



# Analytic Stories or How I Learned to Stop Worrying and Respond to Threats

David Dorsey | Principal Research Engineer

September 2017 | Washington DC

# 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. © 2017 Splunk Inc. All rights reserved.

# Who's This Guy?

- ▶ Splunk Security Research Team
  - We really just create memes all day
- ▶ Been around for almost 15 years now, mainly on defensive side
- ▶ RE, IR, File Analysis, Network Analysis, Machine Learning
- ▶ Loves
  - BBQ
  - Pie
- ▶ Dislikes
  - Pants
  - Socks

```

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15L4FF10ADFF10 HTTP/1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FL-SW-01"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD55L7FF6ADFF9 HTTP/1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=Moz11474-0"
317.27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP/1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD10SL9FF2ADFF3"
"itemId=EST-16&product_id=RP-LI-02" 468 125.17.14 [oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP/1.1] 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1"
"do?action=remove&itemId=EST-1" "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD55L9FF1ADFF3 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1"

```



# Level Setting

---

What are we talking about?

# What Should We Take From This Talk

- ▶ Analytic Stories Will Help
  - Demonstrate the value of your data
  - Get value from your data quicker
  - Prioritize data ingestion
  - Understand your defensive posture
  - Resolve incidents faster
  - Empower your analysts

```

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.
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-20&product_id=Mozill1774" "Opera/9.80.
ows NT 5.1; SV1: - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD10SL9FF2ADFF3" "Opera/9.80.
/buttercup-shopping-16&product_id=RP-LI-02" 468 125.17.14.101 [link?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3] "Opera/9.80.
do?action=purchase&itemId=EST-20&product_id=Mozill1774" "Opera/9.80.
/buttercup-shopping.com/cart.do?action=remove&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD10SL9FF2ADFF3" "Opera/9.80.

```

# Why Are We Here

## ► Analytic Story

- It's about understanding, not detection
- Empowering the analyst
- A collection of searches grouped together around a common theme
- Associated metadata
  - References
  - Industry Frameworks
  - Descriptions
  - Data Required

```

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"
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-2&product_id=Moz11474"
ows NT 27.160.0.0 - - [07/Jan 18:10:56:150] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD10SL9FF2ADFF9"
item_id=EST-16&product_id=RP-LI-02" 468 125.17.14 [link?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1"
opping.com/purchase&itemId=EST-16&product_id=RP-LI-02" 468 125.17.14 [link?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1"
http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1"

```

# Words

- ▶ Detection Search
  - Finds a specific behavior
- ▶ Investigative Search
  - Help investigate the detected event
- ▶ Contextual Search
  - Gathers context to enrich the detected event
- ▶ Support Search
  - Helps setup the detection search

```
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/9.80.20  
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5L7FF6ADFF9 HTTP 1.1" 404 3322 "http://shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CU-01" "Mozilla/5.0 (Macintosh; Intel  
ows NT 5.1; SV1; .NET CLR 1.1.4322)" "0" "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD10SL9FF2ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=compute  
/buttercup-shopping.com/cart.do?action=compute&itemId=EST-16&product_id=RP-LI-02" 468 125.17.14 [link?item_id=EST-26&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-6&JSESSIONID=SD10SL9FF2ADFF9 HTTP 1.1" 200 3865 "http://shopping.com/cart.do?action=compute  
opping.com/purchase&itemId=EST-16&product_id=RP-LI-02" "Opera/9.80.20  
/buttercup-shopping.com/cart.do?action=remove&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD10SL9FF2ADFF9 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-6&JSESSIONID=SD10SL9FF2ADFF9 HTTP 1.1" 200 3865 "http://shopping.com/cart.do?action=compute
```





# More Buzz Words

- ▶ Center for Internet Security Critical Security Controls
  - A list of 20 controls to implement to help secure your organization
- ▶ MITRE ATT&CK
  - Adversarial Tactics, Techniques, and Common Knowledge
  - Threat modeling methodology and suite of models for the various phases of an adversary's lifecycle

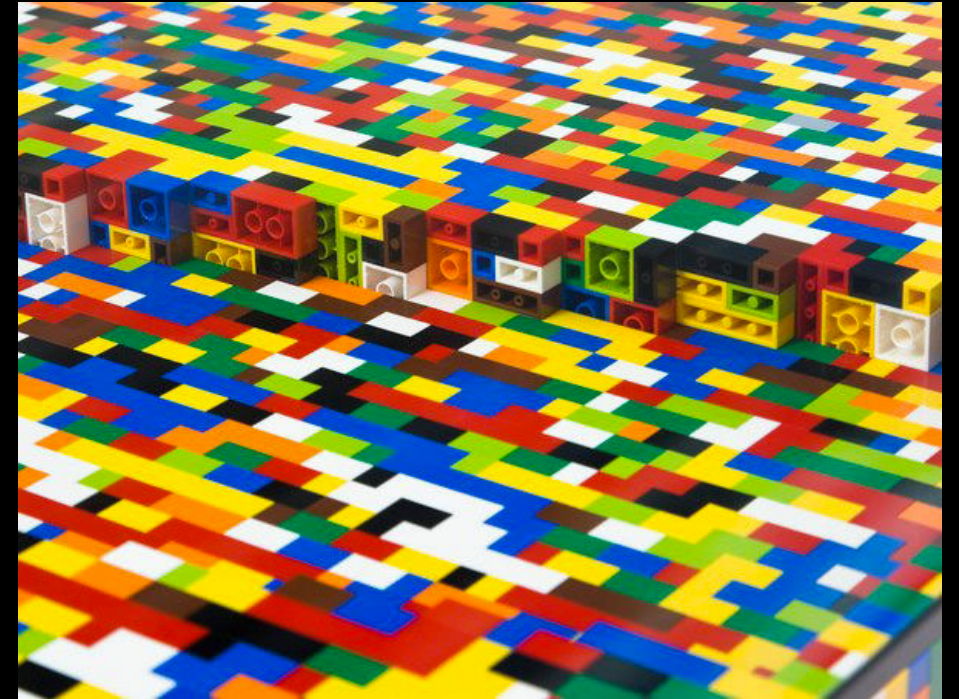
```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FL-SW-01" "Opera/9.80.2013.10; rv:1.9.2.10; Windows NT 6.0; SV1; .NET CLR 3.5.30729; .NET CLR 3.0.30729; .NET CLR 2.0.50727; .NET CLR 1.1.4322"
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-20&product_id=K9-CU-01" "Mozilla/5.0 (Windows NT 6.0; rv:1.9.2.10; Opera/9.80.2013.10; rv:1.9.2.10; 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)"
317.27.160.0 - - [07/Jan 18:10:56:150] "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&product_id=K9-CU-01" "Mozilla/5.0 (Windows NT 6.0; rv:1.9.2.10; Opera/9.80.2013.10; rv:1.9.2.10; 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)"
10.2.1.10 - - [07/Jan 18:10:55:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5SL8FF1ADFF5 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1&product_id=K9-CU-01" "Mozilla/5.0 (Windows NT 6.0; rv:1.9.2.10; Opera/9.80.2013.10; rv:1.9.2.10; 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)"
```

# Analytic Story Anatomy

A story by any other name...

# Building Blocks

- ▶ Manifest File
  - JSON Specification
- ▶ A story can consist of multiple searches
- ▶ A search can belong to multiple stories



```

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.
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/category.screen?category_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10" "Opera/9.80.
ows NT 5.1; SV1: ; .NET CLR 1.1.4322" 468 125.17.14.1 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1&product_id=AV-CB-01&JSESSIONID=SD1SLAFF10ADFF3 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-20&product_id=K9-CU-01" "Opera/9.80.
/buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD1SLAFF10ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS&JSESSIONID=SD1SLAFF10ADFF3" "Opera/9.80.
opping.com/purchase&itemId=EST-16&product_id=RP-LI-02" "Opera/9.80.
/buttercup-shopping.com/cart.do?action=remove&itemId=EST-1&product_id=AV-CB-01&JSESSIONID=SD1SLAFF10ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS&JSESSIONID=SD1SLAFF10ADFF3" "Opera/9.80.
/buttercup-shopping.com/cart.do?action=remove&itemId=EST-1&product_id=AV-CB-01&JSESSIONID=SD1SLAFF10ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS&JSESSIONID=SD1SLAFF10ADFF3" "Opera/9.80.

```

# Schemas

- ▶ Different schemas for searches and stories
  - Facilitate the many to many mappings
  
- ▶ Next few slides will focus on some of the fields we found useful to track
  - Why we found them useful
  - What are the benefits to tracking them

```

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.
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-20&product_id=Maxil1474" "Opera/9.80.
ows NT 5.1; SV1: - - [07/Jan 18:10:56:150] "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
/buttercup-shopping.com/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
/buttercup-shopping.com/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
/buttercup-shopping.com/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

```



# BRACE YOURSELF

# WALLS OF TEXT ARE COMING

makeameme.org

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen  
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.  
ows NY 5.1: SV1: - [07/Jan 18:10:56:156] "GET /oldlin  
itemId=EST-16&product\_id=RP-LI-02" 468 125.17 14.1  
://buttercup-shopping\_id=RP-LI-02" "O  
action=purchase&is.com/oldlin











# Search Manifest – How Does This Fit

- ▶ Mappings
- ▶ Currently we map to three frameworks
  - Kill Chain
  - Center for Internet Security Critical Security Controls
  - MITRE ATT&CK

```
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 (Windows NT 6.0; WOW64; rv:24.0) like Gecko"
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-20&product_id=K9-CU-01" "Mozilla/5.0 (Windows NT 6.0; WOW64; rv:24.0) like Gecko"
317.27.160.0 - - [07/Jan 18:10:56:150] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD10SL9FF2ADFF3 HTTP/1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1&JSESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 200 3865 "Mozilla/5.0 (Windows NT 6.0; WOW64; rv:24.0) like Gecko"
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 (Windows NT 6.0; WOW64; rv:24.0) like Gecko"
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-20&product_id=K9-CU-01" "Mozilla/5.0 (Windows NT 6.0; WOW64; rv:24.0) like Gecko"
317.27.160.0 - - [07/Jan 18:10:56:150] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD10SL9FF2ADFF3 HTTP/1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1&JSESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 200 3865 "Mozilla/5.0 (Windows NT 6.0; WOW64; rv:24.0) like Gecko"
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 (Windows NT 6.0; WOW64; rv:24.0) like Gecko"
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-20&product_id=K9-CU-01" "Mozilla/5.0 (Windows NT 6.0; WOW64; rv:24.0) like Gecko"
317.27.160.0 - - [07/Jan 18:10:56:150] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD10SL9FF2ADFF3 HTTP/1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1&JSESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 200 3865 "Mozilla/5.0 (Windows NT 6.0; WOW64; rv:24.0) like Gecko"
```

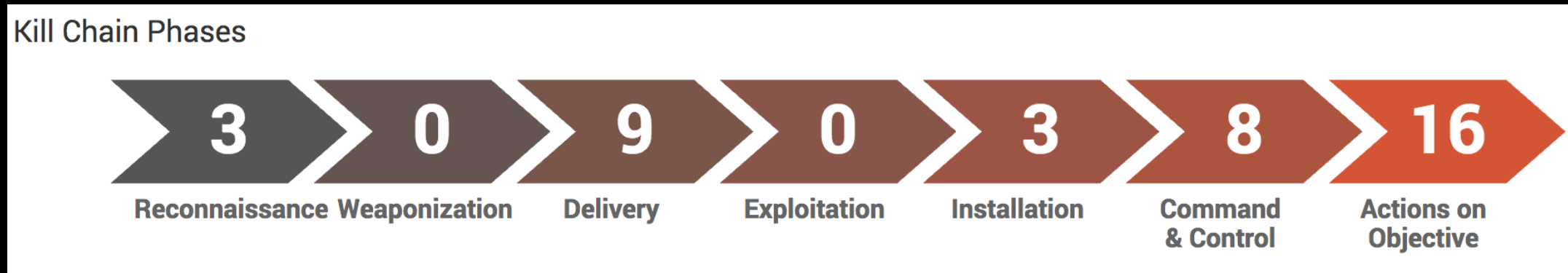
# Why Do We Map?

- ▶ Multiple Frameworks
  - Each framework has its pros and cons
- ▶ Where the search, and ultimately the analytic story, fits into your defensive strategy
- ▶ Allows you to understand what part of your defense is strong
- ▶ Allows you to identify weaknesses in your defense
- ▶ Allows you to navigate a content library to find what you are interested in

```

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"
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-20&product_id=Moz11474-0"
ows NT 27.160.0.0 - - [07/Jan 18:10:56:150] "GET /product.screen?product_id=AV-CB-01&JSESSIONID=SD10SLAF12ADF13 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01"
/buttercup-shopping.com/product_id=RP-LI-02" 468 125.17.14.11 "http://buttercup-shopping.com/product_id=RP-LI-02" 468 125.17.14.11 "http://buttercup-shopping.com/product_id=RP-LI-02"
/buttercup-shopping.com/product_id=RP-LI-02" 468 125.17.14.11 "http://buttercup-shopping.com/product_id=RP-LI-02" 468 125.17.14.11 "http://buttercup-shopping.com/product_id=RP-LI-02"
/buttercup-shopping.com/product_id=RP-LI-02" 468 125.17.14.11 "http://buttercup-shopping.com/product_id=RP-LI-02" 468 125.17.14.11 "http://buttercup-shopping.com/product_id=RP-LI-02"
/buttercup-shopping.com/product_id=RP-LI-02" 468 125.17.14.11 "http://buttercup-shopping.com/product_id=RP-LI-02" 468 125.17.14.11 "http://buttercup-shopping.com/product_id=RP-LI-02"
/buttercup-shopping.com/product_id=RP-LI-02" 468 125.17.14.11 "http://buttercup-shopping.com/product_id=RP-LI-02" 468 125.17.14.11 "http://buttercup-shopping.com/product_id=RP-LI-02"
  
```

# Mapping Example



- ▶ Installation and Recon are relatively low in comparison
- ▶ Strongest in Actions on Objective

```
130.60.4 - - [07/Jan 18:10:57:123] "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/9.80.2013.0 (Windows NT 6.0; WOW64; rv:31.0) like Gecko"
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://shopping.com/cart.do?action=purchase&itemId=EST-20&product_id=Moz11A74-0" "Mozilla/5.0 (Windows NT 6.0; WOW64; rv:31.0) like Gecko"
317.27.160.0 - - [07/Jan 18:10:56:150] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD95L4FFAADF7 HTTP/1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1" "Opera/9.80.2013.0 (Windows NT 6.0; WOW64; rv:31.0) like Gecko"
10.0.2.10 - - [07/Jan 18:10:56:150] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 468 125.17.14 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1" "Opera/9.80.2013.0 (Windows NT 6.0; WOW64; rv:31.0) like Gecko"
10.0.2.10 - - [07/Jan 18:10:55:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5SL7FF6ADFF9 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1" "Opera/9.80.2013.0 (Windows NT 6.0; WOW64; rv:31.0) like Gecko"
10.0.2.10 - - [07/Jan 18:10:55:198] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5SL7FF6ADFF9 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1" "Opera/9.80.2013.0 (Windows NT 6.0; WOW64; rv:31.0) like Gecko"
```



# Story Manifest!

- ▶ author
- ▶ requestor
- ▶ id
- ▶ version
- ▶ modification\_time
- ▶ creation\_time

```

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.
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-2&product_id=K9-CU-01" "Compa
ows NT 5.1; SV1; .NET CLR 1.1.4322" "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=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&product_id=K9-CU-01" "Opera/9.80.
130.60.4 - - [07/Jan 18:10:56:150] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 189 "GET /cart.do?action=changequantity&itemId=EST-6&product_id=FL-SW-01" "Opera/9.80.
130.60.4 - - [07/Jan 18:10:56:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1&product_id=K9-CU-01" "Opera/9.80.
130.60.4 - - [07/Jan 18:10:56:189] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1&product_id=K9-CU-01" "Opera/9.80.
130.60.4 - - [07/Jan 18:10:56:189] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1&product_id=K9-CU-01" "Opera/9.80.

```





# Story Manifest – The Searches

- ▶ detection\_searches
- ▶ investigative\_searches
- ▶ contextual\_searches
- ▶ support\_searches

```
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 (Windows NT 6.0; WOW64; rv:31.0) like Gecko"
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 (Windows NT 6.0; WOW64; rv:31.0) like Gecko"
317.27.160.0 - - [07/Jan 18:10:56:150] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD10SL9FF1ADFF9 HTTP 1.1" "Opera/9.80.2013.10 (Windows NT 6.0; WOW64; rv:31.0) like Gecko"
130.60.4 - - [07/Jan 18:10:56:150] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" "Opera/9.80.2013.10 (Windows NT 6.0; WOW64; rv:31.0) like Gecko"
130.60.4 - - [07/Jan 18:10:56:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" "Opera/9.80.2013.10 (Windows NT 6.0; WOW64; rv:31.0) like Gecko"
130.60.4 - - [07/Jan 18:10:56:189] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" "Opera/9.80.2013.10 (Windows NT 6.0; WOW64; rv:31.0) like Gecko"
```

# Building An Analytic Story

---

# Developing Stories

- ▶ Can be time consuming, so why do it?
- ▶ Empower analysts to explore events
  - Many contextual and investigative searches are shared across stories
  - Quicker response times
- ▶ Demonstrate value of the data you are ingesting
- ▶ Allows you to prioritize what data you want to ingest
- ▶ Map your defensive posture
- ▶ Allows you to prioritize what new analytics to write

```
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/9.80.2013.10; Linux x86_64; rv:15.0 Gecko/20100101 Firefox/15.0"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5L7FF6ADFF9 HTTP/1.1" 404 3322 "http://shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CU-01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_2; rv:42.0) Gecko/20100801 Firefox/42.0"
317.27.160.0 - - [07/Jan 18:10:56:150] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5L9FF1ADFF3 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&surprise=1" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_2; rv:42.0) Gecko/20100801 Firefox/42.0"
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/9.80.2013.10; Linux x86_64; rv:15.0 Gecko/20100101 Firefox/15.0"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5L7FF6ADFF9 HTTP/1.1" 404 3322 "http://shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CU-01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_2; rv:42.0) Gecko/20100801 Firefox/42.0"
317.27.160.0 - - [07/Jan 18:10:56:150] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5L9FF1ADFF3 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&surprise=1" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_2; rv:42.0) Gecko/20100801 Firefox/42.0"
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/9.80.2013.10; Linux x86_64; rv:15.0 Gecko/20100101 Firefox/15.0"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5L7FF6ADFF9 HTTP/1.1" 404 3322 "http://shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CU-01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_2; rv:42.0) Gecko/20100801 Firefox/42.0"
317.27.160.0 - - [07/Jan 18:10:56:150] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5L9FF1ADFF3 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&surprise=1" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_2; rv:42.0) Gecko/20100801 Firefox/42.0"
```

# How We Develop Stories

## ▶ Analytic stories allows for flexibility in topic

- Threat actors
- Malware families
- Malware techniques
- Malware of the day

## ▶ Standard Process

- Knowledge Acquisition
- Codification
- Testing
- Deploy

```

130.60.4 - - [07/Jun 18:10:56:123] "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.
128.241.220.82 - - [07/Jun 18:10:57:153] "GET /category/screen?category_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=AV-CB-01" "Opera/9.80.
317.27.160.0.0 - - [07/Jun 18:10:57:123] "GET /product/screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 200 1316 "http://shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD10SL9FF1ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-31&product_id=AV-CB-01" "Opera/9.80.
ows NT 5.1; SV1: ; NET CLR 1.1.4322" 468 125.17.14.111:189] "GET /category/screen?category_id=FLOWERS&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 200 3865 "http://shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01" "Opera/9.80.
/buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=AV-CB-01" 468 125.17.14.111:189] "GET /category/screen?category_id=FLOWERS&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 200 3865 "http://shopping.com/cart.do?action=remove&itemId=EST-31&product_id=AV-CB-01" "Opera/9.80.
/buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=AV-CB-01" 468 125.17.14.111:189] "GET /category/screen?category_id=FLOWERS&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 200 3865 "http://shopping.com/cart.do?action=remove&itemId=EST-31&product_id=AV-CB-01" "Opera/9.80.

```

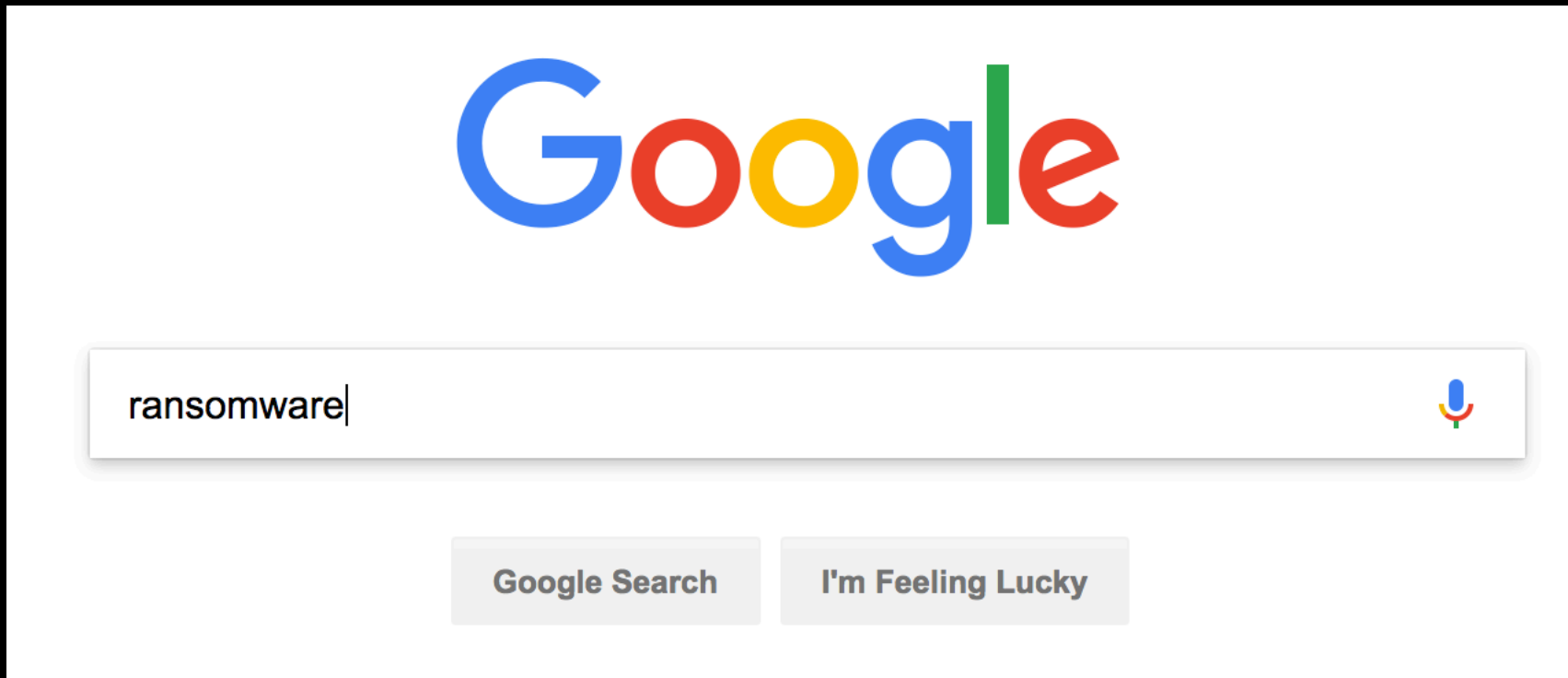
# Ransomware



```
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/9.80.2013.0 (Windows NT 6.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/31.0.1650.63 Safari/537.36"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD10SL9FF1ADFF3 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1"
317.27.160.0 - - [07/Jan 18:10:56:150] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 468 125.17.14.11 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1"
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/9.80.2013.0 (Windows NT 6.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/31.0.1650.63 Safari/537.36"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD10SL9FF1ADFF3 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1"
317.27.160.0 - - [07/Jan 18:10:56:150] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 468 125.17.14.11 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1"
```

# Knowledge Acquisition

- ▶ The sites you go to and learn from become the references



# Codification

- ▶ Start with the basics of the story manifest
- ▶ Some fields are easy to fill out
  - id
  - creation\_time
  - modification\_time
  - version
  - author
  - requester
  - name
  - references

```

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15L9FF1ADFF10 HTTP/1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FL-SW-01" "Opera/9.80.
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=Mx11LW74" "
ows NT 5.1; SV1; .NET CLR 1.1.4322" 468 125 17 14 1189 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD10SL9FF2ADFF9 HTTP/1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=
do?action=purchase&product_id=RP-LI-02" 468 125 17 14 1189 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-3&product_id=FLOWERS&JSESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-6&JSESSIONID=SD10SL9FF2ADFF9 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=
189] "GET /category.screen?category_id=SURPRISE&JSESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-6&JSESSIONID=SD10SL9FF2ADFF9 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=

```



# Codification

- ▶ Some require some thought
  - category
  - description
  - narrative



```
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.  
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-20&product_id=K9-CU-01" "Mozilla/5.0  
ows NT 5.1; SV1; .NET CLR 1.1.4322" 468 125.17.14 [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD10SL9FF1ADFF3 HTTP/1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-11&product_id=LI-02" "Opera/9.80.  
http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-11&product_id=LI-02" "Opera/9.80.  
http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-11&product_id=LI-02" "Opera/9.80.  
http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-11&product_id=LI-02" "Opera/9.80.  
http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-11&product_id=LI-02" "Opera/9.80.  
http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-11&product_id=LI-02" "Opera/9.80.  
http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-11&product_id=LI-02" "Opera/9.80.  
http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-11&product_id=LI-02" "Opera/9.80.
```

# Detection Searches

- ▶ No idea is too horrible at this point
- ▶ Don't have to worry about the details... yet
  - USN Journal Deletion
  - Deleting Shadow Copies
  - Spike in File Writes
  - Common Ransomware Extensions
  - Common Ransomware Notes
  - Detect SMB Traffic Allowed
  - Detect Spike in SMB Traffic
  - Monitor TOR traffic

```

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"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CU-01"
ows NT 27.160.0.0 - - [07/Jan 18:10:56:150] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD5L9FF1ADFF3"
itemId=EST-16&product_id=RP-LI-02" 468 125.17.14.10 [07/Jan 18:10:55:189] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-10&product_id=K9-CU-01"
opping.com/purchase&itemId=EST-16&product_id=RP-LI-02"
http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-10&product_id=K9-CU-01"

```

# Support Searches

- ▶ Still, no idea is too horrible at this point
- ▶ Searches to give you a better understanding of your environment
  - Monitor Successful Backups
  - Monitor Unsuccessful Backups
  - Windows Updates Install Failures
  - Windows Updates Install Successes
  - Common Vulnerabilities Used By Ransomware

```

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"
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-2&product_id=K9-CU-01"
ows NT 27.160.0.0 - - [07/Jan 18:10:56:150] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD10SL9FF2ADFF3"
itemId=EST-16&product_id=RP-LI-02" 468 125.17.14[idlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5SL7FF6ADFF9 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1"
opping.com/purchase&itemId=EST-26&JSESSIONID=SD5SL9FF1ADFF3" 468 125.17.14[idlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5SL7FF6ADFF9 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1"
http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1"

```

# Contextual Searches

- ▶ Once again, no idea is too horrible at this point
- ▶ What would you want to know to help scope this event
  - Backup Status of Endpoint
  - Patch Status of Endpoint
  - Vulnerability Status of Endpoint
  - Get Authentication Logs For Endpoint
  - Get Notable History
  - Get User Information from Identity Table

```
130.60.4 - - [07/Jan 18:10:57:123] "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; Linux x86_64; rv:15.0 Gecko/20100101 Firefox/15.0"
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-20&product_id=Mozillaz74" "Opera/9.80.2013.10; Linux x86_64; rv:15.0 Gecko/20100101 Firefox/15.0"
317.27.160.0 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP/1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD10SL9FF2ADFF3 HTTP/1.1" "Opera/9.80.2013.10; Linux x86_64; rv:15.0 Gecko/20100101 Firefox/15.0"
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; Linux x86_64; rv:15.0 Gecko/20100101 Firefox/15.0"
128.241.220.82 - - [07/Jan 18:10:57:153] "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-20&product_id=Mozillaz74" "Opera/9.80.2013.10; Linux x86_64; rv:15.0 Gecko/20100101 Firefox/15.0"
317.27.160.0 - - [07/Jan 18:10:57:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD10SL9FF2ADFF3 HTTP/1.1" "Opera/9.80.2013.10; Linux x86_64; rv:15.0 Gecko/20100101 Firefox/15.0"
130.60.4 - - [07/Jan 18:10:57:156] "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; Linux x86_64; rv:15.0 Gecko/20100101 Firefox/15.0"
128.241.220.82 - - [07/Jan 18:10:57:156] "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-20&product_id=Mozillaz74" "Opera/9.80.2013.10; Linux x86_64; rv:15.0 Gecko/20100101 Firefox/15.0"
317.27.160.0 - - [07/Jan 18:10:57:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD10SL9FF2ADFF3 HTTP/1.1" "Opera/9.80.2013.10; Linux x86_64; rv:15.0 Gecko/20100101 Firefox/15.0"
130.60.4 - - [07/Jan 18:10:57:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5SL8FF1ADFF3 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1" "Opera/9.80.2013.10; Linux x86_64; rv:15.0 Gecko/20100101 Firefox/15.0"
128.241.220.82 - - [07/Jan 18:10:57:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5SL8FF1ADFF3 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1" "Opera/9.80.2013.10; Linux x86_64; rv:15.0 Gecko/20100101 Firefox/15.0"
317.27.160.0 - - [07/Jan 18:10:57:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5SL8FF1ADFF3 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1" "Opera/9.80.2013.10; Linux x86_64; rv:15.0 Gecko/20100101 Firefox/15.0"
```

# Investigative Searches

- ▶ Things get tricky here
- ▶ Don't have to worry about the details... yet
  - Get Process Info
  - Get Process Information For Port Activity
  - Investigate Web Activity
  - Get Parent Process Info

```
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 (Windows NT 6.0; WOW64; rv:31.0) like Gecko"
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 (Windows NT 6.0; WOW64; rv:31.0) like Gecko"
317.27.160.0 - - [07/Jan 18:10:56:156] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP/1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD10SL9FF2ADFF9 HTTP/1.1" "Opera/9.80.2013.10 (Windows NT 6.0; WOW64; rv:31.0) like Gecko"
10.2.1.10 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 200 189 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1&product_id=FLOWERS&JSESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" "Opera/9.80.2013.10 (Windows NT 6.0; WOW64; rv:31.0) like Gecko"
10.2.1.10 - - [07/Jan 18:10:56:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1&product_id=FLOWERS&JSESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" "Opera/9.80.2013.10 (Windows NT 6.0; WOW64; rv:31.0) like Gecko"
```



# Deleting Shadow Copies

- ▶ Let's write the search
- ▶ `index=* (sourcetype=XmlWinEventLog:Microsoft-Windows-Sysmon/Operational OR tag=process) (process=*vssadmin* OR process=*wmic*) cmdline=*delete* cmdline=*shadow* | stats count min(_time) as firstTime max(_time) as lastTime by dest, user, process, cmdline | `ctime(firstTime)` | `ctime(lastTime)``

```

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15L9FF1ADFF3 HTTP/1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FL-SW-01"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D55L7FF6ADFF9 HTTP/1.1" 404 3322 "http://buttercup-shopping.com/category.screen?category_id=GIFTS"
ows NT 27.160.0.0 - - [07/Jan 18:10:56:150] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP/1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D10SL9FF2ADFF9"
itemId=EST-16&product_id=RP-LI-02" 468 125.17.14.118 [07/Jan 18:10:56:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L7FF6ADFF9 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS&JSESSIONID=5D55L7FF6ADFF9"
opping.com/purchase&id=RP-LI-02" 468 125.17.14.118 [07/Jan 18:10:56:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L7FF6ADFF9 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D10SL9FF2ADFF9"
/buttercup-shopping.com/purchase&id=RP-LI-02" 468 125.17.14.118 [07/Jan 18:10:56:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L7FF6ADFF9 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D10SL9FF2ADFF9"

```

# It's All About The Data

- ▶ What type of data do we need (data\_source field)
  - Endpoint Intelligence
- ▶ Where can we get this data (providing technologies)
  - Carbon Black Response
  - CrowdStrike Falcon
  - Sysmon
- ▶ Fill out data\_sourcetypes or data\_models as appropriate

```

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.
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5L7FF6ADFF9 HTTP/1.1" 404 3322 "http://buttercup-shopping.com/category.screen?category_id=GIFTS" "Mozilla/5.0 (Windows NT 6.0; rv:2.0) Gecko/20100101 Firefox/4.0.1"
317.27.160.0.0 - - [07/Jan 18:10:56:150] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD10SL9FF2ADFF9 HTTP/1.1" 200 2423 "http://buttercup-shopping.com/product.screen?product_id=FL-DSH-01&JSESSIONID=SD5L7FF6ADFF9"
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.
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5L7FF6ADFF9 HTTP/1.1" 404 3322 "http://buttercup-shopping.com/category.screen?category_id=GIFTS" "Mozilla/5.0 (Windows NT 6.0; rv:2.0) Gecko/20100101 Firefox/4.0.1"
317.27.160.0.0 - - [07/Jan 18:10:56:150] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD10SL9FF2ADFF9 HTTP/1.1" 200 2423 "http://buttercup-shopping.com/product.screen?product_id=FL-DSH-01&JSESSIONID=SD5L7FF6ADFF9"
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.
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5L7FF6ADFF9 HTTP/1.1" 404 3322 "http://buttercup-shopping.com/category.screen?category_id=GIFTS" "Mozilla/5.0 (Windows NT 6.0; rv:2.0) Gecko/20100101 Firefox/4.0.1"
317.27.160.0.0 - - [07/Jan 18:10:56:150] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD10SL9FF2ADFF9 HTTP/1.1" 200 2423 "http://buttercup-shopping.com/product.screen?product_id=FL-DSH-01&JSESSIONID=SD5L7FF6ADFF9"

```



# The Details

## ► Search Description

- The vssadmin.exe utility is used to interact with the Volume Shadow Copy Service. Wmic is an interface to the Windows Management Instrumentation. This search looks for either of these tools being used to delete shadow copies

## ► How to Implement

- To successfully implement this search, you need to be ingesting logs with both the process name and command line from your endpoints. If you are using Sysmon, you must have at least version 6.0.4 of the Sysmon TA.

## ► ELI5

- This search looks for execution of vssadmin or wmic with both the "delete" and "shadow" parameters passed on the command line. The two arguments are searched for separately because we can't predict the number of spaces between the words on the command line. The search will return the number of times this activity was observed, and the times of the first and last event."



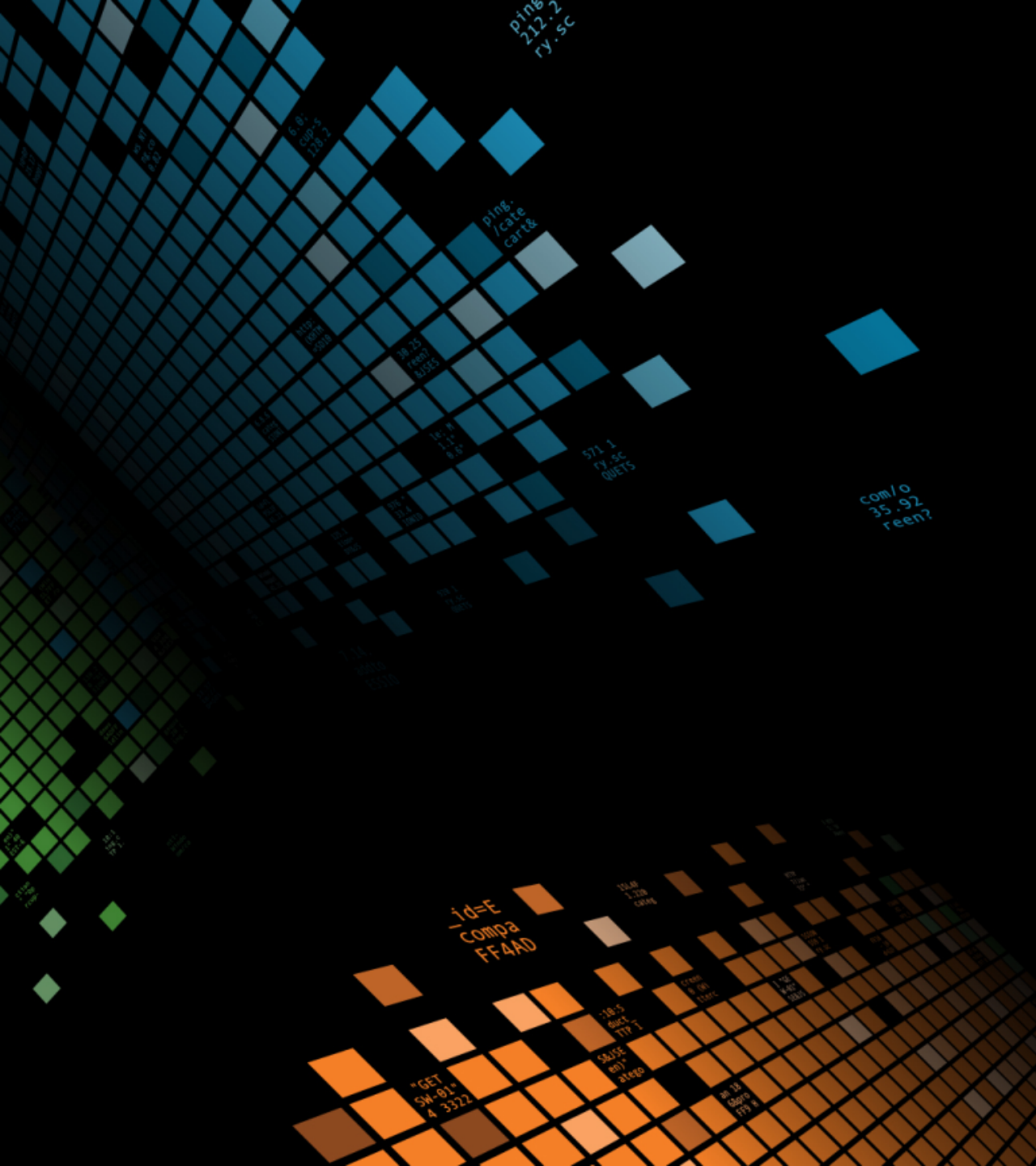
# Why Did I Just Do All That

- ▶ Allows you to prioritize what data you want to ingest
- ▶ Demonstrate value of the data you are ingesting
- ▶ Empower analysts to explore events
- ▶ The beginnings of orchestration
- ▶ Map your defensive posture
- ▶ Allows you to prioritize what new analytics to write



# Analytic Story In Action

---







# Analytic Stories At Splunk

Category: Malware

Version: 1

Created: 07/24/2017

Modified: 09/20/2017

## Ransomware

Run Story

### Description:

Activities, techniques, and best practices associated with detecting, investigating, and mitigating your risk to ransomware

### Narrative:

Ransomware is an ever present risk to many enterprises where by an infected hosts encrypts business critical data until the victim pays the attacker a ransom. There are many types and varieties of Ransomware of which can affect an enterprise. Attackers can deploy Ransomware to enterprises through spear phishing campaigns, drive by downloads as well as through traditional remote service based exploitation. In the case of the WannaCry campaign there was self propagating wormable functionality that was used to maximize infection. To effectively combat Ransomware organizations can apply several techniques to detect and or mitigate the effects of Ransomware.

### Att&ck:

Command and Control

Windows Management Instrumentation

Masquerading Commonly Used Port

Indicator Removal on Host

Exfiltration Over Alternative Protocol Exfiltration

Registry Run Keys / Start Folder Defense Evasion

Execution Persistence

### Kill Chain Phases:

Command and Control Actions on Objective

Delivery

### CIS 20:

CIS 10

CIS 8

CIS 9

CIS 6

CIS 12

CIS 5

CIS 3

### Data Model:

Application\_State

Change\_Analysis

Network\_Traffic

Updates

Vulnerabilities

### Technologies:

Bro

Carbon Black

CrowdStrike Falcon

Linux

Microsoft Windows

Netbackup

OS X

Palo Alto

Splunk Enterprise Security

Splunk Stream

Sysmon

Analytic Story Searches

# Analytic Stories At Splunk

▼ ESCU - Deleting Shadow Copies

## Configure in ES

### Description

The vssadmin.exe utility is used to interact with the Volume Shadow Copy Service. Wmic is an interface to the Windows Management Instrumentation. This search looks for either of these tools being used to delete shadow copies.

### ELI5

This search looks for execution of vssadmin or wmic with both the "delete" and "shadows" parameters passed on the command line. The two arguments are searched for separately because we can't predict the number of spaces between the words on the command line. The search will return the number of times this activity was observed, and the times of the first and last event.

### Search

```
index=* (sourcetype=XmlWinEventLog:Microsoft-Windows-Sysmon
/Operational OR tag=process) (process=*vssadmin* OR process
=*wmic*) cmdline=*delete* cmdline=*shadow* | stats count min
(_time) as firstTime max(_time) as lastTime by dest, user,
process, cmdline | `ctime(firstTime)` | `ctime(lastTime)`
```

### Data Models

### Technology

Carbon Black

CrowdStrike Falcon Sysmon

Tanium Ziften

### Att&ck

Execution

### Kill Chain Phases

Actions on Objective

### CIS 20

CIS 8 CIS 10

### Asset at Risk

Endpoint

### Confidence

medium



# Analytic Stories At Splunk

## ▼ Context

- ▶ ESCU - Get Authentication Logs For Endpoint
- ▶ ESCU - Get Backup Logs For Endpoint
- ▶ ESCU - Get Notable History
- ▶ ESCU - Get Update Logs For Endpoint
- ▶ ESCU - Get User Information from Identity Table
- ▼ ESCU - Get Vulnerability Logs For Endpoint

# Analytic Stories At Splunk

## Adaptive Responses:

Response	Mode	Time	User	Status
ESCU- Contextualize	adhoc	2017-09-22T01:54:49- 0500	system	✓ success
Notable	saved	2017-09-21T15:55:31- 0500	admin	✓ success
Risk Analysis	saved	2017-09-21T15:55:31- 0500	admin	✓ success

[View Adaptive Response Investigations](#)

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category\_id=GIFTS&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product\_id=FL-SW-01" "Opera/9.80.2013.10404; rv:1.9.1.10404; like:Gecko/1.9.1.10404; like:Firefox/10.0.10.10404" "10.0.10.10404"

128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product\_id=FL-DSH-01&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product\_id=AV-CB-01&JSESSIONID=SD5L9FF1ADFF3" "Opera/9.80.2013.10404; rv:1.9.1.10404; like:Gecko/1.9.1.10404; like:Firefox/10.0.10.10404" "10.0.10.10404"

317.27.160.0 - - [07/Jan 18:10:56:150] "GET /oldlink?item\_id=EST-26&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1" "Opera/9.80.2013.10404; rv:1.9.1.10404; like:Gecko/1.9.1.10404; like:Firefox/10.0.10.10404" "10.0.10.10404"

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category\_id=GIFTS&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product\_id=FL-SW-01" "Opera/9.80.2013.10404; rv:1.9.1.10404; like:Gecko/1.9.1.10404; like:Firefox/10.0.10.10404" "10.0.10.10404"

128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product\_id=FL-DSH-01&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product\_id=AV-CB-01&JSESSIONID=SD5L9FF1ADFF3" "Opera/9.80.2013.10404; rv:1.9.1.10404; like:Gecko/1.9.1.10404; like:Firefox/10.0.10.10404" "10.0.10.10404"

317.27.160.0 - - [07/Jan 18:10:56:150] "GET /oldlink?item\_id=EST-26&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1" "Opera/9.80.2013.10404; rv:1.9.1.10404; like:Gecko/1.9.1.10404; like:Firefox/10.0.10.10404" "10.0.10.10404"

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category\_id=GIFTS&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product\_id=FL-SW-01" "Opera/9.80.2013.10404; rv:1.9.1.10404; like:Gecko/1.9.1.10404; like:Firefox/10.0.10.10404" "10.0.10.10404"

128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product\_id=FL-DSH-01&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product\_id=AV-CB-01&JSESSIONID=SD5L9FF1ADFF3" "Opera/9.80.2013.10404; rv:1.9.1.10404; like:Gecko/1.9.1.10404; like:Firefox/10.0.10.10404" "10.0.10.10404"

317.27.160.0 - - [07/Jan 18:10:56:150] "GET /oldlink?item\_id=EST-26&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1" "Opera/9.80.2013.10404; rv:1.9.1.10404; like:Gecko/1.9.1.10404; like:Firefox/10.0.10.10404" "10.0.10.10404"

# Analytic Stories At Splunk

## ESCU Context

### ESCU - Get Notable History

index=main sourcetype=escu-contextualize orig\_sid=scheduler\_\_admin\_REEtRVNtLUNvbnRlbnRvcGRhdGU\_\_RMD5f681a143dfa7cc07\_at\_1506027300\_1020 orig\_rid=0 search\_name="ESCU - Get Notable History" | table \_raw | spath input=\_raw | fields - \_raw raw

All time ▾



owner ▾	priority ▾	rule_name ▾	search_name ▾	severity ▾	status_description ▾	time ▾
unassigned	unknown	Common Ransomware Notes	ESCU - Get Notable History	high	Event has not been reviewed	2017-09-21T11:15:59.000-05:00
unassigned	unknown	Common Ransomware Notes	ESCU - Get Notable History	high	Event has not been reviewed	2017-09-21T11:16:02.000-05:00
unassigned	unknown	Registry Keys Used For Persistence	ESCU - Get Notable History	medium	Event has not been reviewed	2017-09-21T11:21:04.000-05:00
unassigned	unknown	Registry Keys Used For Persistence	ESCU - Get Notable History	medium	Event has not been reviewed	2017-09-21T11:21:04.000-05:00
unassigned	unknown	Registry Keys Used For Persistence	ESCU - Get Notable History	medium	Event has not been reviewed	2017-09-21T11:21:07.000-05:00
unassigned	unknown	Deleting Shadow Copies	ESCU - Get Notable History	medium	Event has not been reviewed	2017-09-21T11:21:24.000-05:00
unassigned	unknown	Common Ransomware Notes	ESCU - Get Notable History	high	Event has not been reviewed	2017-09-21T11:21:57.000-05:00
unassigned	unknown	Common Ransomware Notes	ESCU - Get Notable History	high	Event has not been reviewed	2017-09-21T11:21:57.000-05:00
unassigned	unknown	Common Ransomware Notes	ESCU - Get Notable History	high	Event has not been reviewed	2017-09-21T11:22:02.000-05:00
unassigned	unknown	Registry Keys Used For Persistence	ESCU - Get Notable History	medium	Event has not been reviewed	2017-09-21T11:25:24.000-05:00

« prev 1 2 3 4 5 6 7 8 9 10 next »

### ESCU - Get Backup Logs For Endpoint

index=main sourcetype=escu-contextualize orig\_sid=scheduler\_\_admin\_REEtRVNtLUNvbnRlbnRvcGRhdGU\_\_RMD5f681a143dfa7cc07\_at\_1506027300\_1020 orig\_rid=0 search\_name="ESCU - Get Backup Logs For Endpoint" | table \_raw | spath input=\_raw | fields - \_raw raw

All time ▾



dest ▾	search_name ▾	signature ▾	time ▾
winterfell	ESCU - Get Backup Logs For Endpoint	An error occurred, failed to backup.	2017-09-17T23:53:30.434-05:00
winterfell	ESCU - Get Backup Logs For Endpoint	The task was created.	2017-09-17T23:53:29.434-05:00
winterfell	ESCU - Get Backup Logs For Endpoint	An error occurred, failed to backup.	2017-09-14T21:09:17.324-05:00
winterfell	ESCU - Get Backup Logs For Endpoint	The task was created.	2017-09-14T21:09:16.324-05:00

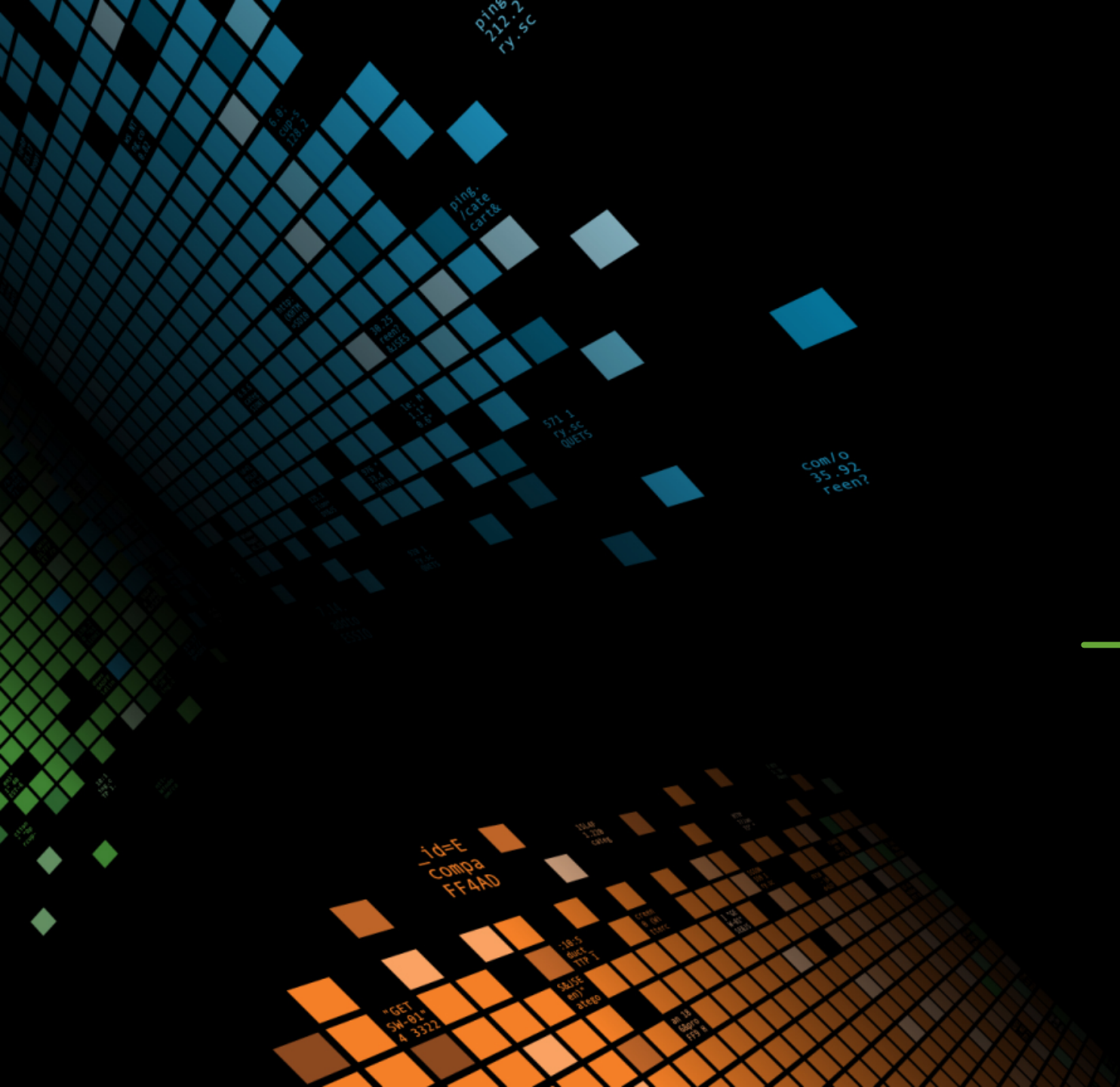
# Where Do We Go From Here

---



# Conclusions

---



# Takeaways

- ▶ It's about understanding, not detection
  - What data do you need
  - What behaviors are you looking for
  - What value are you getting from your data
  - What are the next steps you take to validate your discovery
- ▶ Allows you to map your defensive strategy
  - Know your strengths
  - Know your weaknesses
- ▶ Faster time to resolution
  - Save time (and \$\$\$)
  - Quicker time to value
  - Uplevel your analysts







# Thank You

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

splunk> .conf2017