



# Surprise and Consequences

Breaking through Analysis Paralysis

Joel M. Fulton, PhD | Chief Information Security Officer @ Splunk

Grant Wernick | Chief Executive Officer @ Insight Engines

September 26, 2017

# TURNING DATA INTO ANSWERS

# Agenda

**Patterns of Analysis  
Failure**

Joel M. Fulton, Splunk CISO

**Demo Cyber Security  
Investigator**

Grant Wernick, Insight Engines  
CEO

**Applying CSI, Achieving  
Excellence**

Joel M. Fulton, Splunk CISO

**Next gen Intelligence  
Augmentation**

Grant Wernick, Insight Engines  
CEO

**Q&A**



# Security Intelligence Operations



```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-03" "Mozilla/5.0 (Windows NT 6.0; rv:1.9.0.8) Gecko/20100801/Firefox/3.6.8"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD5L9FF1ADFF3" "Mozilla/5.0 (Windows NT 6.0; rv:1.9.0.8) Gecko/20100801/Firefox/3.6.8"
317.27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 468 125.17 14 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-26&product_id=RP-LI-02" "Mozilla/5.0 (Windows NT 6.0; rv:1.9.0.8) Gecko/20100801/Firefox/3.6.8"
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-03" "Mozilla/5.0 (Windows NT 6.0; rv:1.9.0.8) Gecko/20100801/Firefox/3.6.8"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD5L9FF1ADFF3" "Mozilla/5.0 (Windows NT 6.0; rv:1.9.0.8) Gecko/20100801/Firefox/3.6.8"
317.27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 468 125.17 14 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-26&product_id=RP-LI-02" "Mozilla/5.0 (Windows NT 6.0; rv:1.9.0.8) Gecko/20100801/Firefox/3.6.8"
```



# What are we embarrassed about?

- Data completeness
- Thinking like an analyst
- Accurately prioritized and weighted alerting and triage
- Percentages and judgment calls
- The boy who cried wolf: too much or not enough warning?
- Being surprised.

```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15LAF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-5W-03" "Mozilla/5.0 (Windows NT 6.0; rv:1.9.0.1) Gecko/20100101 Firefox/3.5.1; SV1; .NET CLR 1.1.4322)" "0"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 404 322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268product_id=KQ-CU-01" "Mozilla/5.0 (Windows NT 6.0; rv:1.9.0.1) Gecko/20100101 Firefox/3.5.1; SV1; .NET CLR 1.1.4322)" "0"
317.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D55L9FF1ADFF3" "Mozilla/5.0 (Windows NT 6.0; rv:1.9.0.1) Gecko/20100101 Firefox/3.5.1; SV1; .NET CLR 1.1.4322)" "0"
125.17.14.189 - - [07/Jan 18:10:55:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-18" "Mozilla/5.0 (Windows NT 6.0; rv:1.9.0.1) Gecko/20100101 Firefox/3.5.1; SV1; .NET CLR 1.1.4322)" "0"
```

# What's the purpose of intelligence?

- Buy time in order to make the appropriate decisions and take the necessary counter measures to face the threat

- Assume invulnerability, deny danger
- Underestimate hazard
- Over-estimate resiliency

The analyst's rule: don't speak to clearly or precisely about the future. When pressed to do so, lower the probabilities.

Ambiguous warnings protect the individuals but are useless to protect the entity

```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15L9FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-5W-03"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D55L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/category.screen?category_id=GIFTS"
317.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D55L9FF1ADFF3"
10.0.0.1 - - [07/Jan 18:10:56:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3"
10.0.0.1 - - [07/Jan 18:10:56:189] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3"
10.0.0.1 - - [07/Jan 18:10:56:198] "GET /category.remove?itemId=EST-1&product_id=FI-5W-03" 200 3885 "http://buttercup-shopping.com/category.remove?itemId=EST-1&product_id=FI-5W-03"
```

# Grant Wernick

INSIGHT ENGINES CEO

# Darrien Kindlund

INSIGHT ENGINES VP TECHNOLOGY

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category\_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product\_id=FL-SW-01" "Opera/9.80.2013.10; rv:1.9.1.8; Windows NT 6.0; SV1; .NET CLR 3.5.30729; .NET CLR 3.0.30729; .NET CLR 2.0.50727; .NET CLR 1.1.4322" "0"

128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product\_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product\_id=K9-CU-01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_11\_2; rv:53.0) Gecko/20100801 Firefox/53.0" "0"

317.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item\_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/changequantity&itemId=EST-18&product\_id=AV-CB-01&JSESSIONID=SD10SL9FF2ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1" "0"

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category\_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product\_id=FL-SW-01" "Opera/9.80.2013.10; rv:1.9.1.8; Windows NT 6.0; SV1; .NET CLR 3.5.30729; .NET CLR 3.0.30729; .NET CLR 2.0.50727; .NET CLR 1.1.4322" "0"

128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product\_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product\_id=K9-CU-01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_11\_2; rv:53.0) Gecko/20100801 Firefox/53.0" "0"

317.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item\_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/changequantity&itemId=EST-18&product\_id=AV-CB-01&JSESSIONID=SD10SL9FF2ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1" "0"

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category\_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product\_id=FL-SW-01" "Opera/9.80.2013.10; rv:1.9.1.8; Windows NT 6.0; SV1; .NET CLR 3.5.30729; .NET CLR 3.0.30729; .NET CLR 2.0.50727; .NET CLR 1.1.4322" "0"

128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product\_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product\_id=K9-CU-01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_11\_2; rv:53.0) Gecko/20100801 Firefox/53.0" "0"

317.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item\_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/changequantity&itemId=EST-18&product\_id=AV-CB-01&JSESSIONID=SD10SL9FF2ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1" "0"



# Insight Engines Cyber Security Investigator (CSI)

---

# Splunk SPL

If you want to know what vulnerable systems had failed updates

## Construct SPL like this...

```
| tstats allow_old_summaries=t append=t prestats=t summariesonly=t count values(Updates.severity) as Updates.severity from
datamodel=Updates where Updates.status="failure" earliest=06/20/2016:00:00:00 latest=06/27/2016:00:00:00 by Updates.dest,
Updates.signature
```

```
| tstats allow_old_summaries=t append=t prestats=t summariesonly=t count from datamodel=Vulnerabilities where
earliest=06/20/2016:00:00:00 latest=06/27/2016:00:00:00 by Vulnerabilities.dest
```

```
| fillnull value="" Updates.signature
```

```
| eval dest=coalesce('Updates.dest', 'Vulnerabilities.dest'), join_node=if(isnotnull('Updates.dest'), "Updates", "Vulnerabilities")
```

```
| stats count values(Updates.severity) as Updates.severity by dest, join_node, Updates.signature
```

```
| eval count_Updates=if(join_node=="Updates", 'count', null()), count_Vulnerabilities=if(join_node=="Vulnerabilities", 'count', null())
```

```
| stats list(count_Updates) as count_Updates list(Updates.signature) as Updates.signature list(count_Vulnerabilities) as count_Vulnerabilities
values(Updates.severity) as Updates.severity by dest
```






```
| where isnotnull('count_Updates') AND isnotnull('count_Vulnerabilities')
```

```
| stats sum(count) as count
```








# The World With CSI

## Before – SPL

-  Limited value from Splunk
-  Weakened security posture
-  Limited people can get insight
-  Too much time spent on SPL
-  Hard to find/train/retain SPL experts

## After – CSI

-  Full value of Splunk
-  Stronger security posture
-  Data democratization
-  More time investigating/detecting
-  Less reliance on SPL expertise

```

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15LAF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-5W-01"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?category_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=FI-5W-01"
ows NT 27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&item_id=EST-18&product_id=AV-CB-01&JSESSIONID=5D55L9FF1ADFF3"
//buttercup-shopping.com/cl... [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://shopping.com/cart.do?action=changequantity&item_id=EST-18&product_id=AV-CB-01&JSESSIONID=5D55L9FF1ADFF3"
buttercup-shopping.com/cl... [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://shopping.com/cart.do?action=changequantity&item_id=EST-18&product_id=AV-CB-01&JSESSIONID=5D55L9FF1ADFF3"
shopping.com/purchase&i... [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://shopping.com/cart.do?action=changequantity&item_id=EST-18&product_id=AV-CB-01&JSESSIONID=5D55L9FF1ADFF3"
buttercup-shopping.com/cl... [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://shopping.com/cart.do?action=changequantity&item_id=EST-18&product_id=AV-CB-01&JSESSIONID=5D55L9FF1ADFF3"

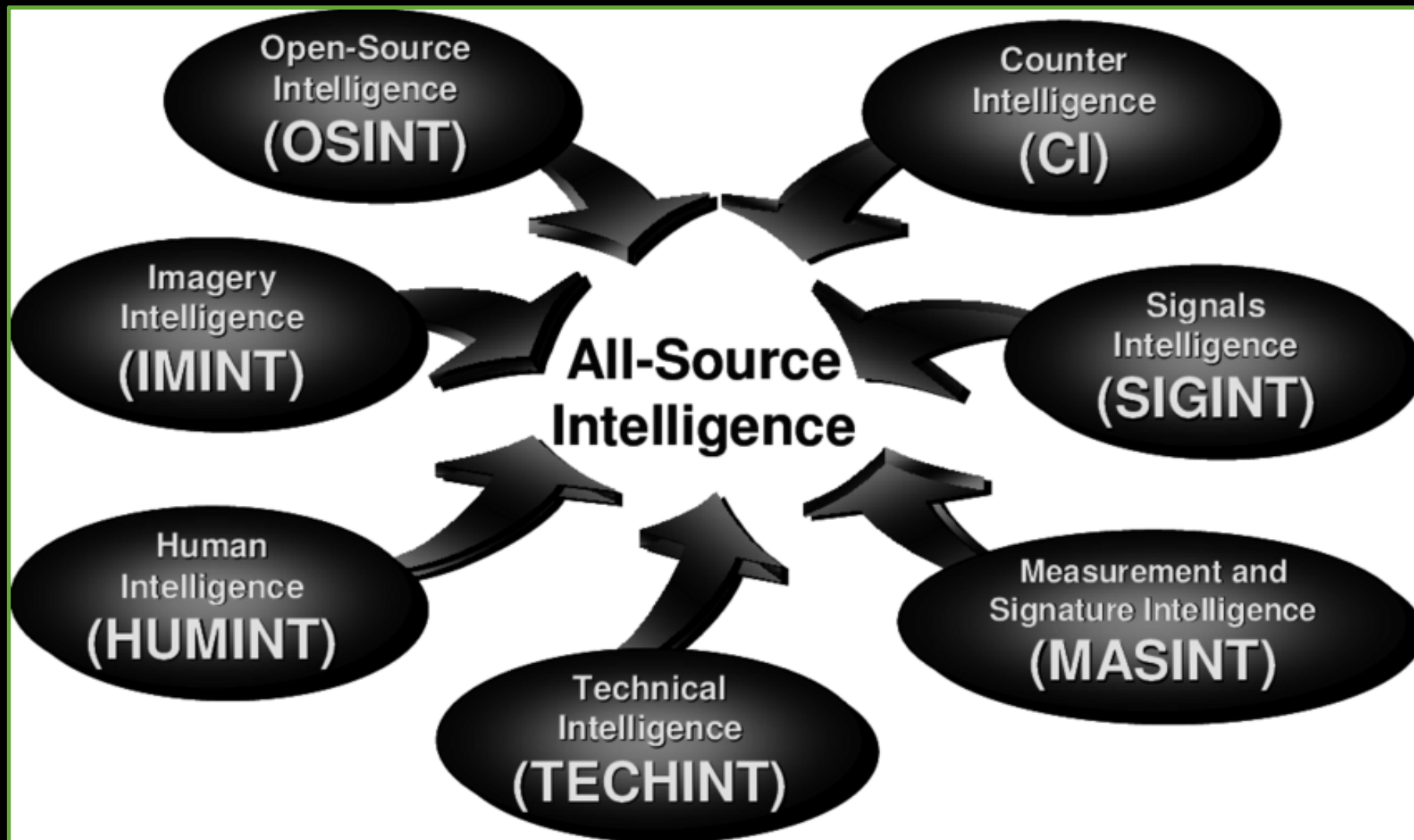
```

# CSI Demo

---

Real time insight engine that understands plain English always learning

# Splunk + CSI + HUMINT + SIGINT => SIO

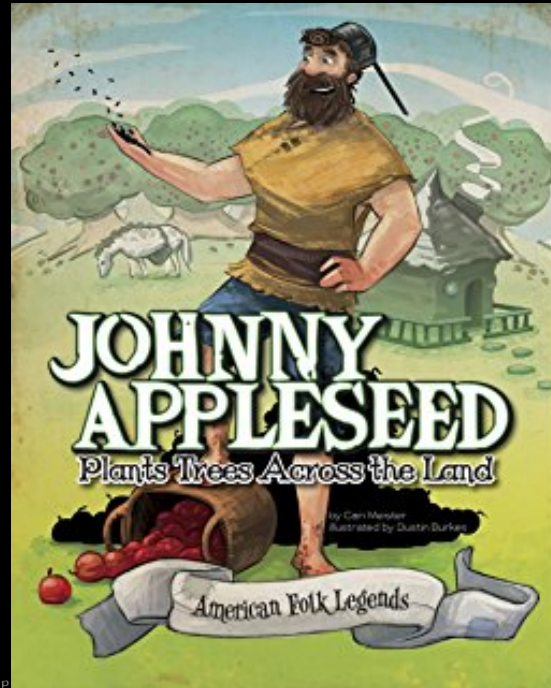
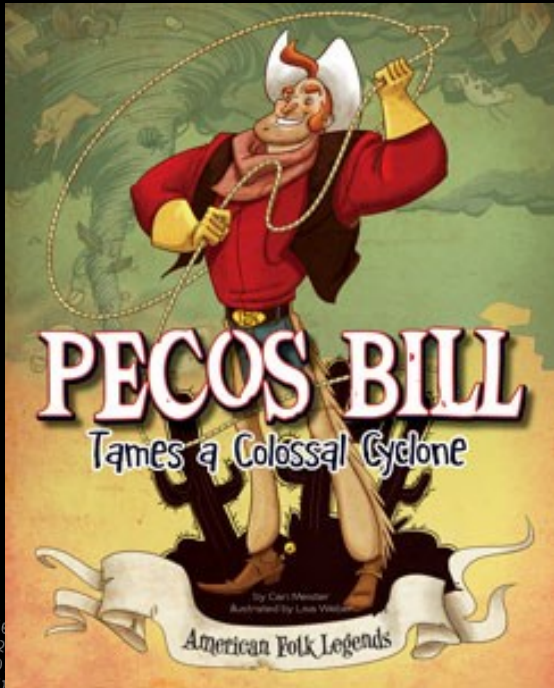
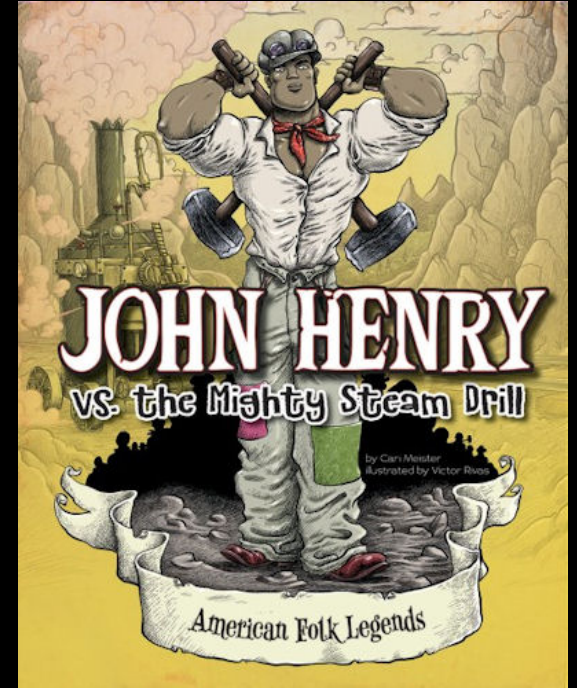
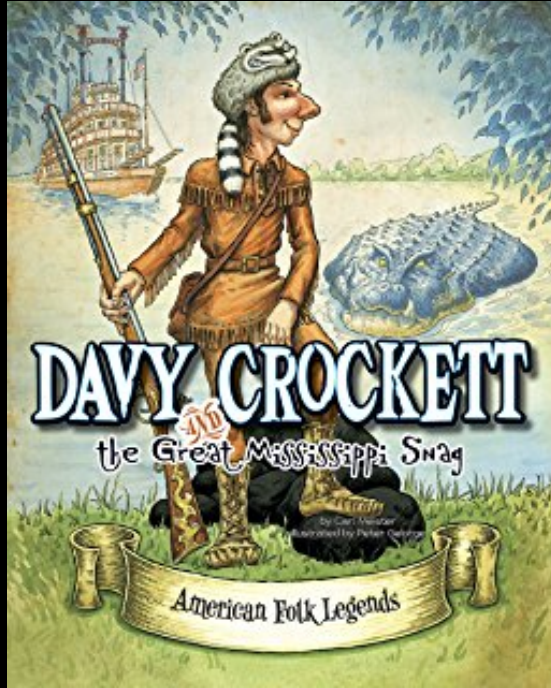


```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD5L9FF1ADFF3 HTTP/1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FL-SW-01" "Opera/9.80.20131026.1040039; rv:1.9.3.6 Presto/2.11.28.33 Version/10.00"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CU-01" "Mozilla/5.0 (Windows NT 6.0; rv:1.9.2.1) Gecko/20100101 Firefox/3.6"
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD5L9FF1ADFF3 HTTP/1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FL-SW-01" "Opera/9.80.20131026.1040039; rv:1.9.3.6 Presto/2.11.28.33 Version/10.00"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CU-01" "Mozilla/5.0 (Windows NT 6.0; rv:1.9.2.1) Gecko/20100101 Firefox/3.6"
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD5L9FF1ADFF3 HTTP/1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FL-SW-01" "Opera/9.80.20131026.1040039; rv:1.9.3.6 Presto/2.11.28.33 Version/10.00"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CU-01" "Mozilla/5.0 (Windows NT 6.0; rv:1.9.2.1) Gecko/20100101 Firefox/3.6"
```

# Building a better Security Intelligence Operations

- There are no such things as cyber-only-risks
- All threats begin with people
- Cyber-analysts understand systems, data, and flow
- Human analysts understand people, motive, and the consequences of intent
- Every company has a physical security “SOC”
- If their HUMINT skills could be applied to SIGINT data, a radical transformation is possible

# Splunk + CSI + HUMINT + SIGINT =>SIO





# Splunk + CSI + HUMINT + SIGINT = >SIO



```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/category.screen?category_id=FL-SW-01"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-D5H-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/category.purchase?category_id=FL-SW-01"
317.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&item_id=EST-188&product_id=AV-CB-01&JSESSIONID=SD10SLAF12ADFF3"
192.168.1.1 - - [07/Jan 18:10:57:123] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/category.purchase?category_id=FL-SW-01"
192.168.1.1 - - [07/Jan 18:10:57:123] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/category.purchase?category_id=FL-SW-01"
192.168.1.1 - - [07/Jan 18:10:57:123] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/category.purchase?category_id=FL-SW-01"
192.168.1.1 - - [07/Jan 18:10:57:123] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/category.purchase?category_id=FL-SW-01"
192.168.1.1 - - [07/Jan 18:10:57:123] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/category.purchase?category_id=FL-SW-01"
```

# ROI By Enabling Physical Security Team

**\$1MM** in savings per year in hiring and training costs

- 40% SOC Analyst Increased Productivity
- 60% Physical Security Analyst Productivity
- 80% Training Reduction

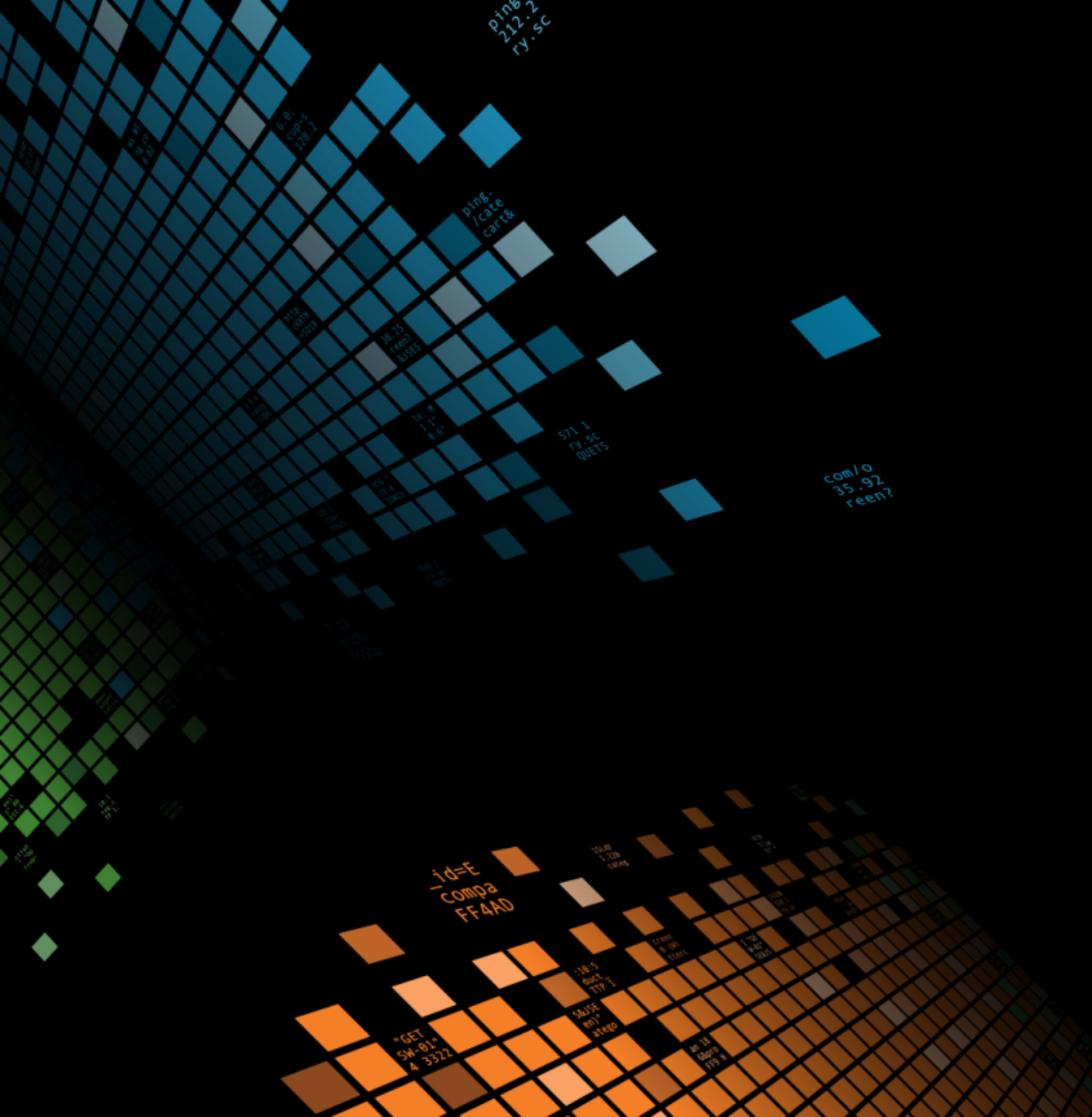


\*Based on enabling physical security team with CSI and hiring more physical security folks to become cyber analysts

# The Next Generation Analyst Workbench

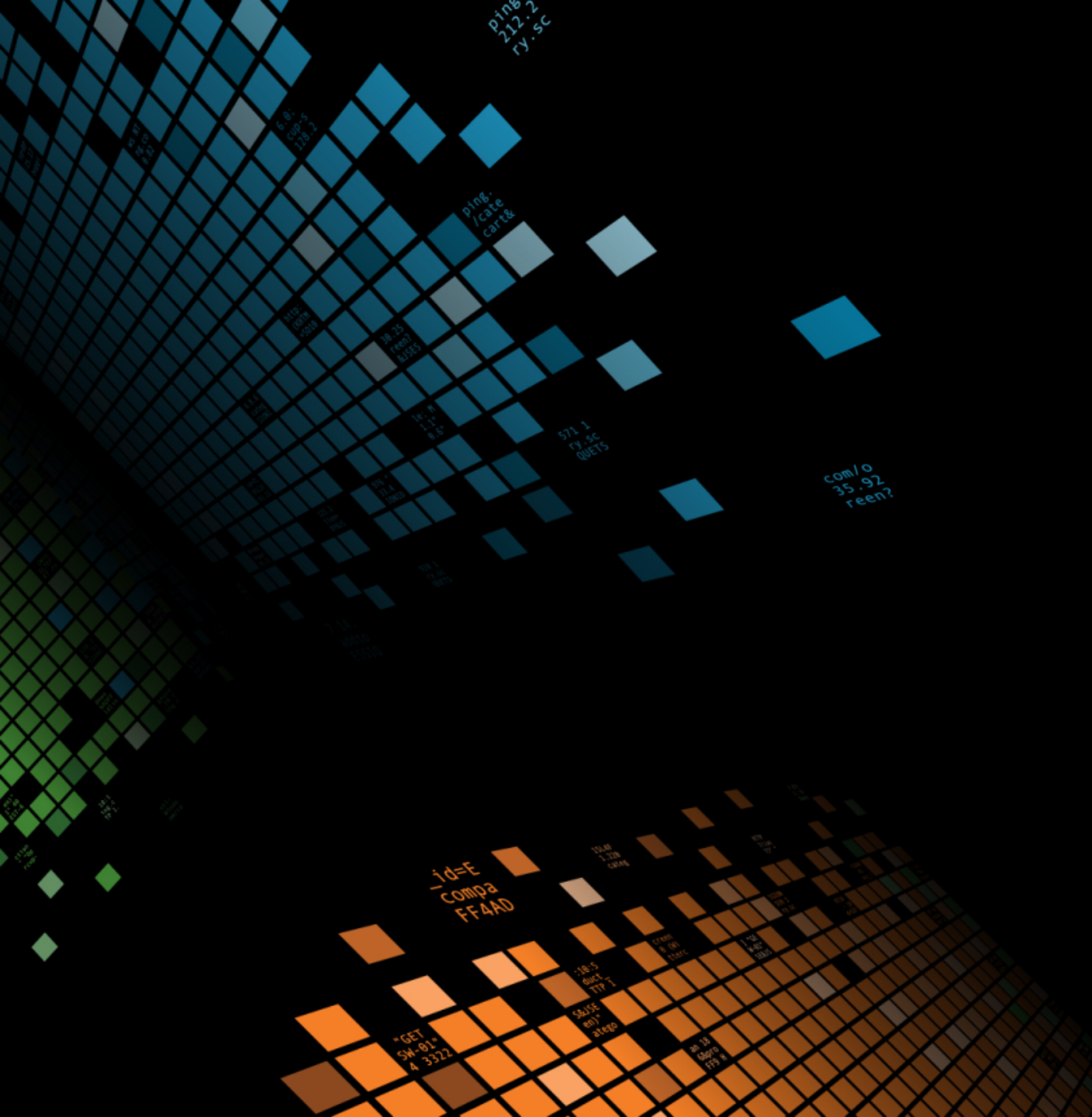
## Hands on Demo





# The Future

---



# Q&A

---

Don't forget to **rate this session** in the  
.conf2017 mobile app

splunk> .conf2017