco.com/lib/pdf/meraki_datasheet_cmx_location_analytics.pdf)

So, first they used Splunk to figure out which member account was being used at lots of stores in the geography. They saw discrepancies here – the "real" member was showing a normal pattern of XXXXXX shopping at a single store, but it was also being used at many other stores to buy a single item.

Next they took that list of stores where the single-item purchases were made and known theft had happened, and correlated for a MAC address that showed up in those stores at the exact times that the single item purchases were made in those stores, and made note of it.

Next they set up a near-real-time search to detect said MAC address the next time it was seen in the stores. As soon as that happened, loss prevention was notified to be on the lookout for suspicious activity – I.e. A person buying a single, cheap item. Once the copied membership card was also scanned, and correlated via cameras with the person buying a single item, the LP team had enough incriminating information to detain the thief.

Wire Transfer Fraud

splunk> App: Fraud demo

Administrator | Messages | Settings | Activity | Help

Search | Pivot | Reports | Alerts | * Ecommerce web site fraud | * Wire transfer fraud | Fraud demo

* Wire transfer fraud

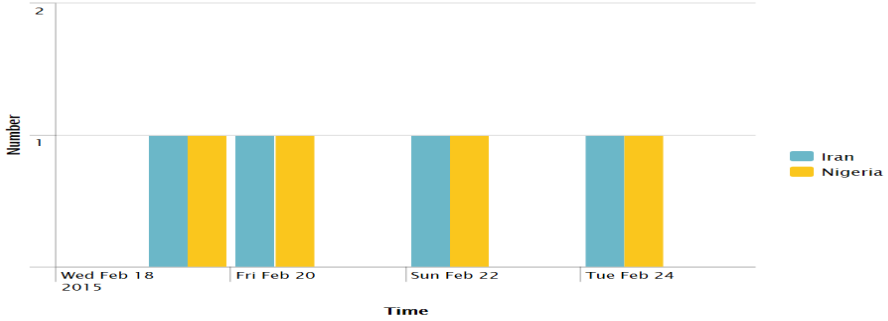
Edit | More Info

*Destination IPs of high-risk countries last 7 days

Loading - 2%

Destination IPs of High Risk Countries Last 7 Days

3m ago



Transfers to High Risk Institutions

3m ago

Dest_Institution	month_day	Transaction_ID	Transaction_amount
Bank of Nigeria	february 24	5553430	9751
Bank of Cuba	february 24	5553371	90
Bank of Nigeria	january 27	5553430	9751
Bank of Cuba	january 26	5553371	90
Bank of Nigeria	january 28	5553430	9751
Bank of Cuba	january 27	5553371	90
Bank of Nigeria	january 29	5553430	9751
Bank of Cuba	january 28	5553371	90
Bank of Cuba	january 29	5553371	90
Bank of Nigeria	january 30	5553430	9751

« prev 1 2 3 4 5 6 7 next »

Abnormally high # of wire transfers per account

3m ago

Account_name	Transactions over last 24 hours	Average daily transactions over prior 7 days	Std Dev over prior 7 days	2 Std Dev above the 7 day average	Last 24 hours less 7 day avg
Acme Bank Inc	109	14.142857	1.463850	17.070557	94.857143
Architecture Design LLC	44	5.714286	1.496026	8.706338	38.285714
Bobs Restaurant Chain	37	4.857143	0.690066	6.23728	32.142857
Jane Smith	39	5.142857	1.069045	7.280947	33.857143
John Doe	20	2.571429	0.534522	3.64047	17.428571

Accounts where over 20% of transactions in last 7 days are suspicious: $9000-$9999

Account_ID	Account_name	total	suspicious	susp_pct
654673	Bobs Restaurant Chain	2392770	631409	26.388203

Loading - 2%

E-Commerce Site Fraud

splunk> App: Fraud demo

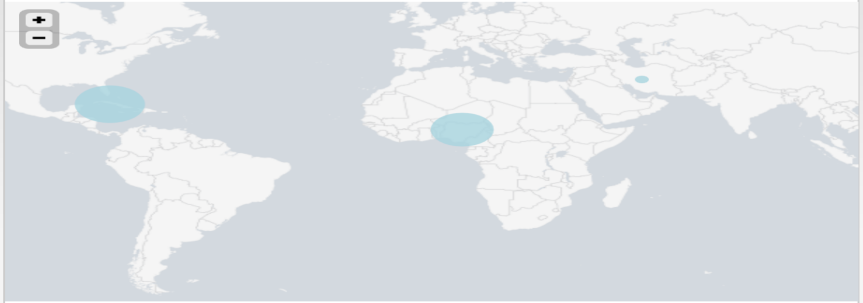
Administrator Messages Settings Activity Help

Search Pivot Reports Alerts * Ecommerce web site fraud * Wire transfer fraud Fraud demo

* Ecommerce web site fraud

Edit More Info

Connections from high-risk countries last 7 days



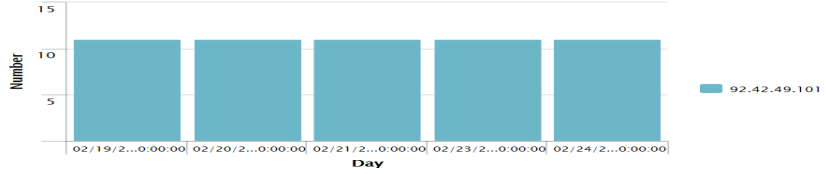
Connections from high-risk IPs

<1m ago

Source	month_day	Session_ID	Acct_Name_Logged_Into
Amazon Web Services	february 25	123099	Robert Gold
Amazon Web Services	february 19	123099	Robert Gold
Amazon Web Services	february 20	123099	Robert Gold
Amazon Web Services	february 21	123099	Robert Gold
Amazon Web Services	february 22	123099	Robert Gold
Amazon Web Services	february 24	123099	Robert Gold

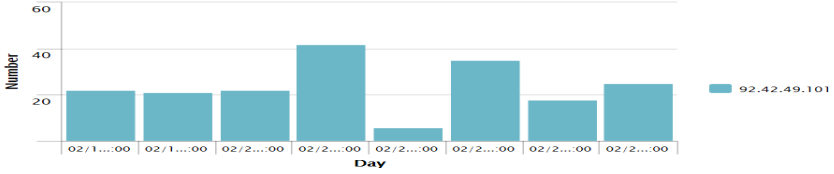
IPs Accessing Excessive Number of Accounts (over 5 in a day)

<1m ago



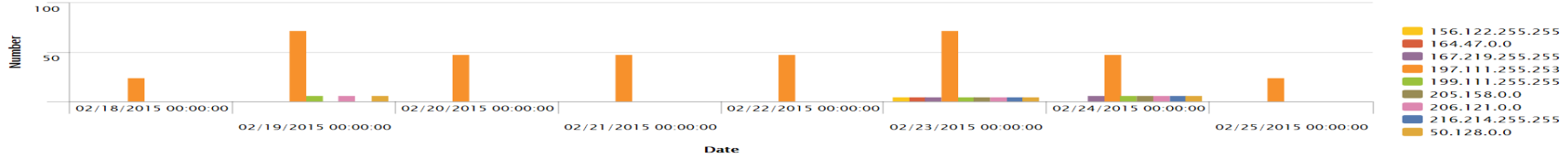
Excessive Failed Logins from Single IP (over 5 in a day)

<1m ago



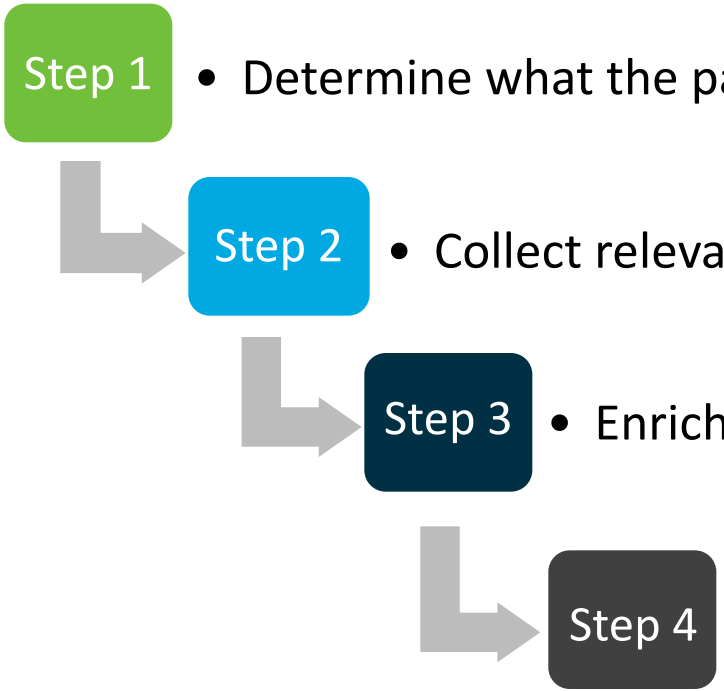
Single IPs Creating Excessive Accounts (over 10 in a day)

<1m ago



About Support File a Bug Documentation Privacy Policy

How to Detect Fraud Using Machine Data



- Determine what the patterns of fraud are for the specific organization
- Collect relevant machine/structured data in one location
- Enrich with external content (threat intel, HR, asset info)
- Detect and alert on patterns of fraud

Reality of Detecting Fraud

- No easy button
- Requires people, process, technology
- Big data is only as good as the data in it and people behind the UI
- Sophisticated, highly technical fraudsters are difficult to catch

DB CONNECT IN THE BIG PICTURE

PREMIUM CONTENT

- Security & Compliance
- Application & Infrastructure
- Business Analytics
- Internet of Things

FOUNDATION (FREE)

- App for Stream, App for AWS, App for MINT, …
- Add-ons for Unix, Windows, OPSEC LEA, JMX, …
- DB Connect, ODBC, Add-on for Amazon Web Services, …

splunk>

THE NEW STUFF

Security

- Simplified architecture reduces potential for security and stability issues
- Enabled use of SSL for many back ends
- Identities improve access control abstraction
- Clarified ownership and rights of objects in the add-on

Scalability

- Resource pool system allows job dispatching to multiple DB Connect nodes
- New architecture allows install in clustered environments

Ease of Use

- New user interface makes it easy to configure and edit data connections
- Health dashboard makes it easy to troubleshoot problems

Increased back end support

- Back end abstraction makes it easier to add new connections
- Added Postgres
- Added MemSQL
- Added Teradata
- Added Informix

Configuration Files

1.x.x

$SPLUNK_HOME/etc/apps/**dbx**/README/*.spec

- database.conf
- database_types.conf
- dblookup.conf
- inputs.conf
- java.conf

2.x.x

$SPLUNK_HOME/etc/apps/**splunk_app_db_connect**/README/*.spec

- db_connections.conf
- db_connection_types.conf
- healthlog.conf
- identities.conf
- inputs.conf

Database Connections (1 of 2)

1.x.x

database_types.conf

- Lists the supported database types, driver parameters, test queries

database.conf

- All configuration necessary for connecting to a specific database

2.x.x

db_connection_types.conf

- Lists the supported database types, driver parameters, test queries

db_connections.conf

- All configuration necessary for connecting to a specific database, *unless overridden by parameters from identities.conf*

identities.conf

- Username and password used to connect to the database (stored in standard Splunk credential store)

Pre-Login Clicks
Frontend=1234

Login Page Click
Username=Newman
Frontend=5678

Post Login Clicks
Frontend=9012

CheckOut Clicks
Frontend=9012

1. Group sessions (frontend) into clickstreams
2. Maintain context such as Username
3. Build viz/kfi/rules against clickstreams

*** Hint: There is a handoff between sessions