



# Don't Blow Your Budget Fighting Fraud

Matthew J Joseff, CFE

Director N. Asia, Korea, & Japan Specialists | Splunk

Abhishek Dujari

Sr. Security Specialist | Splunk

# Forward-Looking Statements

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 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.

Splunk, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2019 Splunk Inc. All rights reserved.

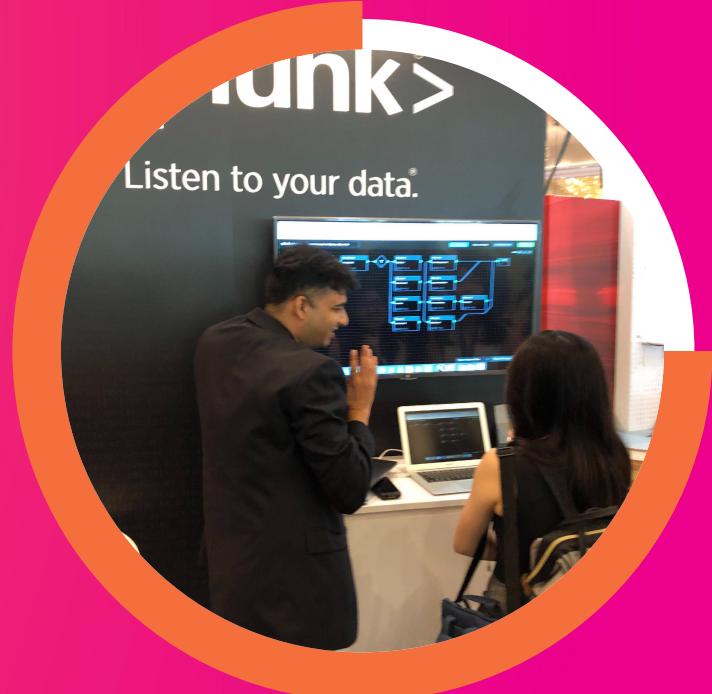
.conf19

splunk>



## Matthew J Joseff

Director N. Asia & Japan Specialists | Splunk

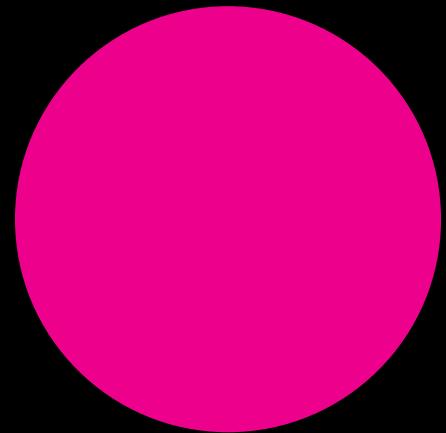


## Abhishek Dujari

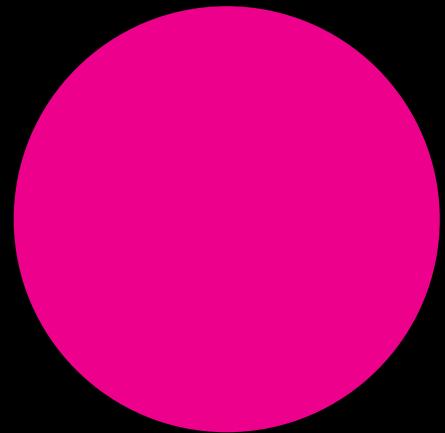
Sr. Security Specialist | Splunk

# Agenda

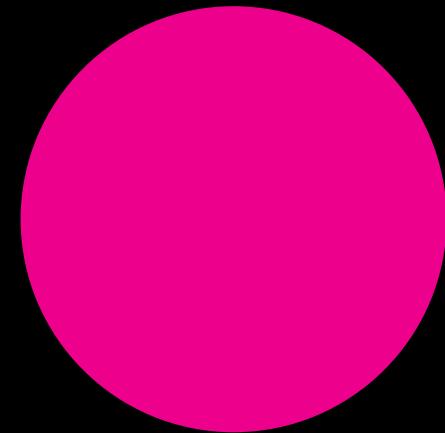
Why are you here?



Fraud Overview



Automating



Demo

# Fraud

---

The daughter of greed

.conf19

splunk>



# What is Fraud?

Let's define what we're talking about

- ▶ **1a** : DECEIT, TRICKERY; *specifically* : intentional perversion of truth in order to induce another to part with something of value or to surrender a legal right
  - was accused of credit card *fraud*
  - **b** : an act of deceiving or misrepresenting:
    - TRICK
      - automobile insurance *frauds*
- ▶ **2a** : a person who is not what he or she pretends to be : IMPOSTOR He claimed to be a licensed psychologist, but he turned out to be a *fraud*.; *also* : one who defrauds : CHEAT
  - **b** : one that is not what it seems or is represented to be The UFO picture was proved to be a *fraud*.

# Compliance, Security, Fraud

What's the difference?

## Compliance



## Security



## Fraud

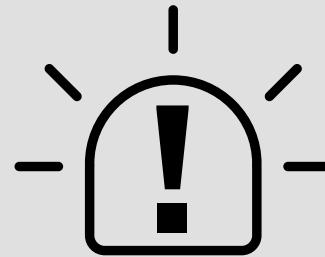


# Example Patterns of Fraud in Machine Data

Industry	Type of Fraud	Pattern of fraud
 <b>Financial Services</b>	<b>Account takeover</b>	Abnormal velocity or \$ of transaction
 <b>Healthcare</b>	<b>Physician billing</b>	Physician billing for drugs outside their expertise area
 <b>E-tailing</b>	<b>Account takeover</b>	Many accounts accessed from one IP or user agent string
 <b>Telecoms</b>	<b>Roaming abuse</b>	Excessive roaming on partner network by unlimited use customers
 <b>Online education</b>	<b>Student loan fraud</b>	Student with loans has IP in high-risk country and is absent from classes & assignments

# Fraud is Pervasive and Costly

- External & internal
- Types: Account takeover, credit card, wire transfer, money laundering, education loans, insurance, healthcare, and more
- No industry or region is immune



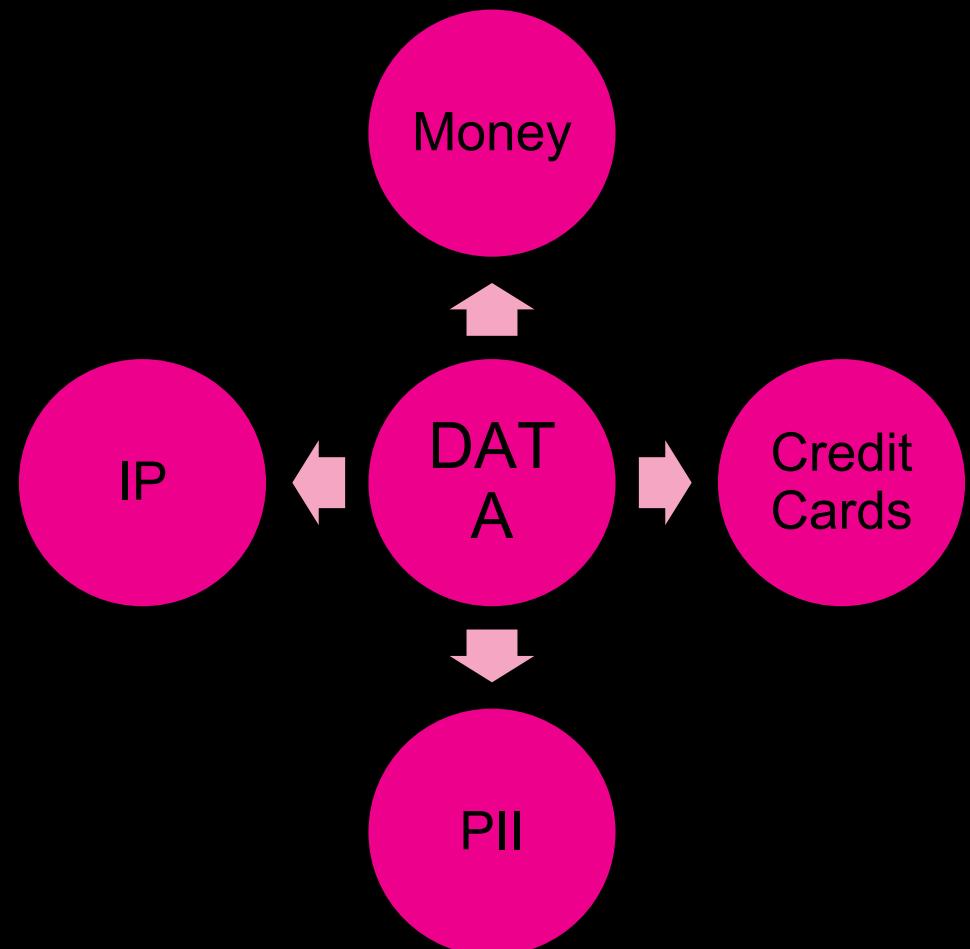
- Cost/dollar of fraud loss<sub>(avg)</sub>: \$3.50<sub>1</sub>
- Growing: 
- 9%<sub>2</sub>
- Reputation/brand damage



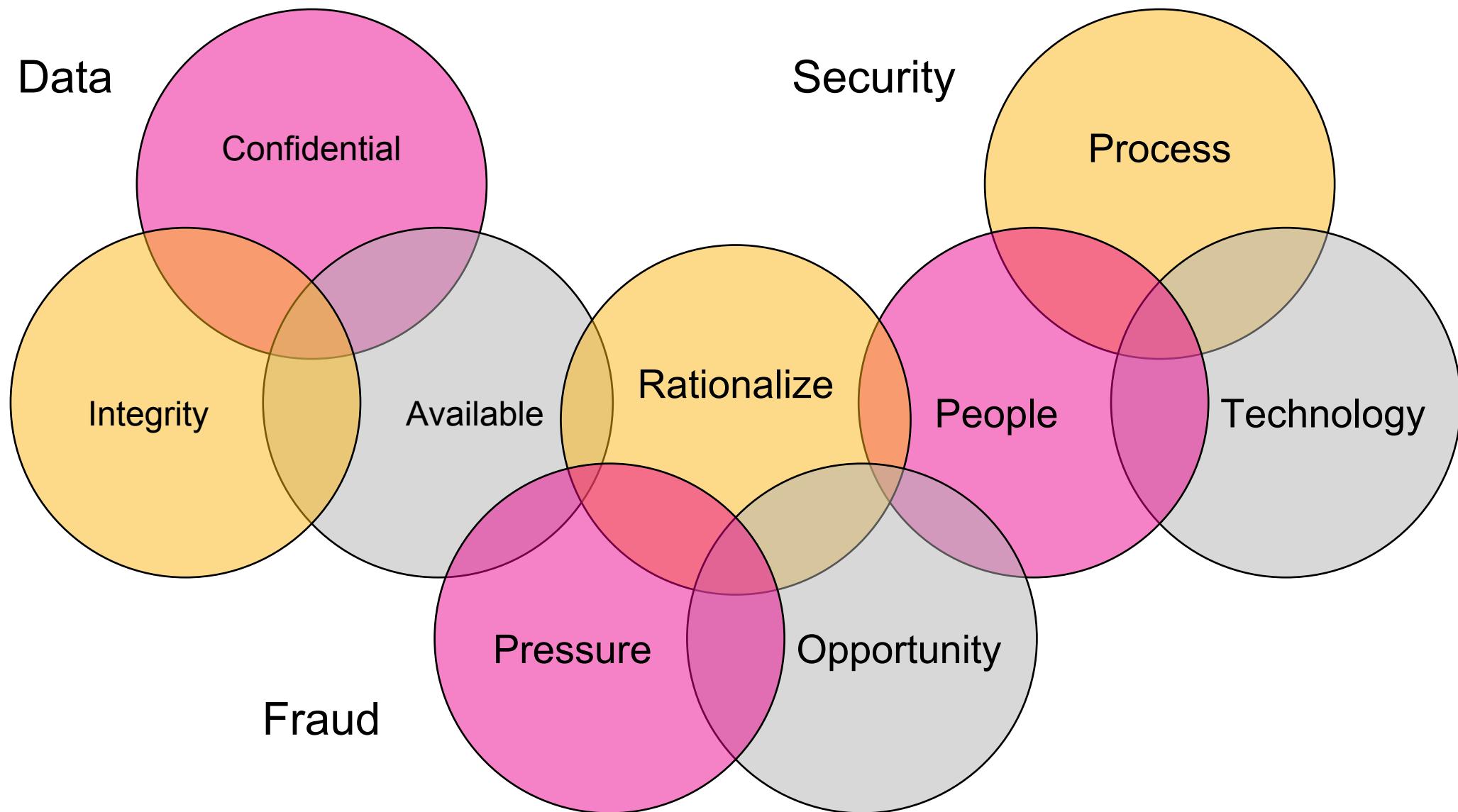
- Association of Certified Fraud Examiners  
1. LexisNexis Risk Solutions 2018 True Cost of Fraud Study  
2. LexisNexis Risk Solutions 2018 True Cost of Fraud Study

# What are you protecting?

92% of money is data



# Interrelated Components of Fraud



A collage of nine photographs showing various building entrances and doorways. The styles range from modern red brick to classical stone and wood. The doors are painted in a variety of colors including red, green, blue, and black. Some have arched windows above them. A central black rectangular box contains the text.

# Access Points



# **Egress & Ingress Data**

# Risk Based Approach

How easy is it to walk?



## Payment Cards: Anomalous Transactions - 3D

Clustering Algorithm

KMeans k=18

Select time period (of available data)

Last 24 hrs (full txn data)

Submit

Hide Filters

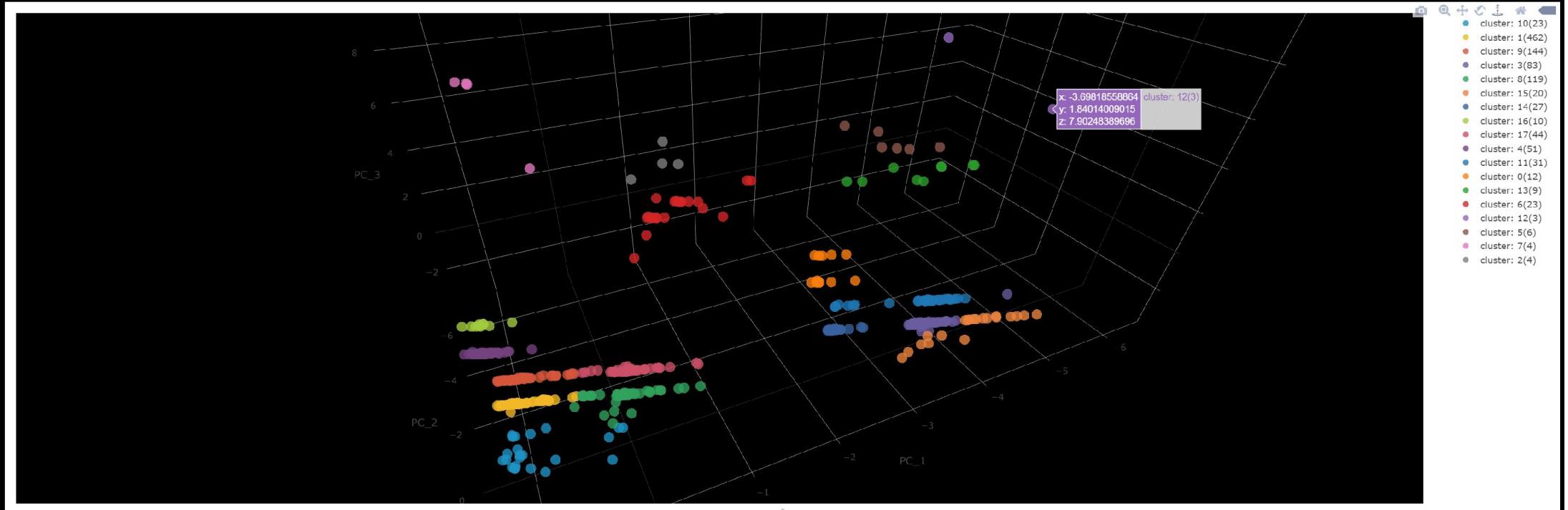
Edit Export ...

(Reset Dashboard)

3D view of data clusters

# Transform Your Data

## Set your own reality



## Detected Anomalies:

	PC_1	PC_2	PC_3	cluster	_time	card_number_masked	compromise_type	txn_region	region_change	merchant_change	merchant_name	txn_terminal_id	time_delta	txn_type	txn_amount	txn_min_max_avg
1	-3.69818558864	1.84014009015	7.90248389696	12(3)	2017-03-10 21:43:00	CARD010600920408030		US	1	1	WM SUPERCENTER #	0W000357930004	47	PURCHASE	45.0	3.37 / 128.22 / 30.26
2	-3.81810533094	1.85866264517	7.82107865432	12(3)	2017-03-19 15:35:34	CARD010600924668027		US	1	1	WM SUPERCENTER #	0W000320260012	43	PURCHASE	50.0	2.06 / 131.0 / 22.97
3	-2.75726098295	0.95874873927	9.98585473828	12(3)	2017-03-17 18:31:34	CARD010600926071014		US	0	0	WM SUPERCENTER #	0W000320260002	55	PURCHASE	100.0	1.68 / 500.0 / 22.37
4	1.03352279421	7.28241919574	0.965314069716	2(4)	2017-04-17 04:35:58	CARD010529244010		PR	0	0	BURGER KING 4978	300V5009	413490	PURCHASE*	3.33	3.33 / 149.84 / 29.01
5	-1.69742835467	-7.13687324121	1.40936879098	2(4)	2017-04-06 19:28:45	CARD010600924668027		PR	0	0	ECONO PONCE ECR	IIATIBTRN00010003	24165	P CSH BACK	41.02	2.06 / 131.0 / 22.97
6	-1.47003123285	-7.17256131112	1.57935592253	2(4)	2017-04-19 19:18:14	CARD010600924668027		PR	0	0	ECONO PONCE ECR	HATHIBTRN00010003	13546	P CSH BACK	17.58	2.06 / 131.0 / 22.97
7	-1.49407942138	-7.13030794842	2.72618418865	2(4)	2017-02-17 09:57:13	CARD010600926385018		PR	0	0	ECONO AGUAS BUENAS	30V29301	1725	P CSH BACK	11.1	2.01 / 170.0 / 20.31
8	0.719092413593	-0.0300507904028	9.94790513374	7(4)	2017-03-22 13:52:44	CARD010591538040	fraud	PR	0	0	NATIONAL LUMBER AGUAS B	7147J803	50	PURCHASE	5.87	5.11 / 181.52 / 26.94
9	0.462247005604	0.296467092427	7.07100406282	7(4)	2017-02-12 12:59:56	CARD010600924668027		PR	0	1	THE HOME DEPOT SPANISH	06217216	47	PURCHASE	16.15	2.06 / 131.0 / 22.97

## Patient Claims, Cost and Diagnosis Anomaly Investigator - 3D

Edit Export ...

Clustering Algorithm

KMeans k=18

Select time window

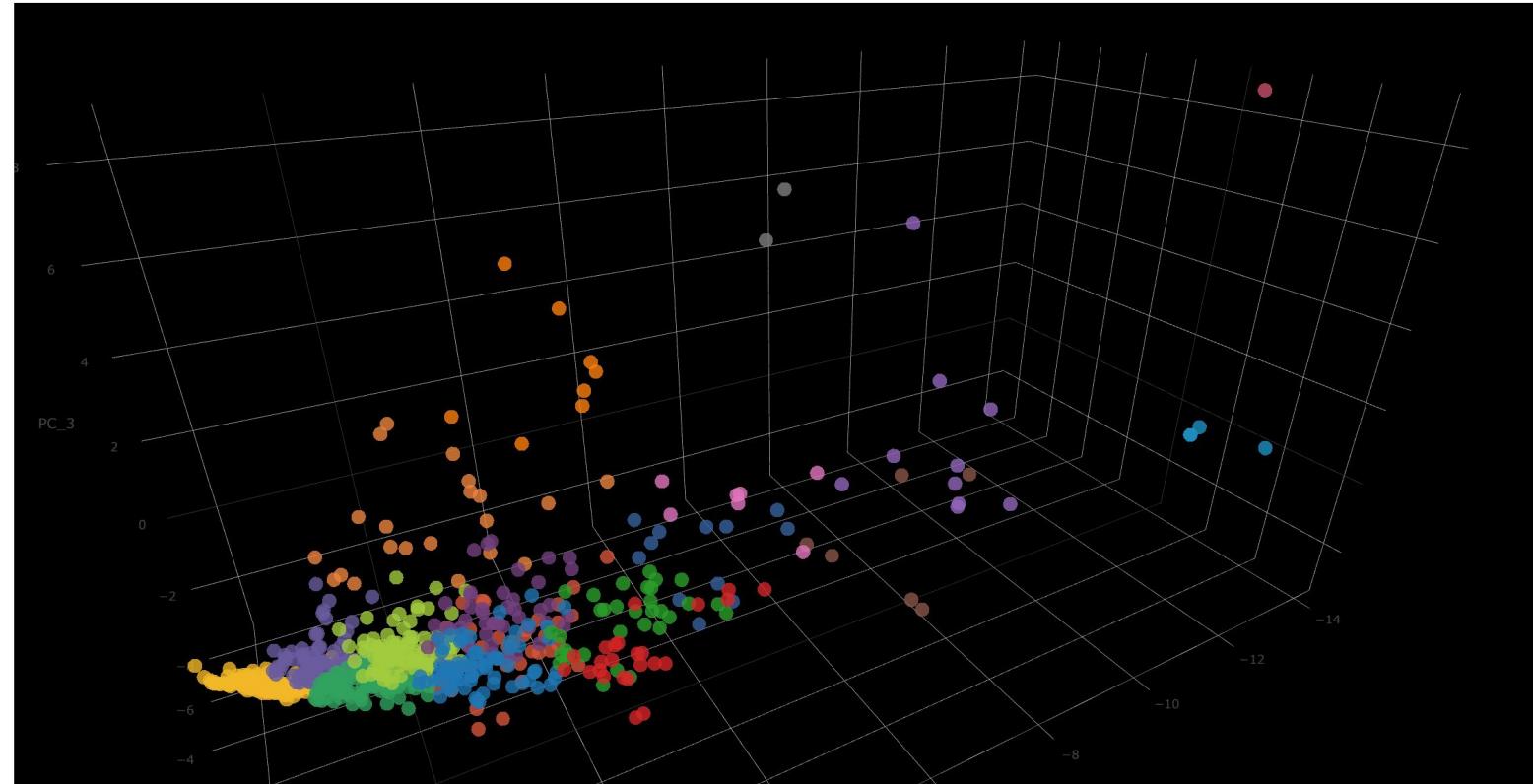
Last 7 days

Submit

Hide Filters

[Reset Dashboard](#)

Clustered Claims Data by: Total \$ amount paid out, Insurance \$ cost, Patient co-pay amount, Primary diagnosis codes used, Secondary diagnosis codes used, Drug codes used.



- cluster: 13(4 elements)
- cluster: 4(276 elements)
- cluster: 16(44 elements)
- cluster: 1(144 elements)
- cluster: 8(198 elements)
- cluster: 15(21 elements)
- cluster: 9(12 elements)
- cluster: 12(91 elements)
- cluster: 10(1 elements)
- cluster: 6(47 elements)
- cluster: 2(73 elements)
- cluster: 5(8 elements)
- cluster: 17(33 elements)
- cluster: 14(24 elements)
- cluster: 3(10 elements)
- cluster: 0(6 elements)
- cluster: 11(7 elements)
- cluster: 7(2 elements)

## Detected Anomalies:

	PC_1 (x) ◁	PC_2 (y) ◁	PC_3 (z) ◁	cluster ◁	ENROLID ◁	TOTCOST ◁	copaytot ◁	ingtot ◁	netpaytot ◁	num_drug ◁	num_dx ◁	num_proc ◁
1	-13.9460300716	1.23333181943	8.66409981836	10(1 elements)	853532301	175370.98	778.15	9067.79	165525.04	10	17	72
2	-7.28332188576	-6.80316072015	4.81332180042	7(2 elements)	884268802	55297.46	638.34	24346.42	30312.7	22	23	32
3	-8.20940917125	-8.55247798253	5.66966119146	7(2 elements)	2059938602	61514.4	606.31	27938.93	32969.16	39	13	30
4	-13.1334643037	2.24187114206	0.225561438913	13(4 elements)	1064879704	91184.11	56.89	6551.5	84575.72	62	46	141
5	-11.18554131149	6.11646101014	1.87965286941	13(4 elements)	25433641701	109547.29	150.89	730.97	108665.43	15	50	145
6	-12.10046160077	0.21187114206	0.005561438913	13(4 elements)	1064879704	91184.11	56.89	6551.5	84575.72	62	46	141

# “Machine Generated Data is a Definitive Record of Human-to-Machine and Machine-to-Machine Interaction”

---

Data defines reality

# The Fight

---

Be like water

.conf19

splunk>



# Three Questions

Let's get to know each other



What kind of Fraud?



How do you know it  
exists?



How much does it cost?

# If Time Is Money

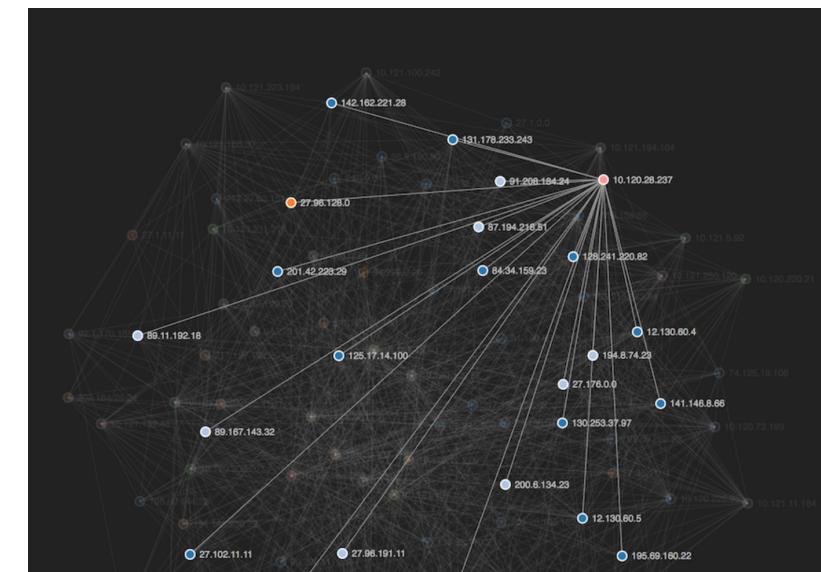
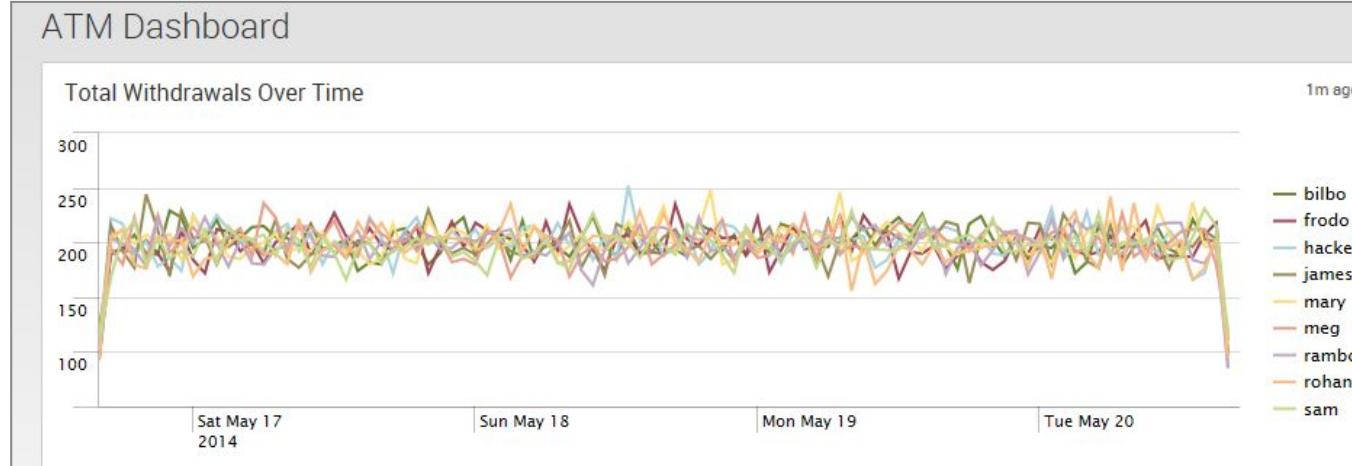
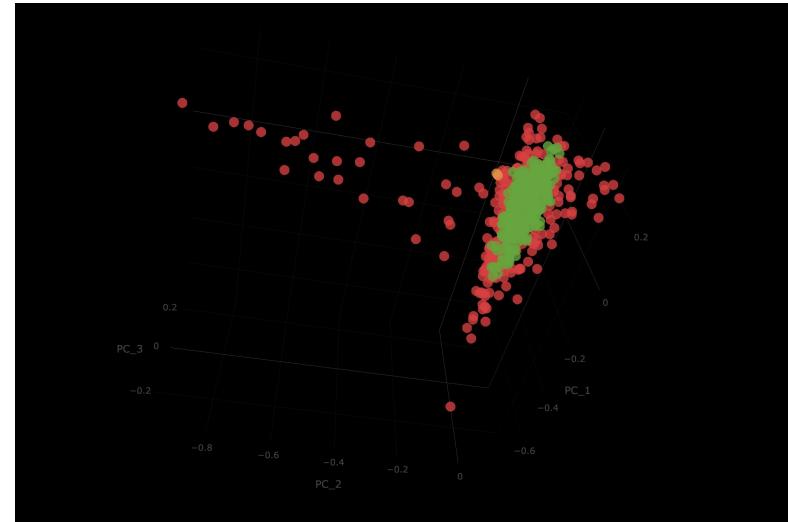
How do you spend your time?

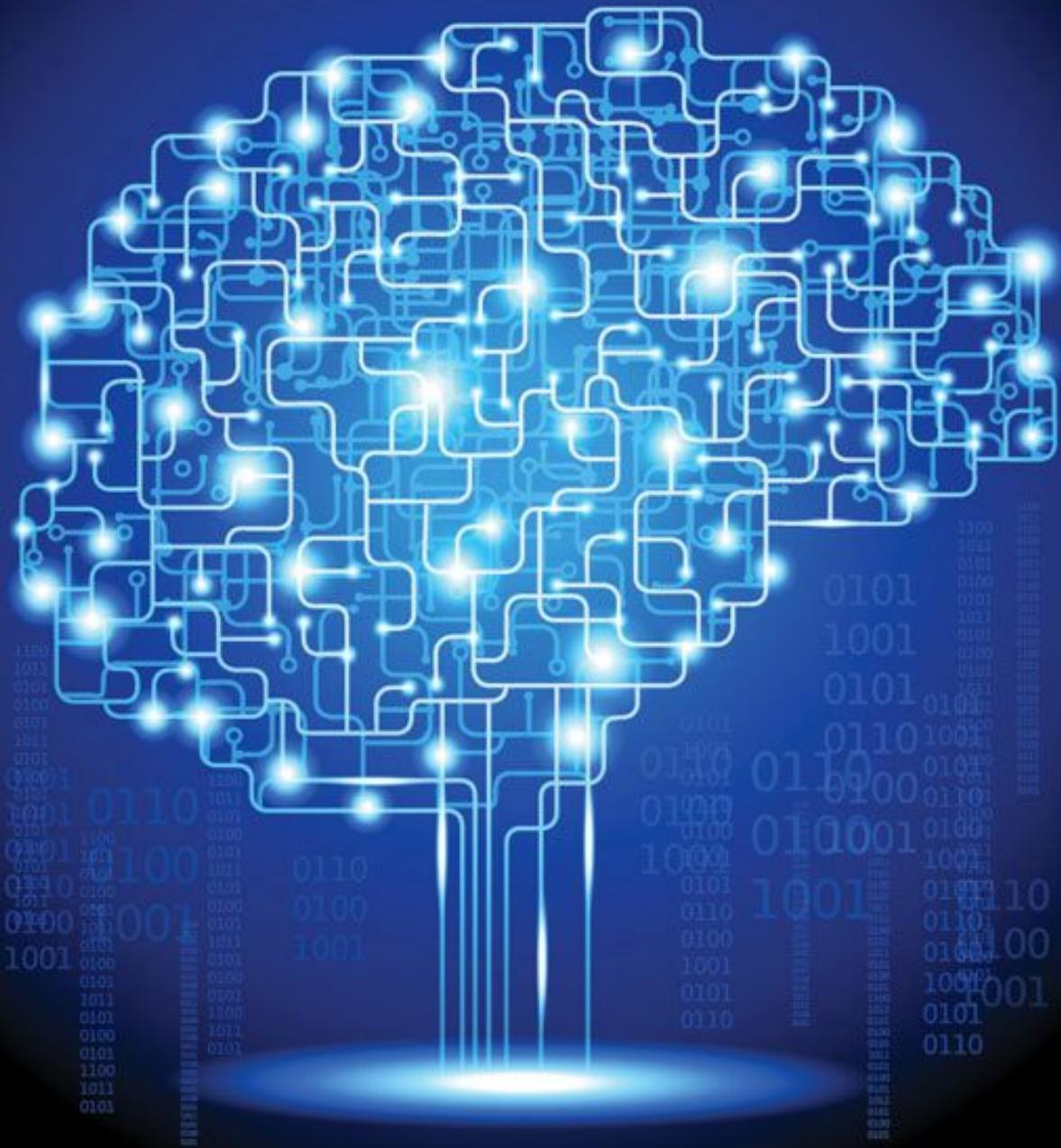


# Fraud Investigations



# Fraud Analytics and Reporting





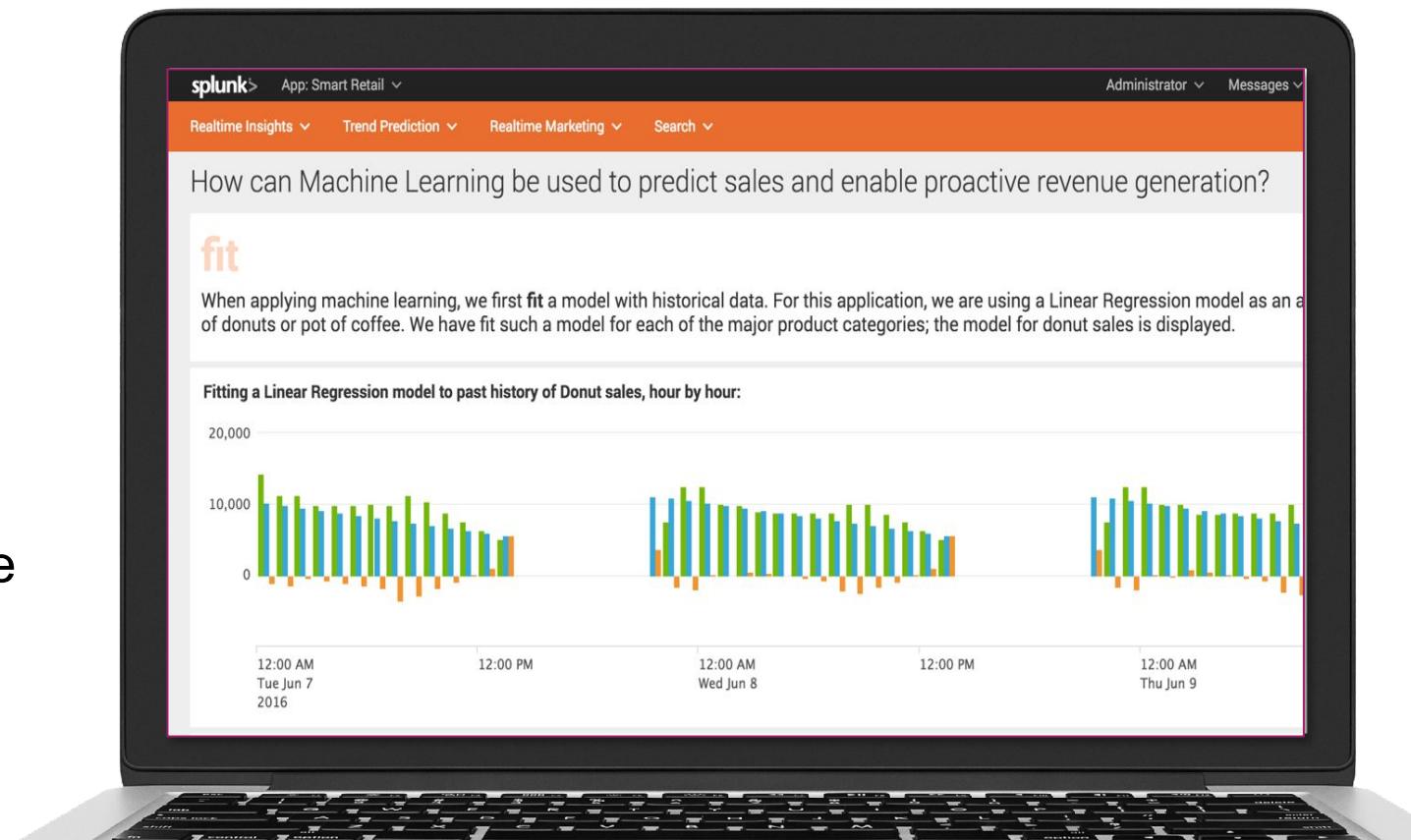
# Machine Learning

Automating analytical model building using algorithms that iteratively learn from data without requiring explicit programming

# Splunk Machine Learning Toolkit

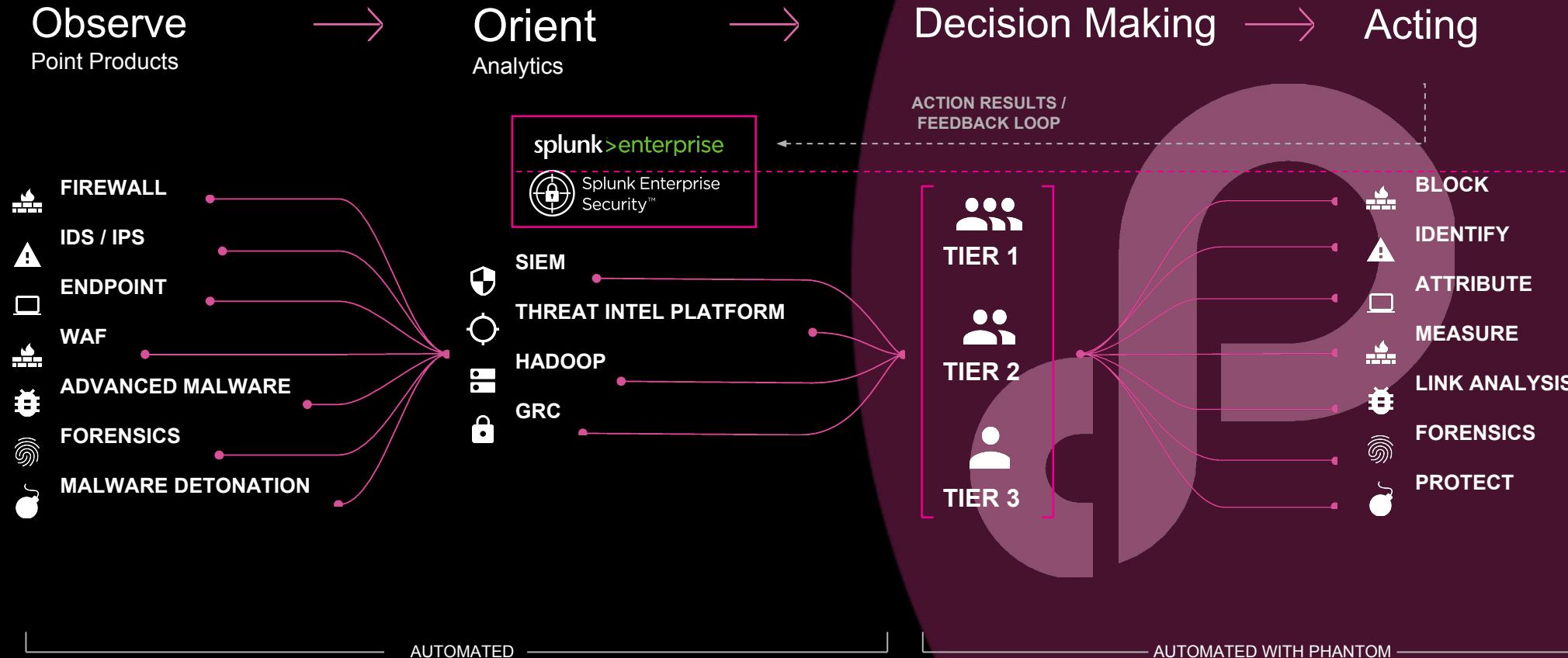
Guided and easy-to-use interface, modeling assistance and ready-to-use examples

- ▶ **Showcases:** Interactive examples for common IT, security, business and IoT use cases
- ▶ **Assistants:** Guided model building, testing and deployment
- ▶ **Models:** Includes 25+ standard algorithms
- ▶ **Commands:** SPL commands to fit, test and operationalize models
- ▶ **Free:** Machine Learning Toolkit available via the Splunkbase™ app ecosystem



# SOAR for Security Operations

Faster execution through the loop yields better security



# How it Works

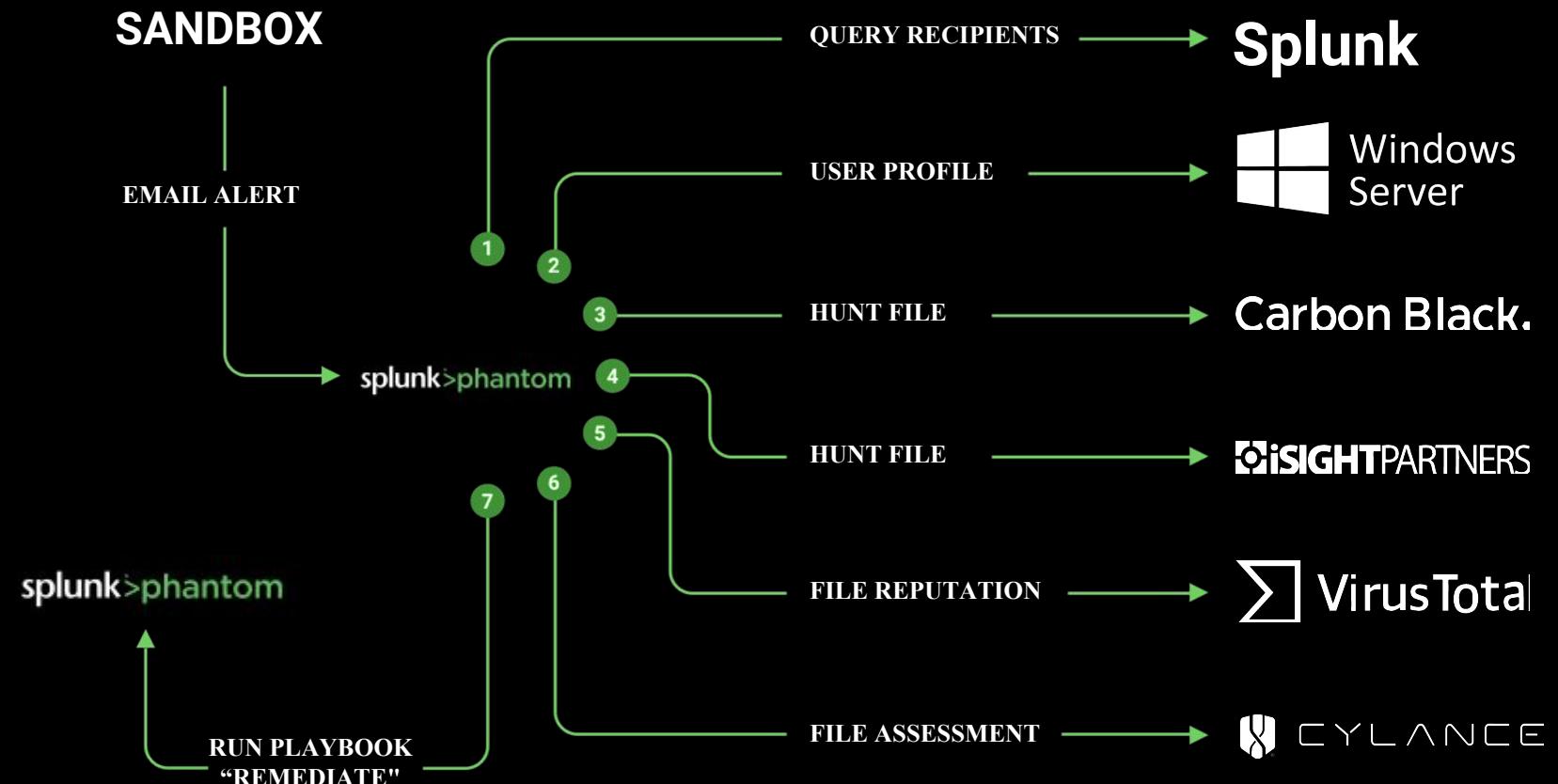
## A Phantom Case Study

### Automated Fraud Investigation

"Automation with Phantom enables us to process malware email alerts in about 40 seconds vs. 30 minutes or more."

**Adam Fletcher**  
CISO

Blackstone



# Call to Action!

---

Put that in your | and Splunk it.





# Splunk Security Essentials

<https://splunkbase.splunk.com/app/3435/>

## Identify bad guys in your environment:

- ✓ 45+ use cases common in UEBA products, all free on Splunk Enterprise
- ✓ Target external attackers and insider threat
- ✓ Scales from small to massive companies
- ✓ Save from the app, send results to ES/UBA



You can solve use cases today for free, then use Splunk UBA for advanced ML detection.

splunk > App: Splunk Security Essentials

Introduction Use Cases Assistants Search Setup Administrator Messages

### Use Cases

All Examples (47 examples) Access Domain (11 examples) Data Domain (6 examples) Endpoint Domain (20 examples) Network Domain (9 examples) Threat Domain (3 examples)

#### Highlights

**Authentication Against a New Domain Controller**  
 A common indicator for lateral movement is when a user starts logging into new domain controllers.  
 Alert Volume: Medium  
 Examples:  

- Demo Data
- Live Data

**Concentration of Hacker Tools by Filename**  
 It's uncommon to see filenames associated with attacker tools used in rapid succession on an endpoint. The first time, it's probably fine. The fourth or fifth file used should be suspicious. (MITRE CAR Reference)  
 Alert Volume: Low  
 Examples:  

- Demo Data
- Live Data

**Detect Data Exfiltration**  
 Find users who are exfiltrating data.  
 Splunk UBA Use Case

**First Time Accessing a Git Repository**  
 Finds users who accessed a git repository for the first time.  
 Alert Volume: High  
 Examples:  

- Demo Data
- Live Data
- Accelerated Data

**First Time Accessing a Git Repository Not Viewed by Peers**  
 Finds users who accessed a git repository for the first time, where their peer group also hasn't accessed it before.  
 Alert Volume: Medium  
 Examples:  

- Demo Data

**First Time Logon to New Server**  
 Finds users who logged into a new server for the first time.  
 Alert Volume: Very High  
 Examples:  

- Demo Data
- Live Data
- Accelerated Data

**Healthcare Worker Opening More Patient Records Than Usual**  
 If a healthcare worker (or someone associated, such as a DBA) views more patient records than normal, or more than their peers, then it could be a sign that their system is infected, or that they are exfiltrating patient data.  
 Alert Volume: Low  
 Examples:  

- Demo Data
- Live Data

**Increase in Pages Printed**  
 Finds users who printed more pages than normal.  
 Alert Volume: Medium  
 Examples:  

- Demo Data
- Live Data
- Accelerated with Data Models

**Anomalous New Listening Port**  
 New listening ports can be a sign of malware persistence, so detect them in your data!  
 Alert Volume: Medium  
 Splunk ES Use Case

**Concentration of Discovery Tools by Filename**  
 It's uncommon to see filenames associated with host discovery tools used in rapid succession on an endpoint, except in very specific situations. The first time, it's probably fine. The fourth or fifth file used should be suspicious. (MITRE CAR Reference)  
 Alert Volume: Low (unless your company specifically does this)  
 Examples:  

- Demo Data
- Live Data



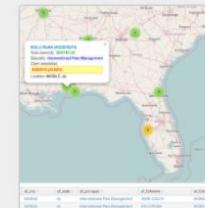
# Splunk for Fraud Detection

<https://splunkbase.splunk.com/app/3693/>

Learn how Splunk Enterprise may be used to detect various forms of fraud using the example scenarios.



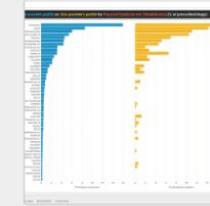
## Healthcare Fraud



Find anomalous healthcare providers

Find nationwide and statewide anomalies in prescription drug claims

6.5 6.6 7.0

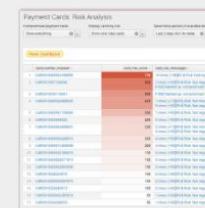


Investigate specific healthcare provider

Find all prescription claims, compare specific provider profile to typical nationwide or statewide profile

6.5 6.6 7.0

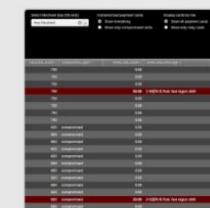
## Payment Cards Fraud



Risk scoring of payment cards

Show most risky payment cards with summary details of activity for each card

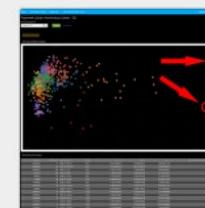
6.5 6.6 7.0



Detailed card transactions

Show detailed transaction activity of every payment card. Mark compromised payment cards.

6.5 6.6 7.0



Detect anomalous payment cards

Leverage unsupervised learning to discover anomalously behaving payment cards

6.5 6.6 7.0



Risk analysis of merchants and payment terminals

Analyze risk factors and predisposition to fraudulent activity of specific merchant and payment terminal.

6.5 6.6 7.0

# “Machine Generated Data is a Definitive Record of Human-to-Machine and Machine-to-Machine Interaction”

---

Data defines reality

# Thank You & Demo

splunk>