



Keeping Track Of All The Things

A use-case and content management story

Matt Parks | Manager, Kaiser Permanente

Ruperto Razon | Sr. Threat Analyst, Kaiser Permanente

What Questions? These Questions

- What does our security coverage look like, from a use-case perspective?
- Bob in accounting was infected by **<insert-threat-of-the-day-here>**, who else was infected?
- How are we tracking towards our high level security goals for the year?
- What does your development team do all day?

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15LAFF10ADFF10 HTTP/1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-03" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_7; rv:53.0) Gecko/20100801 Firefox/53.0"

128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D355L7FF6ADFF0 HTTP/1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268product_id=KQ-CW-01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_7; rv:53.0) Gecko/20100801 Firefox/53.0"

ows NT 5.1; SV1; .NET CLR 1.1.4322)" "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15LAFF10ADFF10 HTTP/1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D355L7FF6ADFF0" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_7; rv:53.0) Gecko/20100801 Firefox/53.0"

item_id=EST-16&product_id=RP-LI-02" 468 125.17 14.1.189] "GET /cart.do?action=changequantity&itemId=EST-6&JSESSIONID=5D15LAFF10ADFF10 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-6&JSESSIONID=5D15LAFF10ADFF10" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_7; rv:53.0) Gecko/20100801 Firefox/53.0"

action=purchase&itemId=EST-26&JSESSIONID=5D355L7FF6ADFF0" 468 125.17 14.1.189] "GET /oldlink?item_id=EST-26&JSESSIONID=5D355L7FF6ADFF0 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D355L7FF6ADFF0" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_7; rv:53.0) Gecko/20100801 Firefox/53.0"

0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D355L7FF6ADFF0 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D355L7FF6ADFF0" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_7; rv:53.0) Gecko/20100801 Firefox/53.0"

action=purchase&itemId=EST-26&JSESSIONID=5D355L7FF6ADFF0" 468 125.17 14.1.189] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D355L7FF6ADFF0 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D355L7FF6ADFF0" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_7; rv:53.0) Gecko/20100801 Firefox/53.0"

0 - - [07/Jan 18:10:55:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D355L7FF6ADFF0 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D355L7FF6ADFF0" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_7; rv:53.0) Gecko/20100801 Firefox/53.0"

0 - - [07/Jan 18:10:55:189] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D355L7FF6ADFF0 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D355L7FF6ADFF0" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_7; rv:53.0) Gecko/20100801 Firefox/53.0"

Who are you guys?

Matt Parks

Manager, Security Analytics, Cyber Risk Defense Center



▶ Matthew.Parks@kp.org

▶ [linkedin.com/in/matthewparks](https://www.linkedin.com/in/matthewparks)

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=5D15L9FF1ADFF3 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-5W-03" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5D55L7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/category.screen?category_id=GIFTS" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=5D15L9FF1ADFF3 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-5W-03" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5D55L7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/category.screen?category_id=GIFTS" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=5D15L9FF1ADFF3 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-5W-03" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5D55L7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/category.screen?category_id=GIFTS" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14

Who are you guys?

Ruperto Razon

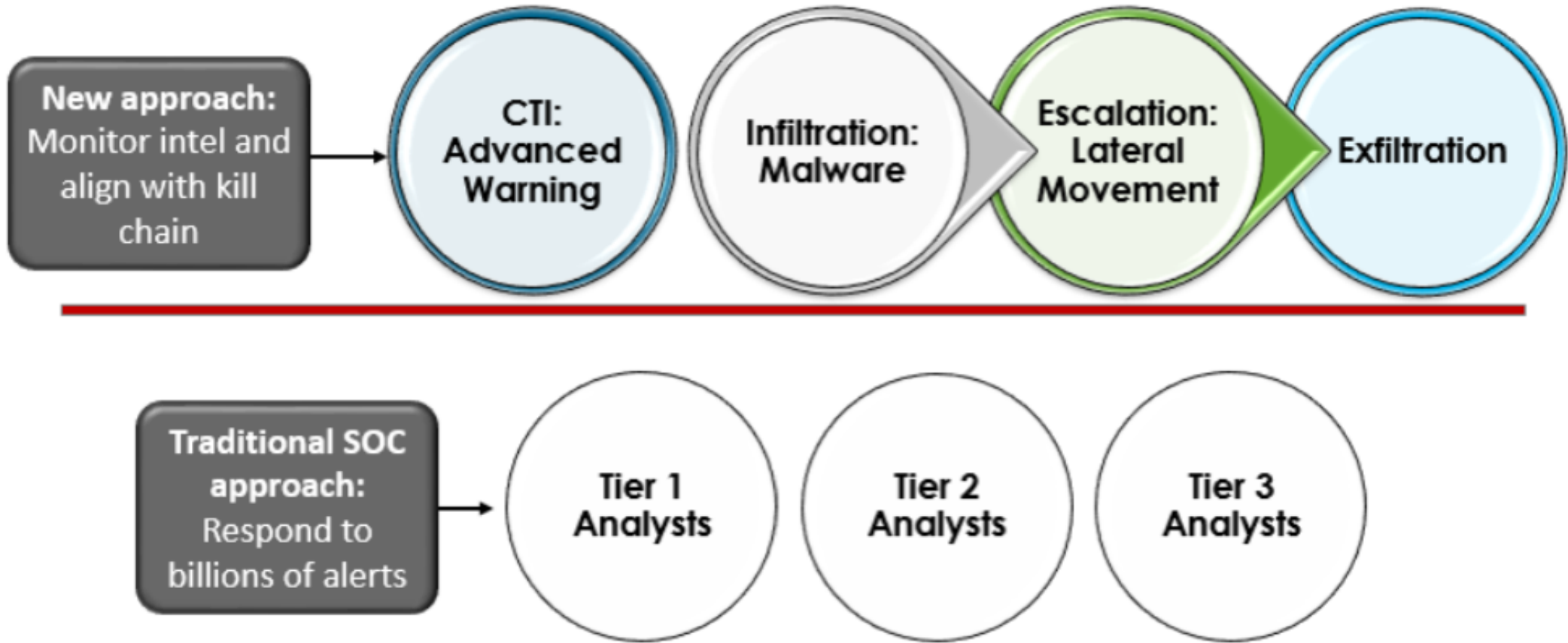
Sr. Threat Analyst, Security Analytics, Cyber Risk Defense Center



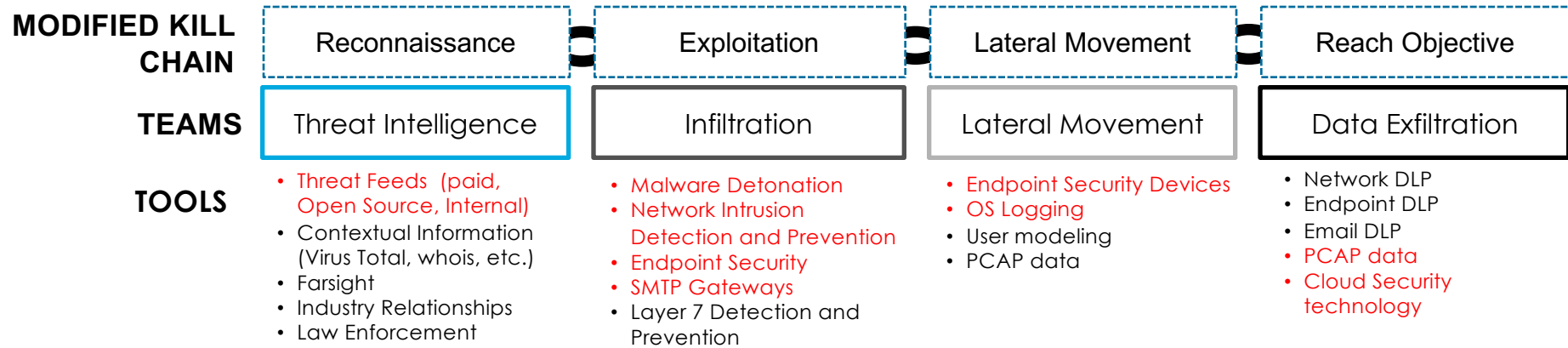
- ▶ Ruperto.S.Razon@kp.org
- ▶ [linkedin.com/in/PertoRazon](https://www.linkedin.com/in/PertoRazon)
- ▶ @thatperto

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D55L9FF1ADFF3 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=5D55L7FF6ADFF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268&product_id=KQ-CW-01"
1317 27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3"
1317 27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3"
1317 27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3"
1317 27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3"
1317 27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3"
1317 27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3"
1317 27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3"
1317 27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3"

Cyber Risk Defense Center (CRDC)



Advanced and Actionable Intelligence



**DATA
LAYER**

Splunk

Other Big Data Platforms

ACTIONABLE INTELLIGENCE

130.60.4... [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=5D15L9FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-01" MozIl1aZs0 "q9erf9; 20
128.241.220.82... [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=KO-CY-01" "Comp4iD1Cm
ows NT 5.1: SV1; .NET CLR 1.1.4322" "GET /oldlink?item_id=EST-26&SESSIONID=5D5L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&SESSIONID=5D5L9FF1ADFF3" "Post11821Cm
://buttercup-16&product_id=RP-LI-02" 468 125.17 14.1... rreen?category_id=FLOWERS&SESSIONID=5D5L9FF1ADFF3 HTTP 1.1" 200 385 "PCAP data" "11
do?action=purchase&itemId=EST-26&SESSIONID=5D5L9FF1ADFF3 HTTP 1.1" "GET /category.screen?category_id=FLOWERS&SESSIONID=5D5L9FF1ADFF3 HTTP 1.1" 200 385 "PCAP data" "11
/buttercup-16&product_id=RP-LI-02" "GET /category.screen?category_id=FLOWERS&SESSIONID=5D5L9FF1ADFF3 HTTP 1.1" 200 385 "PCAP data" "11

Where We Are Today

- ▶ 8+TB data/day
- ▶ 60+ distinct sourcetypes
- ▶ 75+ Custom Threat Use-Cases
- ▶ 100+ Scheduled Reports/Dashboards/Form Searches

| Name | Date Modified | Size | Kind |
|---|------------------------|------------|--|
| Report | Jun 21, 2017, 11:53 AM | 2 KB | TextEd...ument |
| | 017, 4:07 PM | Zero bytes | TextEd...ument |
| 1 What do you want to do? | 017, 4:00 PM | 779 bytes | TextEd...ument |
| | 017, 4:12 PM | 592 bytes | TextEd...ument |
| | 2017, 9:42 AM | 5 KB | TextEd...ument |
| | 2017, 9:12 AM | 6 KB | TextEd...ument |
| | 2017, 4:02 PM | 5 KB | TextEd...ument |
| | 2017, 9:04 AM | 700 bytes | TextEd...ument |
| | 2017, 2:43 PM | 9 KB | Plain Text |
| | 2017, 12:01 PM | 4 KB | TextEd...ument |
| | 2017, 8:29 AM | 325 bytes | TextEd...ument |
| | 2017, 5:15 PM | 425 bytes | TextEd...ument |
| | 017, 7:59 AM | 2 KB | TextEd...ument |
| | 017, 7:59 AM | 2 KB | TextEd...ument |
| | 017, 2:09 PM | 13 KB | TextEd...ument |
| | 017, 4:02 PM | 12 KB | TextEd...ument |
| | 2017, 12:53 PM | 1 KB | TextEd...ument |
| 2 splunk system. Close it. | 2195 4/7/15 20:27 | Started | Data Science Other/Gener Security 4/7/15 20:27 |
| 3 Ports Authority is in production. Close it. | 2213 4/8/15 8:47 | Started | Data Science Other/Gener Security 4/8/15 8:47 |
| 4 Needs to be addressed - the default content is meh. | 2210 4/8/15 7:41 | Started | Data Science Other/Gener Security 4/8/15 7:41 |
| 5 In production... close it. | 2226 4/8/15 13:54 | Started | Data Science Other/Gener Other 4/8/15 13:54 |

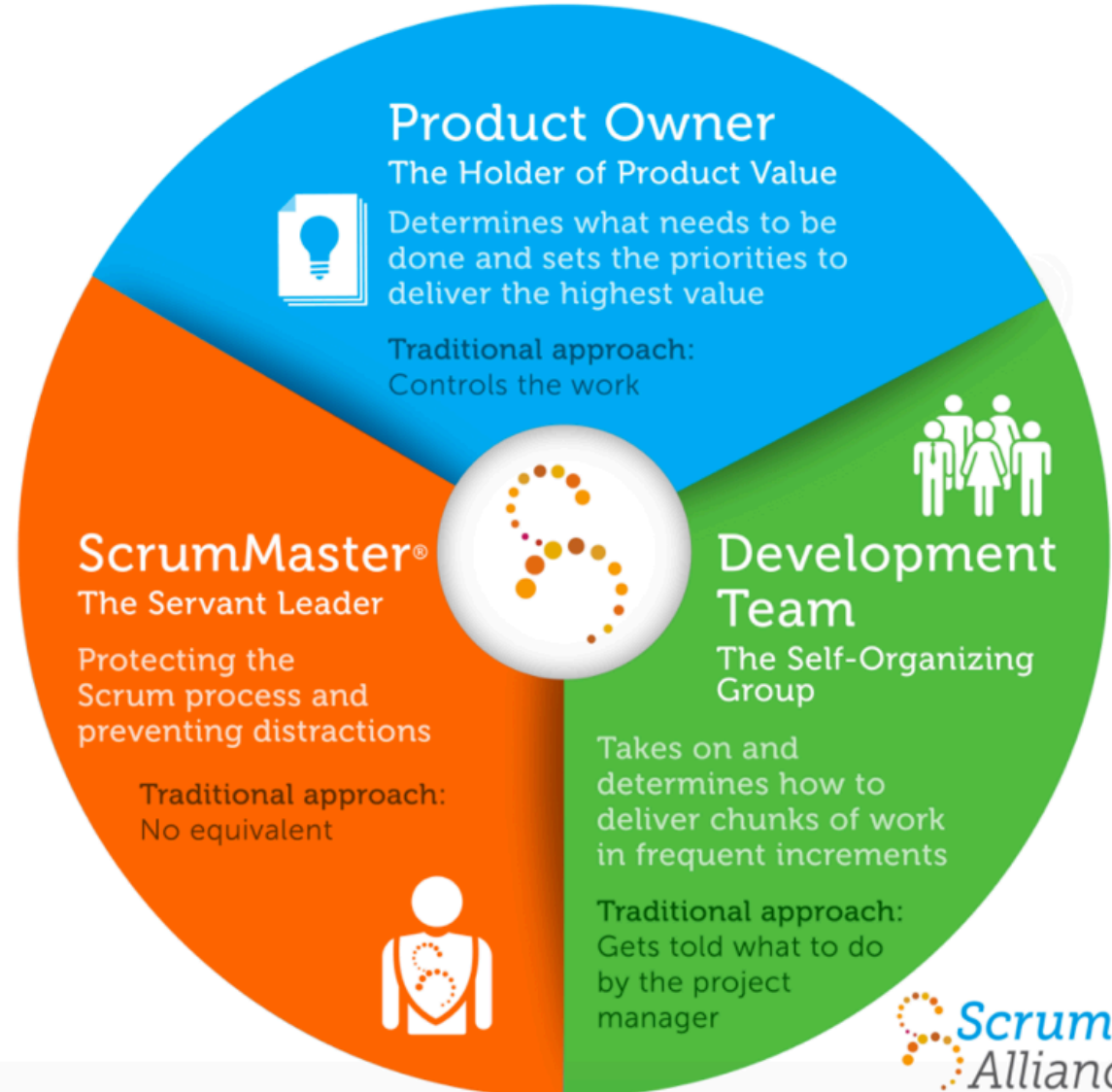
| A | I |
|------------------------------|---|
| 241 BB:Kaiser:MalwareF: USER | |
| 242 BB:Kai | A |
| 243 BB:Kai | |
| 244 BB:Kai 1 What do y ID | |
| 245 BB:Kai 8 Drop/Canc | |
| 246 BB: 9 Drop/Canc | |
| 247 BB: 11 Drop/Canc | |
| 248 BB: | |
| 251 BB: | |
| 253 BB: | |
| 254 MV | |
| 255 BB: | |
| 256 BB: | |
| 257 BB: | |
| 260 Pol | |
| 261 Pol | |
| 264 BB: 12 Drop/Canc | |
| 265 BB:Kai 13 Drop/Canc | |
| 266 BB: Cr | |
| 267 BB:Kai | |

130.60.4 - - [07/Jun 21 18:10:57:123] "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-SW-03" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.11.189] "GET /category.screen?category_id=FLOWERS&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 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1" 130.60.4 - - [07/Jun 21 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&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 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1" 130.60.4 - - [07/Jun 21 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&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 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1" 130.60.4 - - [07/Jun 21 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&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 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1"

Scrum in 100 Words

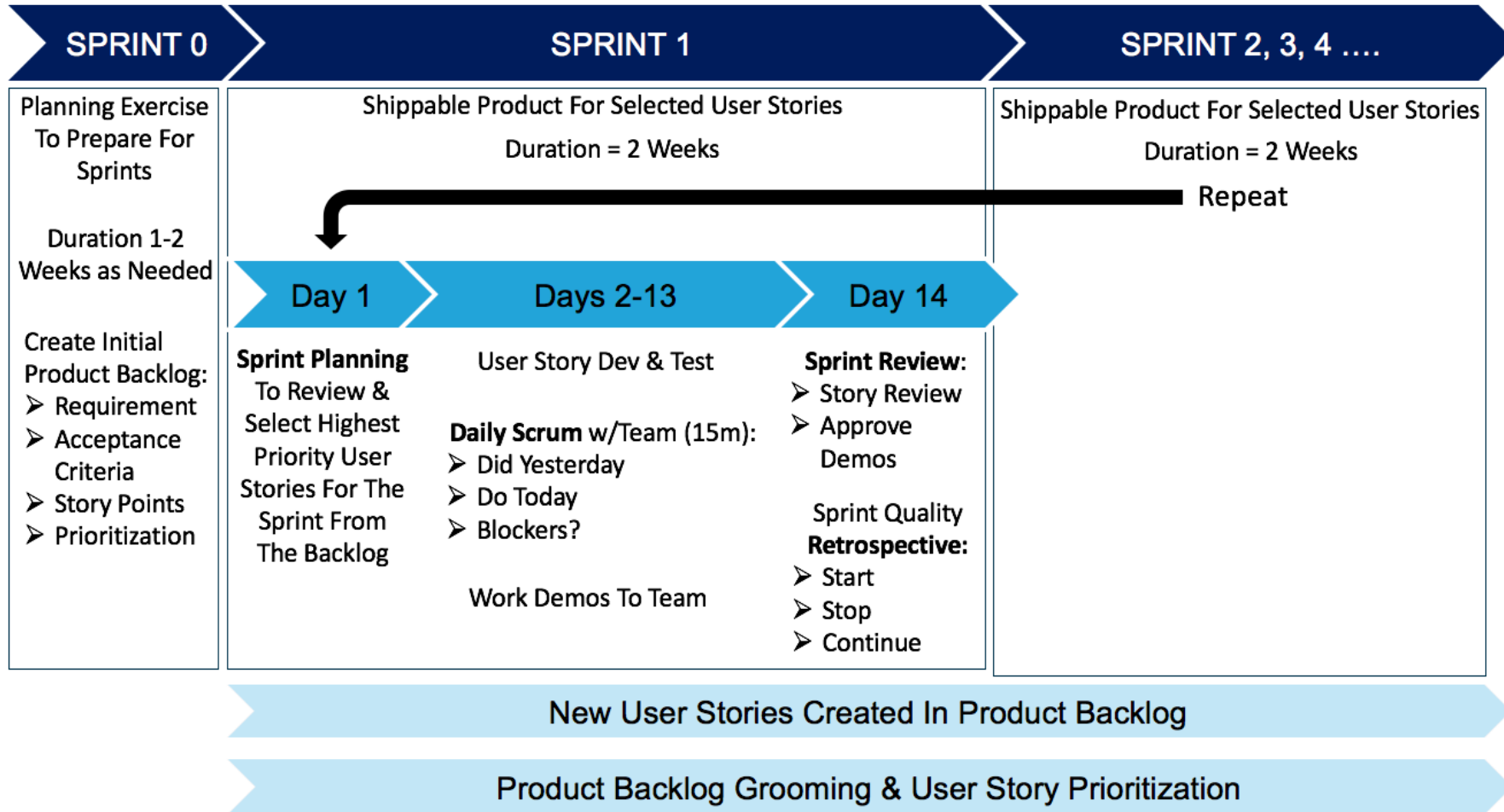
- Scrum is an agile process that allows us to focus on delivering the highest business value in the shortest time.
- It allows us to rapidly and repeatedly inspect actual working software (every two weeks to one month).
- The business sets the priorities. Teams self-organize to determine the best way to deliver the highest priority features.
- Every two weeks to a month anyone can see real working software and decide to release it as is or continue to enhance it for another sprint.

What does a Scrum look like?



130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/category.screen?category_id=F1-SW-01" ...

Scrum Framework Process



130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15L9FF10ADFF10 HTTP 1.1" 404 322 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14

Example Story

Summary* **MW -Attacking IP High Data Rate Outbound**

Issue Type* **Story**

Reporter*

Component/s **None**

Description

Style | B | I | U | A | | | | | | | | | |

As a member of the team I need to do detect attacking IP's that are receiving a high ratio of data so we can detect potential attacker activity corresponding with potential data exfiltration and respond accordingly.

Acceptance Criteria:

All sub-tasks are Complete and the correlation search/model has been implemented and is enabled in Production as at least Informational or a low Severity/Confidence

New Story Created for TV Team to do use case validation

Fix Version/s

Priority **Medium**

Attachment

Linked Issues **relates to**

Issue

Assignee **Matt Parks**

[Assign to me](#)

Epic Link **Security Analytics Operations**

Sprint

Completed sprints **Use Case Content Sprint 9**

Story Points **13**

CRDC Tag **MW x SA x es x**

Actual Work **13**

TL; DR **Alert for attackers with high volume outbound**

```

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&item_id=EST-6&product_id=FI-SW-01"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D55L7FF6ADF0 HTTP 1.1" 404 322 "http://buttercup-shopping.com/cart.do?action=purchase&item_id=EST-268product_id=KQ-CU-0"
317.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&item_id=EST-18&product_id=AV-CB-01&JSESSIONID=5D15L9FF1ADF3 HTTP 1.1"
125.17.14 - - [07/Jan 18:10:55:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=remove&item_id=EST-SURPRISE&JSESSIONID=5D55L9FF1ADF3 HTTP 1.1"

```

So what do we do with all this JIRA Data?

- Improve situational awareness
- Visualize our JIRA activity
- Improve our development process
- Answer questions

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=FI-SW-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268&product_id=KQ-CW-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)"
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=FI-SW-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268&product_id=KQ-CW-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)"
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=FI-SW-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268&product_id=KQ-CW-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)"

Bob in accounting was infected by <insert-threat-of-the-day-here>, who else was infected?

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-SW-01" "Mozilla/5.0 (Windows NT 6.0; WOW64; rv:55.0) Gecko/20100101 Firefox/55.0"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268product_id=KB-CW-01" "Mozilla/5.0 (Windows NT 6.0; WOW64; rv:55.0) Gecko/20100101 Firefox/55.0"
137.27.160.0 - - [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 HTTP 1.1" 200 3865 "Mozilla/5.0 (Windows NT 6.0; WOW64; rv:55.0) Gecko/20100101 Firefox/55.0"
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-SW-01" "Mozilla/5.0 (Windows NT 6.0; WOW64; rv:55.0) Gecko/20100101 Firefox/55.0"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268product_id=KB-CW-01" "Mozilla/5.0 (Windows NT 6.0; WOW64; rv:55.0) Gecko/20100101 Firefox/55.0"
137.27.160.0 - - [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 HTTP 1.1" 200 3865 "Mozilla/5.0 (Windows NT 6.0; WOW64; rv:55.0) Gecko/20100101 Firefox/55.0"
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-SW-01" "Mozilla/5.0 (Windows NT 6.0; WOW64; rv:55.0) Gecko/20100101 Firefox/55.0"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268product_id=KB-CW-01" "Mozilla/5.0 (Windows NT 6.0; WOW64; rv:55.0) Gecko/20100101 Firefox/55.0"
137.27.160.0 - - [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 HTTP 1.1" 200 3865 "Mozilla/5.0 (Windows NT 6.0; WOW64; rv:55.0) Gecko/20100101 Firefox/55.0"

Anyone heard of Wannacry?

▶ 14 separate JIRA Stories

- 3 new Correlation Searches
- 6 Research Stories
- 2 Tuning Requests
- 3 Stories for Follow-up/Remediation

Security Analytics / **New Threat Detection - Code Execution Vulnerability** - Microsoft Windows SMB Remote 15 of 15

Edit Comment Assign More Admin Export

Details

| | | | |
|--------------------|-------|----------------|-----------------|
| Type: | Story | Status: | APPROVED |
| Priority: | High | | (View Workflow) |
| Affects Version/s: | None | Resolution: | Unresolved |
| | | Fix Version/s: | None |

Epic Link: [Security Analytics Operations](#)

Sprint: Use Case Content Sprint 14

Story Points: 13

CRDC Tag: SA es ransomware wannacry

Actual Work: 8

People

Assignee: Ruperto Razon

Reporter:

Votes: [Vote for this issue](#)

Watchers: [Start watching this issue](#)

Dates

Created: 26/Jun/17 11:25 AM

Updated: 26/Jun/17 11:25 AM

Agile

Completed Sprint: [Use Case Content Sprint 14 ended 17/May/17](#)

[View on Board](#)

Description

As a member of TDA I need to do create a Use Case so we can detect any potential WannaCry ransomware outbreak, and respond accordingly. See original notes from [\[link\]](#) in [\[link\]](#) Comments.

Acceptance Criteria:

1. All sub-tasks are Complete and the correlation search/model has been implemented and is enabled in Production as at least Informational or a low Severity/Confidence
2. Notification is sent to the TDA manager and team lead
3. **New Story** Created for TV Team to do use case validation - Clone [\[link\]](#) and change the data source name.
4. **New Tuning Request** created for SA team to set accordingly the Correlation Search Severity or I [\[link\]](#) Alert Severity/Confidence, based on TDA teams research.

What does our security coverage look like, from a use-case perspective?

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=FI-5W-03"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D95L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268product_id=KQ-CW-01"
137.27.160.0 - - [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 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-148"
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=FI-5W-03"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D95L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268product_id=KQ-CW-01"
137.27.160.0 - - [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 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-148"

Deployed Use-Case Visibility

Security Analytics Visibility

[Edit](#)
[More Info](#)
↓
🔄

Enabled Correlation Search Breakdown by Team

Enabled Correlation Search Breakdown by Severity

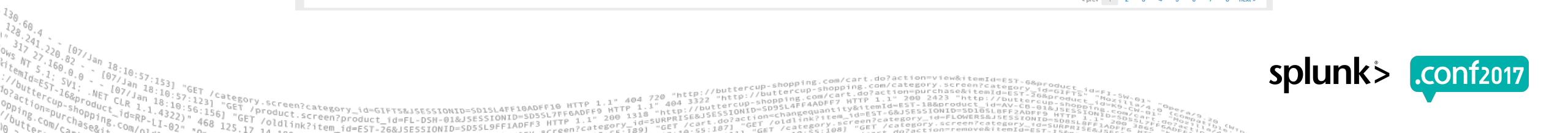
Use Case Count by Team / Severity

| designation | 1-critical | 2-high | 3-medium | 4-low | 5-informational |
|-------------|------------|--------|----------|-------|-----------------|
| DE | 3 | 1 | 1 | 3 | 1 |
| DL | 0 | 0 | 1 | 1 | 1 |
| LM | 2 | 5 | 5 | 6 | 13 |
| MW | 2 | 3 | 5 | 7 | 14 |
| TD | 0 | 0 | 0 | 0 | 2 |

Changes in Triggered Notable Events - Past 30 Days - by Correlation Search

Enabled Use Case - Details

| designiation | rule_name | description | severity | status |
|--------------|--|--|---------------|---------|
| 1 DE | b-High Rate of Transfer Outside US | Detects a high rate of transfer of data destined for locations outside of the United States | low | Enabled |
| 2 DE | -Slow Rate of Transfer | Identifies slow rate transfers, these may be potential | low | Enabled |
| 3 DE | a-L2R DNS IDS Events By Src | Detects L2R DNS intrusion detection alerts that are not blocked | low | Enabled |
| 4 DE | -TOR Activity Detected | Alerts when traffic classified as TOR is detected | informational | Enabled |
| 5 DE | -Abnormally High Number of HTTP Method Events By Src | Alerts when a host has an abnormally high number of HTTP requests by http method. | medium | Enabled |
| 6 DE | -Excessive DNS Queries | Alerts when a host starts sending excessive DNS queries | high | Enabled |
| 7 DE | -Unknown TCP Traffic - High Volume Outbound | Triggers when a large amount (over 500MB) of data outbound triggers where the can't identify the application, rather identifies it as unknown-tcp. | critical | Enabled |
| 8 DE | a-Malware and Exfiltration Activity -24hrs | Monitor for possible data exfiltration 24hrs before a Malware event | critical | Enabled |
| 9 DE | b-Malware and Exfiltration Activity +24hrs | Monitor for possible data exfiltration 24hrs after a Malware event | critical | Enabled |
| 10 DL | -Outbound DLP Unencrypted Traffic | This alert gathers activity that is non email related; heading to outbound IP's as well as DMZ IP address | low | Enabled |



Searches!

Note: <insertyourdatahere>

► SA Visualization Dashboard

- Enabled Correlation Search Breakdown by Team
 - `|rest /services/alerts/correlationsearches splunk_server=local | rename eai:acl:app as application, title as csearch_name |join type=outer app csearch_name [rest /services/saved/searches| rename eai:acl:app as application, title as csearch_name, search as csearch|table app, csearch_name, csearch, disabled]|eval status=if(disabled==1,"Disabled","Enabled") | search status=Enabled | eval splitdes = split(rule_title, "-"), designation = mvindex(splitdes, 0) |table designation security_domain, rule_title, csearch_name, description, severity, csearch, disabled, status | stats count by designation | sort -count`
- Enabled Correlation Search Breakdown by Severity
 - `|rest /services/alerts/correlationsearches splunk_server=local | search rule_title!="" | rename eai:acl:app as application, title as csearch_name |join type=outer app csearch_name [rest /services/saved/searches| rename eai:acl:app as application, title as csearch_name, search as csearch|table app, csearch_name, csearch, disabled]|eval status=if(disabled==1,"Disabled","Enabled") | search status=Enabled | eval splitdes = split(rule_title, "-"), designation = mvindex(splitdes, 0) |table designation security_domain, rule_title, csearch_name, description, severity, csearch, disabled, status | eval Severity=case(severity=="critical","1-critical", severity=="high","2-high", severity=="medium","3-medium", severity=="low","4-low", severity=="informational","5-informational") | stats count by Severity`

Searches!

Note: <insertyourdatahere>

► SA Visualization Dashboard (cont.)

- Use Case Count by Team / Severity
 - `|rest /services/alerts/correlationsearches splunk_server=local | rename eai:acl:app as application, title as csearch_name |join type=outer app csearch_name [rest /services/saved/searches| rename eai:acl:app as application, title as csearch_name, search as csearch|table app, csearch_name, csearch, disabled]|eval status=if(disabled==1,"Disabled","Enabled") | search status=Enabled | eval splitdes = split(rule_title, "-"), designation = mvindex(splitdes, 0) | table designation rule_title description, severity, status | eval Severity=case(severity=="critical","1-critical", severity=="high","2-high", severity=="medium","3-medium", severity=="low","4-low", severity=="informational","5-informational") | chart count as "Rule Count" by designation, Severity`
- Changes in Triggered Notable Events - Past 30 Days - by Correlation Search
 - ``notable` | search search eventtype!=notable_suppression* | bin _time span=24h |stats count by _time, search_name | streamstats window=2 global=f current=t first(count) as previous by search_name | eval delta=count-previous | eval time=_time | table search_name, time, delta, count`
- Enabled Use Case – Details
 - `|rest /services/alerts/correlationsearches splunk_server=local | search rule_title!="" | rename eai:acl:app as application, title as csearch_name |join type=outer app csearch_name [rest /services/saved/searches| rename eai:acl:app as application, title as csearch_name, search as csearch|table app, csearch_name, csearch, disabled]|eval status=if(disabled==1,"Disabled","Enabled") | search status=Enabled | eval splitdes = split(rule_title, "-"), designation = mvindex(splitdes, 0) |table designation rule_name description, severity, status | sort designation, rule_name`

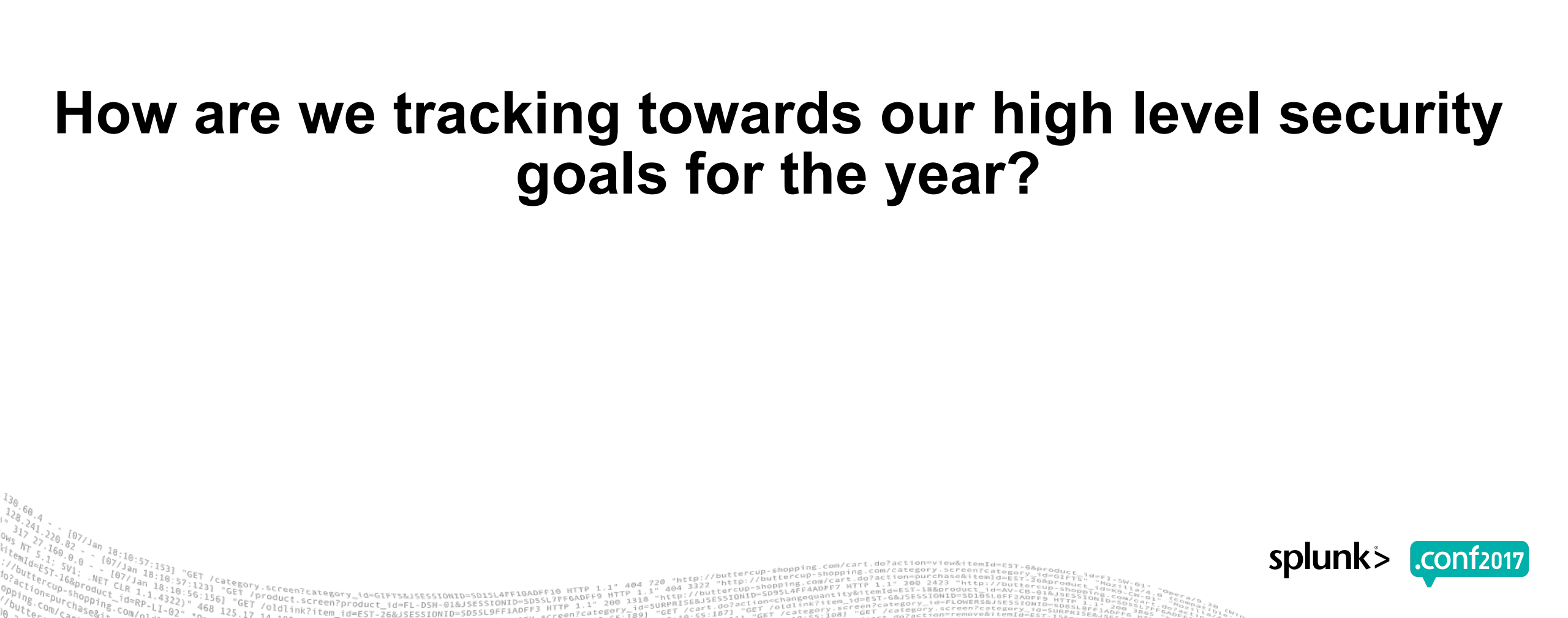
Searches!

Note: <insertyourdatahere>

► SA Visualization Dashboard (cont.)

- Correlation Search Performance
 - index=_internal host=<yourSHhost> source=*scheduler.log app="" savedsearch_name="" (app=DA-* OR app=SA-*) (savedsearch_name=<yourcorrsearchname> OR savedsearch_name=<yourcorrsearchname> OR savedsearch_name=<yourcorrsearchname>)| eval run_time=run_time/60|stats min(run_time) as "Min runtime (min)", avg(run_time) as avg_runtime, max(run_time) as max_runtime, count(eval(status!="continued")) AS total_exec, count(eval(status=="success")) as "Successful executions", count(eval(status=="skipped")) AS "Skipped executions" by app, savedsearch_name, user host | stats first(*) as * by savedsearch_name | eval interval_usage_ratio=round((median_runtime/schedule_period),2) | search total_exec>0 | rename savedsearch_name AS Rule_name app AS App avg_runtime AS "Avg runtime (min)" max_runtime AS "Max runtime (min)" user AS User total_exec AS "Total executions" | table Rule_name "Min runtime (min)" "Avg runtime (min)" "Max runtime (min)" "Total executions" "Successful executions" "Skipped executions"| sort - "Avg runtime (min)" "Total executions"|join Rule_name [] rest splunk_server=* /servicesNS/-/-/admin/savedsearch/ earliest_time=-0s@s latest_time=+2d@d search="is_scheduled=1" search="disabled=0" search="(eai:acl.app=SA-* OR eai:acl.app=DA-*)"| dedup title| rename title AS Rule_name dispatch.earliest_time AS earliest_time dispatch.latest_time AS latest_time|table Rule_name cron_schedule earliest_time latest_time]
- Skipped Correlation Searches
 - index=_internal host=<yourSHhost> source=*scheduler.log savedsplunker status=skipped (app=SA-* OR app=DA-*) (savedsearch_name=<yourcorrsearchname> OR savedsearch_name=<yourcorrsearchname> OR savedsearch_name=<yourcorrsearchname>)| stats count values(scheduled_time) as scheduled_time values(_time) as _time by host savedsearch_name, app | sort - SkipCount | rename savedsearch_name AS "Scheduled search name" count AS "Skip count" host AS Server | fieldformat scheduled_time=strftime(scheduled_time, "%c") | fieldformat _time=strftime(_time, "%c")

How are we tracking towards our high level security goals for the year?



Status Metricization

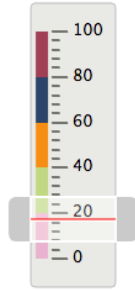
Used to show completeness of status regardless of velocity in a given Scrum related to Epic that have heretofore been unaccomplished but are tied to the current Sprint.

Edit More Info Download Print

Percent Completometer

12.17 %

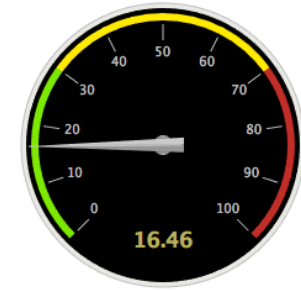
Truthiness



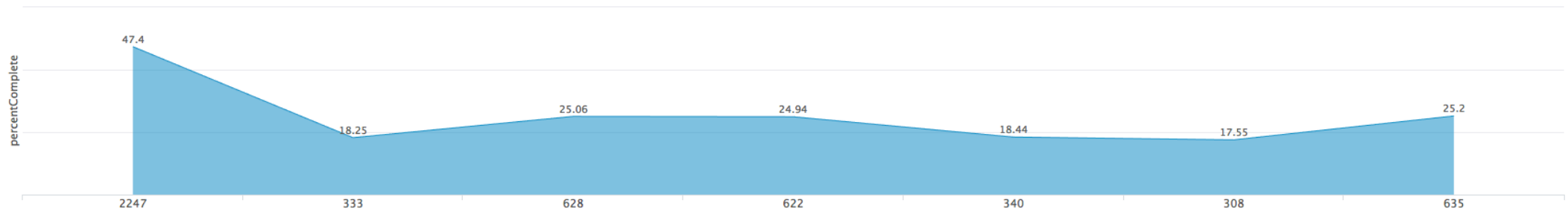
Number of



Visualization of Velocity of Completeness



Completion Percentage History



Should we develop this incredibly well designed use-case?

no

Excessive Extraneous Authentication Trend

596,713 number of things -209,501 ↓

```
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=F1-5W-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"
125.17.14. - - [07/Jan 18:10:55:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/product.do?action=remove&itemId=EST-14"
125.17.14. - - [07/Jan 18:10:55:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/product.do?action=remove&itemId=EST-14"
125.17.14. - - [07/Jan 18:10:55:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/product.do?action=remove&itemId=EST-14"
125.17.14. - - [07/Jan 18:10:55:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/product.do?action=remove&itemId=EST-14"
125.17.14. - - [07/Jan 18:10:55:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/product.do?action=remove&itemId=EST-14"
125.17.14. - - [07/Jan 18:10:55:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/product.do?action=remove&itemId=EST-14"
125.17.14. - - [07/Jan 18:10:55:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/product.do?action=remove&itemId=EST-14"
125.17.14. - - [07/Jan 18:10:55:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/product.do?action=remove&itemId=EST-14"
```

Searches!

Note: <insertyourdatahere>

► Metricization Dashboard

- Percent Completometer
 - `index=<yourindex> sourcetype=<yoursourcetype> | head 5000 | search bytes<9801 | head 1 | table bytes | eval percentComplete=tostring(sqrt(bytes), "commas") | fields percent`
- Complete Truthiness
 - `index=<yourindex> sourcetype=<yoursourcetype> | head 110 | search bytes<9801 | tail 1 | table bytes | eval percentComplete=tostring(sqrt(bytes), "commas") | fields percentCompleteNumber ofindex=* | head 1 | eval sourcetype=0 | table sourcetype`
- Visualization of Velocity of Completeness
 - `index=<yourindex> sourcetype=<yoursourcetype> | head 100 | search bytes<9801 | head 1 | table bytes | eval percentComplete=tostring(sqrt(bytes), "commas") | fields percentComplete`
- Completion Percentage History
 - `index=<yourindex> sourcetype=<yoursourcetype> | head 10000 | search bytes<9801 bytes>4 | head 7 | table bytes | eval percentComplete=tostring(sqrt(bytes), "commas") | rename bytes as "Timechart Histor-o-meter"`

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-SW-03" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/50.0.2688.132 Safari/537.36" 128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=KQ-CW-01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/50.0.2688.132 Safari/537.36" 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 HTTP 1.1" 200 3855 "http://shopping.com/cart.do?action=purchase&itemId=EST-16&product_id=RP-LI-02" "0" 125.17.14.189 "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D15LAF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-6&product_id=FI-SW-03" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/50.0.2688.132 Safari/537.36" 128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=KQ-CW-01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/50.0.2688.132 Safari/537.36" 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 HTTP 1.1" 200 3855 "http://shopping.com/cart.do?action=purchase&itemId=EST-16&product_id=RP-LI-02" "0" 125.17.14.189 "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D15LAF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-6&product_id=FI-SW-03" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/50.0.2688.132 Safari/537.36"

Searches!

Note: <insertyourdatahere>

► Metricization Dashboard (cont.)

- Should we develop this incredibly well designed use-case?
 - index=<yourindex> | stats count | eval countresult=if(count=5,"no","yes") | rename countresult AS value | table value count
- Completion Percentage History
 - index=<yourindex> sourcetype=<yoursourcetype> | head 10000 | search bytes<9801 bytes>4 | head 7 | table bytes | eval percentComplete=tostring(sqrt(bytes), "commas") | rename bytes as "Timechart Histor-o-meter"
- Excessive Extraneous Authentication Trend
 - | tstats prestats=t count where index=<yourindex> sourcetype=<yoursourcetype> by _time span=1d | timechart count

JIRA Epic Tracking

Demo JIRA Epic Tracking
demo jira epic tracking
Edit Export ...

Stories Completed By Epic 2017

Expansion Models

Operationalization of platform support

Operationalize

Response Orchestration

Red Team/Blue Team Exercises

Cloud Security: Defined

Data Onboarding

Data Science Migration

Implement Splunk releases

Story Summaries by Epic

| Epic Link | Epic Name | Story Count | Story ID | Summary |
|-----------|-----------------------------------|-------------|----------|--|
| | Security Analytics Operations | 13 | | <p>Upgrade/Migration - Prod</p> <p>Data Dictionary Indexes N-Z: short and long descriptions</p> <p>Data Dictionary: index descriptions</p> <p>Remove From Alerts</p> <p>TV team test</p> <p>Missing alerts</p> <p>Research: - alternate case</p> <p>Security Analytics Visibility Dashboard: Update searches for ES upgrade</p> <p>Tuning Request - Update Report correlation searches</p> <p>Tuning: Further Adjustments</p> <p>Tuning: not firing correctly/has "no results found"</p> <p>Tuning: - Update rule to take into account the</p> <p>Update</p> |
| | Implement releases | 1 | | Validate Splunk |
| | Response Orchestration | 1 | | Review data gathering searches |
| | Operationalize | 1 | | - Notable Tuning |
| | Expansion of UBA Models (11/2017) | 8 | | <p>adding service accounts</p> <p>- Port Scan</p> <p>- Upload to new country</p> <p>- phase 1 report out</p> <p>- phase 1 report out mgmt</p> |
| | | | Testing | acis |

Searches!

Note: <insertyourdatahere>

► JIRA Epic Tracking

- Stories Completed By Epic 2017
 - |jira issues <issue filter> | join type=left "Epic Link" [|jira issues 10412 | rename Key AS "Epic Link" | fields "Epic Link" "Epic Name"] | stats count(Key) AS "Story Count" by "Epic Name"
- Story Summaries by Epic
 - |jira issues <issue filter> | stats count(Key) AS "Story Count" values(Key) AS "Story ID" values(Summary) AS Summary by "Epic Link" | join type=left "Epic Link" [|jira issues 10412 | rename Key AS "Epic Link" | fields "Epic Link" "Epic Name"] | table "Epic Link" "Epic Name" "Story Count" "Story ID" Summary



In General, This Is What We Do...

The screenshot shows a Confluence page for 'Security Analytics'. The page header includes navigation options like 'Spaces', 'People', 'Questions', 'Calendars', and 'Create'. The page content is organized into sections: 'Who We Are' with a team table, 'What We Do' with sub-sections for 'Data Science', 'Security Analytics', and 'Process Engineering', and 'Our Tools' with a description of a log collection tool and a security framework. A sidebar on the left contains navigation links for 'Pages', 'Blog', 'Questions', 'Calendars', and 'SPACE SHORTCUTS'. A top navigation bar shows 'Edit', 'Save for later', 'Watching', and 'Share' options.

Who We Are:

| | | | | | | | |
|-------------------|--------------------------|----------------|--------------------|--------------------|-------------------|-------------------|------------------|
| | @ Matt Parks | | | @ Ruperto S. Razon | | | |
| Director Emeritus | Manager and Buffalooney! | Data Scientist | Security Analytics | That Guy | Threat Validation | Threat Researcher | Process Engineer |

What We Do:

- Data Science**
Research and development of advanced analytical models to improve the security of the KP network. Correlation of multiple disparate large-scale data sets to find interesting patterns and behavior. Assistance with investigations that require big data tools to process large requests.
- Security Analytics**
The Security Analytics team is comprised of Data Scientists and Sr. Security Analysts and Engineers. Our goals are to provide actionable, integrated, and context rich alerts leveraging expertise in Information Security and Big Data Analytics tools; using an Agile (Scrum) method to help manage workflow. Also Pertorio like to do Metrics dashboards.
- Process Engineering**
is our resident Agile Coach, Process Engineer, Scrum Master, Project Coordinator, and all around good guy. He helps shepherd the Security Analytics and other CRDC teams through the process quagmire, looking to streamline and simplify where appropriate (which is just about everywhere).

Our Tools:

Log collection, aggregation, and analysis tool that collects various types of security, application, server and other machine data. hearts time series data.

Security Framework for logs collected by core
This is the application from which the Threat Detection Analysis team triages, investigates and escalates threats to the KP network.



Searches!

Note: <insertyourdatahere>

► JIRA Current Sprint Dashboard

- Current Sprint Stories Resolved
 - | jira issues <current sprint filter> | search Resolved!=null | rex field=Assignee "\"displayName\": \"(?<Assignee_Name>\w+\s\w+)\" | table Key Summary "TL; DR" Assignee_Name
- current sprint stories in progress
 - | jira issues <current sprint filter> | search Resolved=null | rex field=Assignee "\"displayName\": \"(?<Assignee_Name>\w+\s\w+)\" | table Key Summary "TL; DR" Assignee_Name
- closed in the last 24h - for morning call
 - | jira issues <current sprint filter> | rex field=Assignee "\"displayName\": \"(?<Assignee_Name>\w+\s\w+)\" | table Key Summary "TL; DR" Assignee_Name
- story points available
 - | jira issues <current sprint filter> | stats sum("Story Points") AS value | eval value=rnd(value,0)
- story points completed
 - | jira issues <current sprint filter> | search Resolved!=null | stats sum("Story Points") AS value | eval value=round(value,0)
- story points remaining
 - | jira issues <current sprint filter> | search Resolved=null | stats sum("Story Points") AS value | eval value=round(value,0)

Searches!

Note: <insertyourdatahere>

► JIRA Current Sprint Dashboard

- Current Sprint Stories Resolved
 - | jira issues <current sprint filter> | search Resolved!=null | rex field=Assignee "\"displayName\": \"(?<Assignee_Name>\w+\s\w+)\" | table Key Summary "TL; DR" Assignee_Name
- current sprint stories in progress
 - | jira issues <current sprint filter> | search Resolved=null | rex field=Assignee "\"displayName\": \"(?<Assignee_Name>\w+\s\w+)\" | table Key Summary "TL; DR" Assignee_Name
- closed in the last 24h - for morning call
 - | jira issues <current sprint filter> | rex field=Assignee "\"displayName\": \"(?<Assignee_Name>\w+\s\w+)\" | table Key Summary "TL; DR" Assignee_Name
- story points available
 - | jira issues <current sprint filter> | stats sum("Story Points") AS value | eval value=rnd(value,0)
- story points completed
 - | jira issues <current sprint filter> | search Resolved!=null | stats sum("Story Points") AS value | eval value=round(value,0)
- story points remaining
 - | jira issues <current sprint filter> | search Resolved=null | stats sum("Story Points") AS value | eval value=round(value,0)

Sprint Review/Monthly Demo

| Key | Summary | Assignee | Status | CRDC Tag | Story Points | Sprint |
|-----|--|----------|----------|--|--------------|--|
| | Use Case DBIR Present Coverage Evaluation 2017 | | Approved | SA, demo | 21 | Use Case Content Sprint 14, Use Case Content Sprint 15 |
| | xxxxx - Attacking IP Long Duration Connection | | Approved | SA, demo, es | 13 | Use Case Content Sprint 13, Use Case Content Sprint 14 |
| | xxxxx - TV team test | | Approved | SA, TV, demo, tvtest | 5 | Use Case Content Sprint 15 |
| | xxxxx - Attacking IP Successful Authentication | | Approved | SA, demo, es | 13 | Use Case Content Sprint 13, Use Case Content Sprint 14 |
| | xxxxx - TV team test | | Approved | SA, TV, demo, tvtest | 5 | Use Case Content Sprint 14 |
| | Testing xxxxx-Unknown TCP Traffic - High Volume Outbound | | Approved | SA, TV, demo, tvtest | 8 | Use Case Content Sprint 15 |
| | Research: Long domain activity similar to the Wannacry sandbox domains | | Approved | SA, demo, wannacry | 3 | Use Case Content Sprint 14 |
| | New Correlation Search xxxxx-WannaCry Ransomware-AV Infection | | Approved | LM, SA, demo, es, ransomware, wannacry | 5 | Use Case Content Sprint 14 |
| | New Threat Detection - xxxxx - Microsoft Windows SMB Remote Code Execution Vulnerability | | Approved | SA, demo, es, ransomware, wannacry | 13 | Use Case Content Sprint 14 |
| | Upgrade - Enterprise Security from xxxx to xxxx | | Approved | DPS, SA, demo, es, | 13 | Use Case Content Sprint 15 |
| | suspicious external connection from PCI devices | | Approved | SA, demo | 5 | Use Case Content Sprint 15 |
| | a new Windows event logs dashboard | | Approved | SA, demo | 3 | Use Case Content Sprint 12, Use Case Content Sprint 13, Use Case Content Sprint 14, Use Case Content Sprint 15 |

```

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=5D15LAF10ADFF10 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&SESSIONID=5D55L7FF6ADFF9 HTTP 1.1" 404 322 "http://shopping.com/category.screen?category_id=GIFTS"
ows NT 27.160.0.0 - - [07/Jan 18:10:56:156] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5D55L7FF6ADFF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&SESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 385 "http://shopping.com/category.screen?category_id=FLOWERS&SESSIONID=5D55L9FF1ADFF3"
://buttercup-shopping.com/ol-?product_id=RP-LI-02" 468 125.17 14 "http://shopping.com/category.screen?category_id=FLOWERS&SESSIONID=5D55L9FF1ADFF3"
do?action=purchase&itemId=EST-26&SESSIONID=5D55L9FF1ADFF3" 189 "GET /category.screen?category_id=FLOWERS&SESSIONID=5D55L9FF1ADFF3" 189 "GET /category.remove&itemId=EST-1"

```

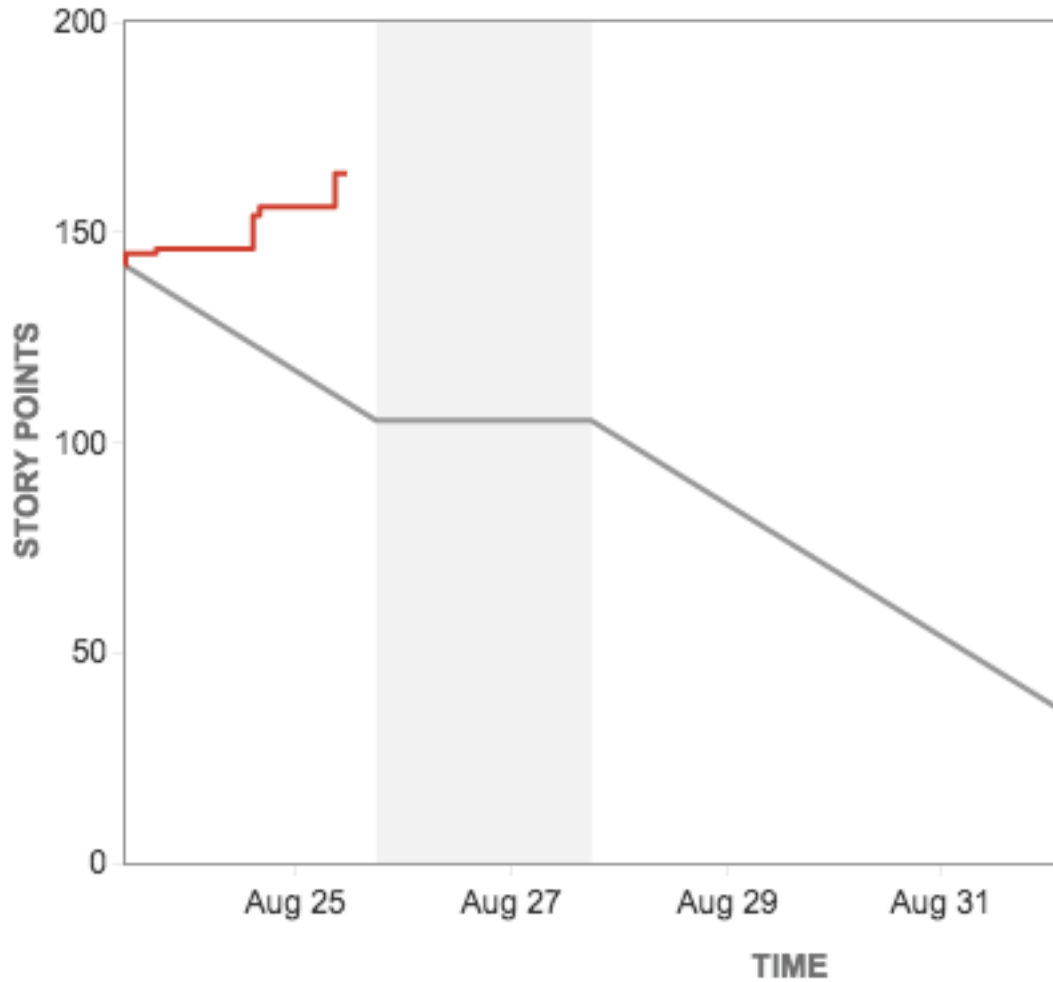
Recap

- ▶ Gave you tips on how you can build a flexible content development process
- ▶ Shared with you a real-world example of how this flexible process works in practice
- ▶ Provided you with dashboards and searches that will improve visibility of your security posture, high-level goal tracking and content dev capacity



What will we do in the next 12 months?

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=FI-SW-01" Mozil...
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD3SL7FFGADFF0 HTTP 1.1" 404 3322 "http://shopping.com/cart.do?action=purchase&itemId=EST-268product_id=KQ-CU-01" Comp...
ows NT 5.1; SV1; .NET CLR 1.1.4322) "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FFIADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD18SL8FF2ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268product_id=KQ-CU-01" Comp...
://buttercup-shopping.com/product_id=RP-LI-02" 468 125.17 14.1.1.189) "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5SL9FFIADFF3 HTTP 1.1" 200 3865 "http://shopping.com/cart.do?action=purchase&itemId=EST-268product_id=KQ-CU-01" Comp...
://buttercup-shopping.com/product_id=RP-LI-02" 468 125.17 14.1.1.189) "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5SL9FFIADFF3 HTTP 1.1" 200 3865 "http://shopping.com/cart.do?action=purchase&itemId=EST-268product_id=KQ-CU-01" Comp...

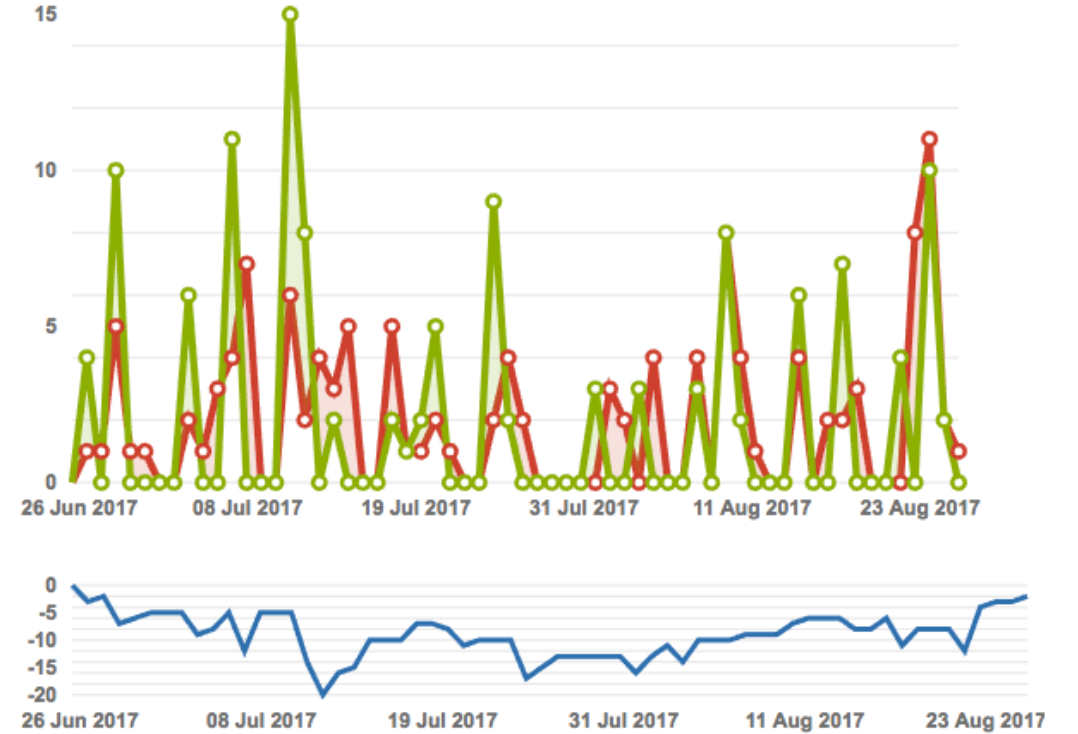


| |
|--------|
| |
| |
| Sprint |
| 1 |
| 1 |
| 1 |
| 1 |
| 1 |
| 1 |
| 1 |
| 1 |
| 1 |
| 1 |
| 1 |
| 1 |
| 2 |
| 2 |
| 2 |
| |
| |
| |

| | | | | | | |
|----|--------------------|--|------------|------------|------------|------------|
| 12 | Hot Sprints | | 288 | 144 | 4/2 | 555 |
| | Avg/Sprint | | 24 | 12 | 39 | 30 |

- Guideline
- Remaining Values

Created vs. Resolved Chart: Security Analytics Issues



Issues in the last 60 days (grouped daily) [View in Issue Navigator](#)

- Created issues (123)
- Resolved issues (125)

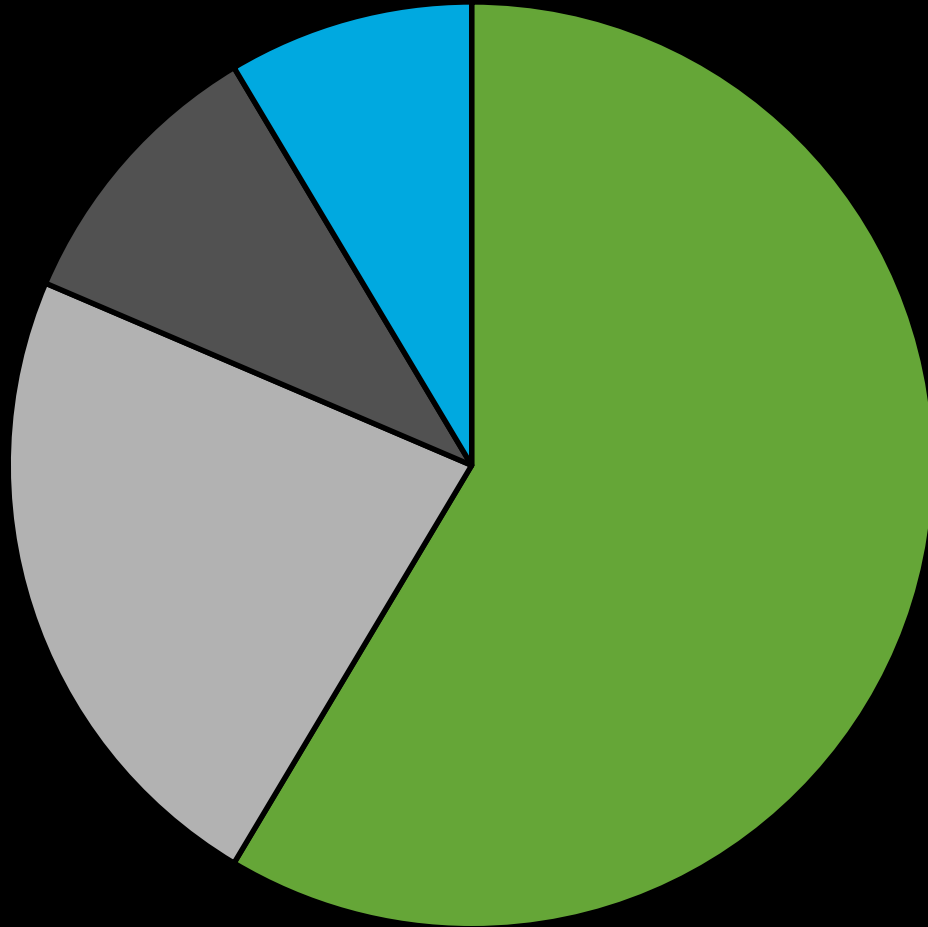
130.60.4 - - [07/Jun 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15L9FF1ADFF3 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FL-5W-03" Moz/1.12.0
 128.241.220.82 - - [07/Jun 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D15L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&item_id=EST-6&JSESSIONID=5D15L9FF1ADFF3 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-6&product_id=FL-5W-03" Moz/1.12.0
 317.27.160.0 - - [07/Jun 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D15L9FF1ADFF3 HTTP 1.1" 468 125.17.14. - - [07/Jun 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-5W-03" Moz/1.12.0
 130.60.4 - - [07/Jun 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-5W-03" Moz/1.12.0
 128.241.220.82 - - [07/Jun 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D15L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&item_id=EST-6&JSESSIONID=5D15L9FF1ADFF3 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-6&product_id=FL-5W-03" Moz/1.12.0
 317.27.160.0 - - [07/Jun 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D15L9FF1ADFF3 HTTP 1.1" 468 125.17.14. - - [07/Jun 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-5W-03" Moz/1.12.0

What can you do in the next 12 months?

- ▶ Identify the key metadata in your currently deployed use-cases
- ▶ Listen to your dev team. Examine your current dev process and improve on the challenges identified by your team
- ▶ When building your process, work towards a minimum viable product (MVP)

```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=5D15L9FF1ADFF3 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?product_id=FL-DSH-01&SESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=KQ-CB-01"
ows NT 27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&SESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&SESSIONID=5D55L9FF1ADFF3"
:/buttercup-16&product_id=RP-LI-02" 468 125.17.14.189] "GET /category.screen?category_id=FLOWERS&SESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-14"
action=purchase&itemId=EST-16&product_id=RP-LI-02" 468 125.17.14.189] "GET /category.screen?category_id=FLOWERS&SESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-14"
```

96%





Do or do not, there is no try.

- Abraham Lincoln



Links!

▶ KP Career Site

- <https://www.kaiserpermanentejobs.org/>

▶ Scrum Alliance

- <https://www.scrumalliance.org/>

▶ Great Video on Thought Leadership

- https://www.youtube.com/watch?v=_ZBKX-6Gz6A&sns=em

▶ Splunk App for Jira

- <https://splunkbase.splunk.com/app/1438/>

▶ JIRA and Confluence Info

- <https://www.atlassian.com/>

Questions?

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=F1-5W-03"
 128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268product_id=K9-CW-01"
 317.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D5L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D55L7FF6ADFF0"
 ://buttercup-shopping.com/oldlink?item_id=EST-26&JSESSIONID=5D5L9FF1ADFF3 HTTP 1.1" 468 125.17 14.1.1.189] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L7FF6ADFF0 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-14"
 ://buttercup-shopping.com/oldlink?item_id=EST-26&JSESSIONID=5D5L9FF1ADFF3 HTTP 1.1" 468 125.17 14.1.1.189] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L7FF6ADFF0 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-14"
 ://buttercup-shopping.com/oldlink?item_id=EST-26&JSESSIONID=5D5L9FF1ADFF3 HTTP 1.1" 468 125.17 14.1.1.189] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L7FF6ADFF0 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-14"