© 2017 SPLUNK INC.

splunk> .conf2017

# 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

8/12/2017 | ver 5.2.2

© 2017 SPLUNK INC.

# Our Purpose

- Share our lessons learned in consolidating artifacts of our migration from a previous SIEM to our current SIEM/logging solution
- Describe the process our team developed to manage our security use-case and content development efforts
- Provide you some answers to a few familiar questions

© 2017 SPLUNK INC.

# 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?

splunk> .conf2017

© 2017 SPLUNK INC.

# Who are you guys?

**Matt Parks**

**Manager, Security Analytics, Cyber Risk Defense Center**


- Matthew.Parks@kp.org
- linkedin.com/in/matthewparks

splunk> .conf2017

© 2017 SPLUNK INC.

# Who are you guys?

**Ruperto Razon**

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

- Ruperto.S.Razon@kp.org
- linkedin.com/in/PertoRazon
- @thatperto

splunk> .conf2017

© 2017 SPLUNK INC.

# KAISER PERMANENTE®

FAST FACTS

**11.8 M**
Members

AS OF MARCH 2017

**21,275**
Physicians

AS OF DECEMBER 2016

**54,072**
Nurses

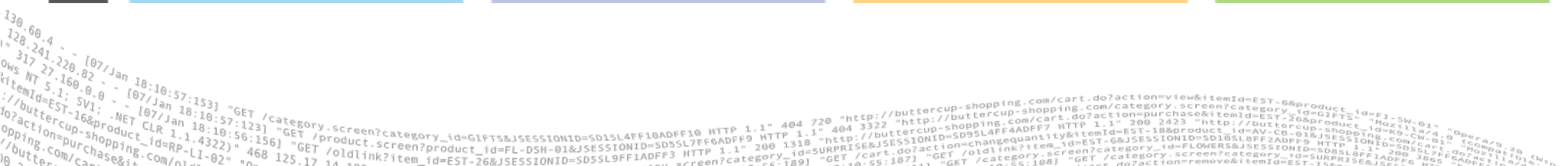
AS OF DECEMBER 2016

**201,776**
Employees

AS OF MARCH 2017

**711**
Hospitals, medical offices

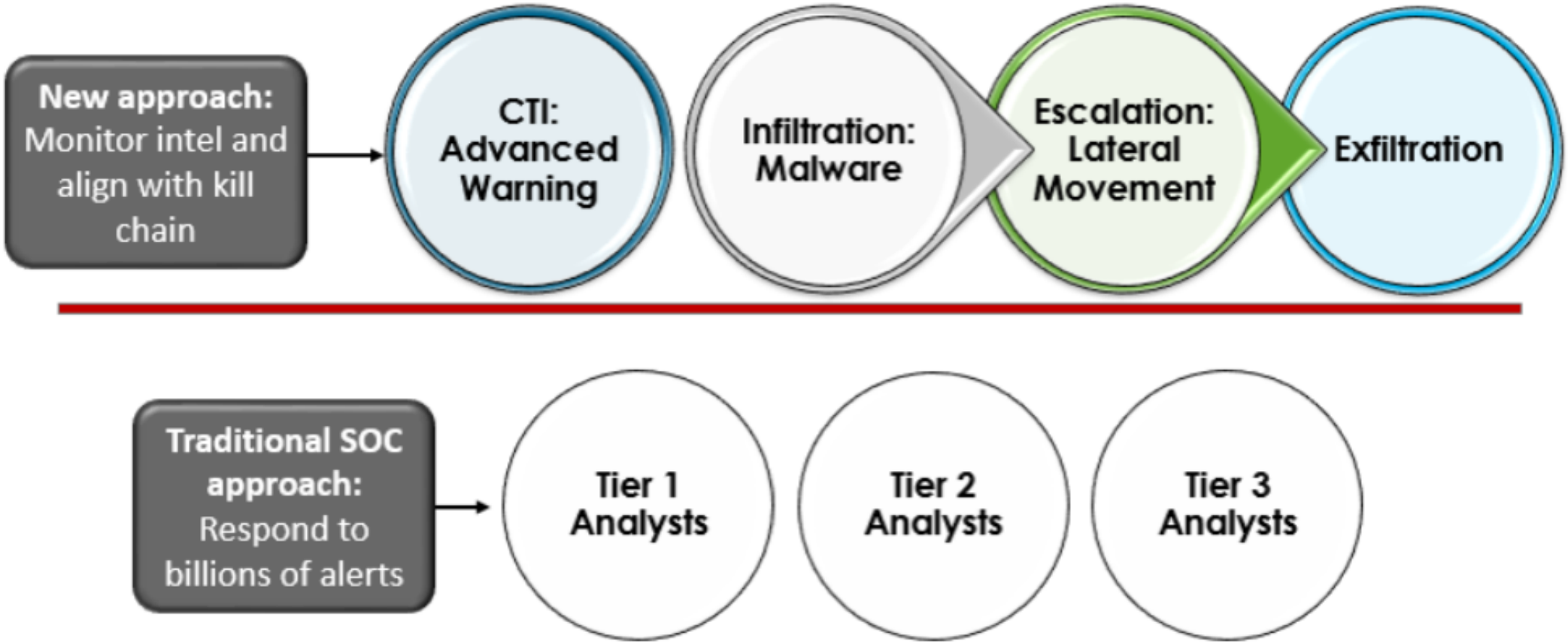
AS OF MARCH 2017



splunk> .conf2017

© 2017 SPLUNK INC.

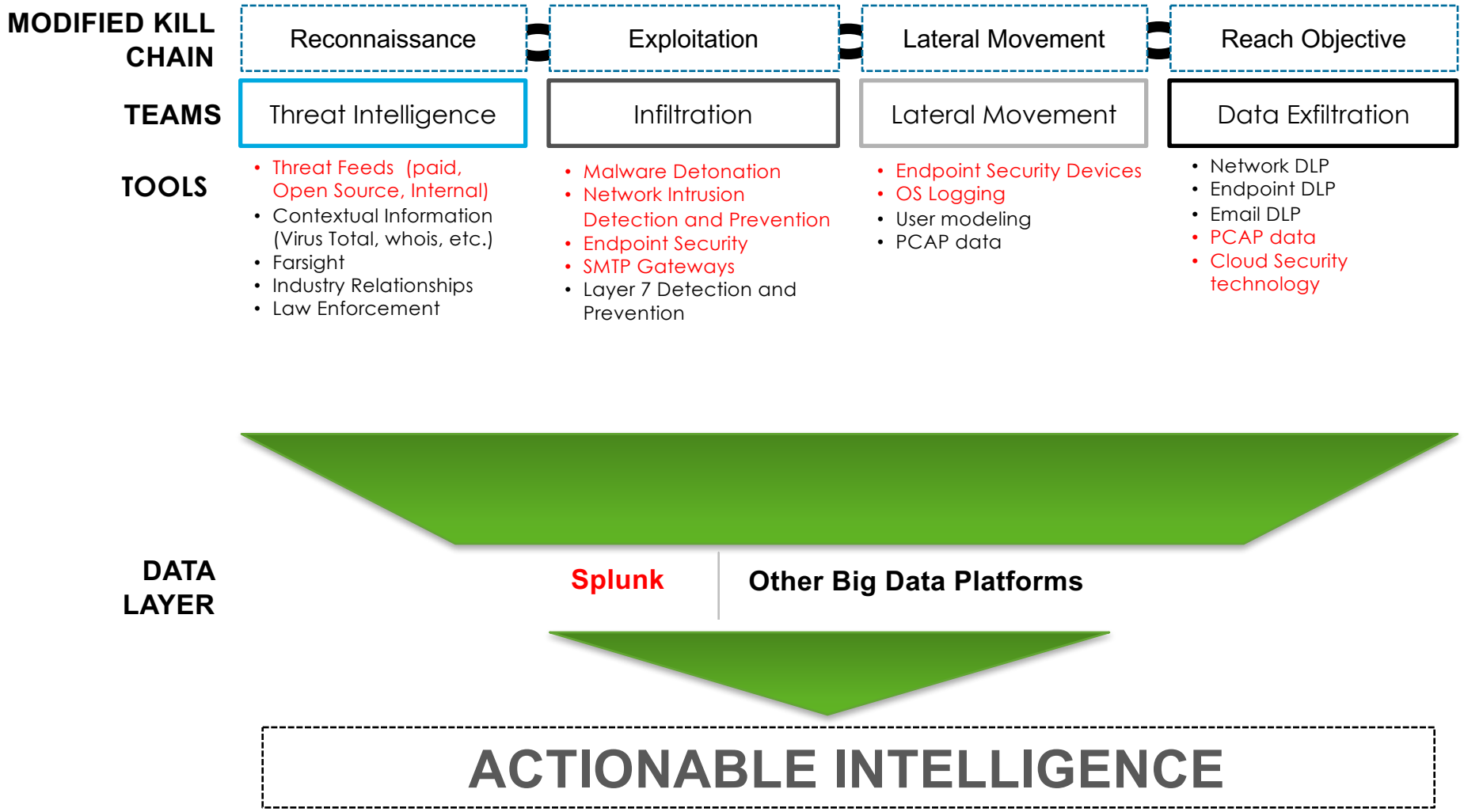
# Cyber Risk Defense Center (CRDC)




splunk> .conf2017

© 2017 SPLUNK INC.

# Advanced and Actionable Intelligence




splunk> .conf2017

© 2017 SPLUNK INC.

# Let's start from the middle….

## Pre-Migration (Summer 2015)

- 2TB+ data/day
- 128 Threat Use-Cases
- 60 Scheduled Reports
- 652 "Knowledge Objects"
- 15+ Documentation Repositories

## Migration Complete (Spring 2016)

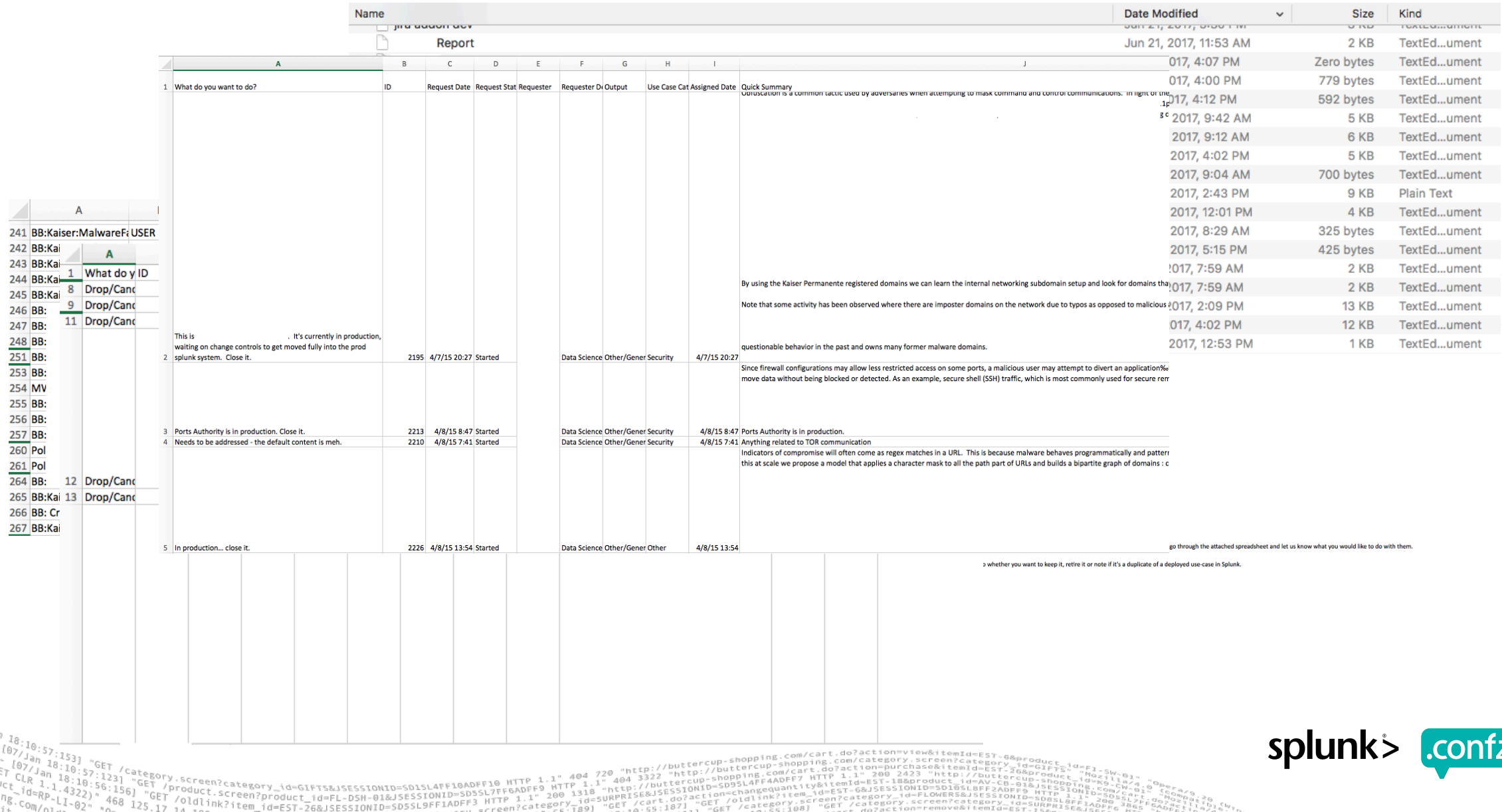
- 4TB+ data/day
- 43 Threat Use-Cases
- 33 Scheduled Reports
- 121 Knowledge Objects
- 4 Documentation Repositories

© 2017 SPLUNK INC.

# Where We Are Today

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

© 2017 SPLUNK INC.



Name | Date Modified | Size | Kind

Report — Jun 21, 2017, 11:53 AM — 2 KB — TextEd...ument

| | A | B | C | D | E | F | G | H | I | J |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | What do you want to do? | ID | Request Date | Request Stat | Requester | Requester D | Output | Use Case Cat | Assigned Date | Quick Summary |
| 2 | This is . It's currently in production, waiting on change controls to get moved fully into the prod splunk system. Close it. | 2195 | 4/7/15 20:27 | Started | | Data Science | Other/Gener | Security | 4/7/15 20:27 | questionable behavior in the past and owns many former malware domains. |
| 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 | Ports Authority is in production. |
| 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 | Anything related to TOR communication |
| 5 | In production... close it. | 2226 | 4/8/15 13:54 | Started | | Data Science | Other/Gener | Other | 4/8/15 13:54 | |

017, 4:07 PM — Zero bytes — TextEd...ument
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

Obfuscation is a common tactic used by adversaries when attempting to mask command and control communications. In light of the

By using the Kaiser Permanente registered domains we can learn the internal networking subdomain setup and look for domains tha

Note that some activity has been observed where there are imposter domains on the network due to typos as opposed to malicious

Since firewall configurations may allow less restricted access on some ports, a malicious user may attempt to divert an application%e move data without being blocked or detected. As an example, secure shell (SSH) traffic, which is most commonly used for secure rem

Indicators of compromise will often come as regex matches in a URL. This is because malware behaves programmatically and patter this at scale we propose a model that applies a character mask to all the path part of URLs and builds a bipartite graph of domains : c

go through the attached spreadsheet and let us know what you would like to do with them.

o whether you want to keep it, retire it or note if it's a duplicate of a deployed use-case in Splunk.

| | A |
|---|---|
| 241 | BB:Kaiser:MalwareFa USER |
| 242 | BB:Kai |
| 243 | BB:Kai |
| 244 | BB:Kai |
| 245 | BB:Kai |
| 246 | BB: |
| 247 | BB: |
| 248 | BB: |
| 251 | BB: |
| 253 | BB: |
| 254 | MV |
| 255 | BB: |
| 256 | BB: |
| 257 | BB: |
| 260 | Pol |
| 261 | Pol |
| 264 | BB: |
| 265 | BB:Kai |
| 266 | BB: Cr |
| 267 | BB:Kai |

| | A |
|---|---|
| 1 | What do y ID |
| 8 | Drop/Canc |
| 9 | Drop/Canc |
| 11 | Drop/Canc |
| 12 | Drop/Canc |
| 13 | Drop/Canc |

splunk> .conf2017

© 2017 SPLUNK INC.

# Artifacts of Note

- Naming conventions
- Search logic
- Knowledge objects
- Scheduling of searches/reports
- Asset Categories
- Recipients/Users
- Original Requestor
- Tribal Knowledge

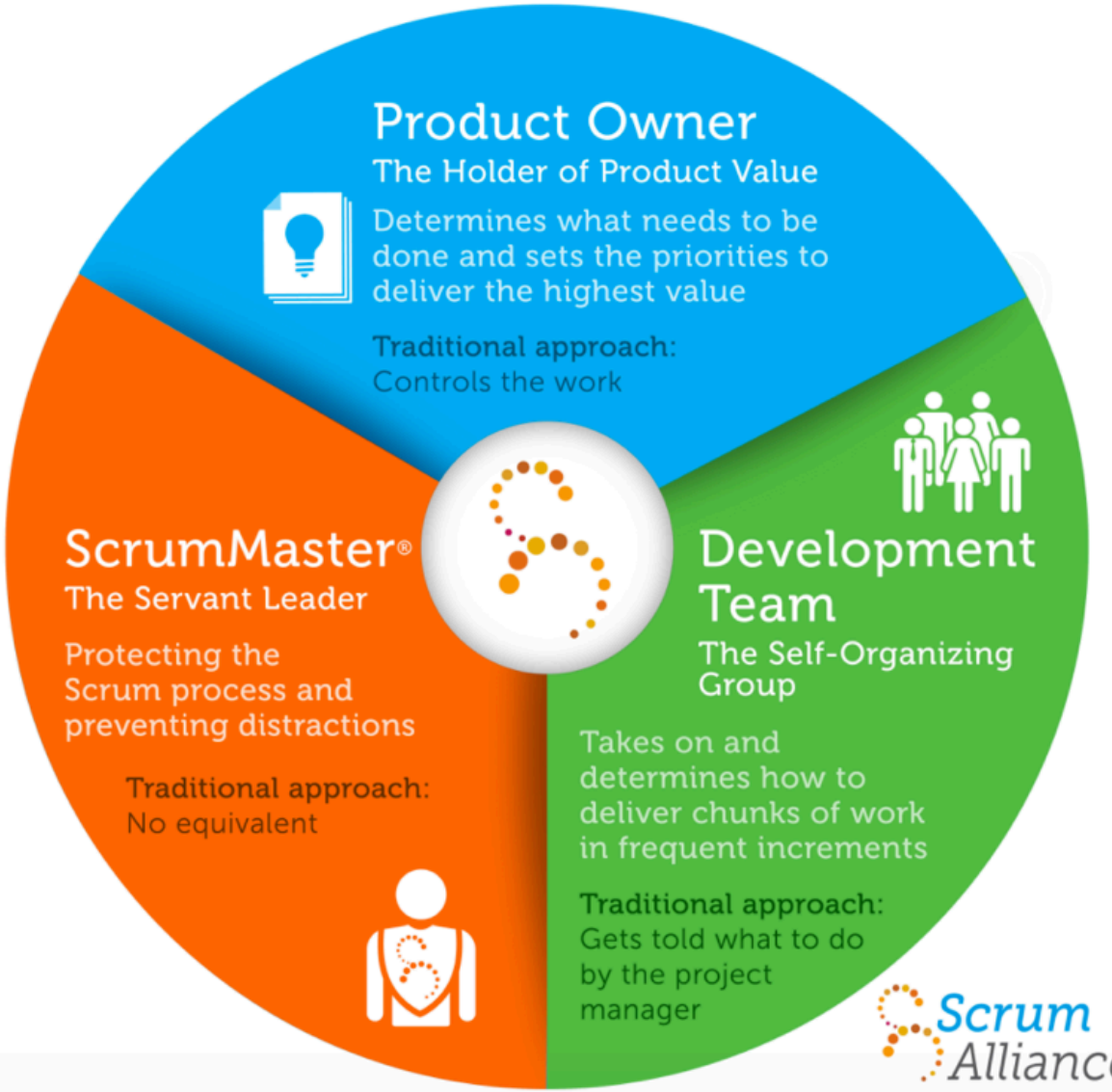
© 2017 SPLUNK INC.

# 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.

© 2017 SPLUNK INC.

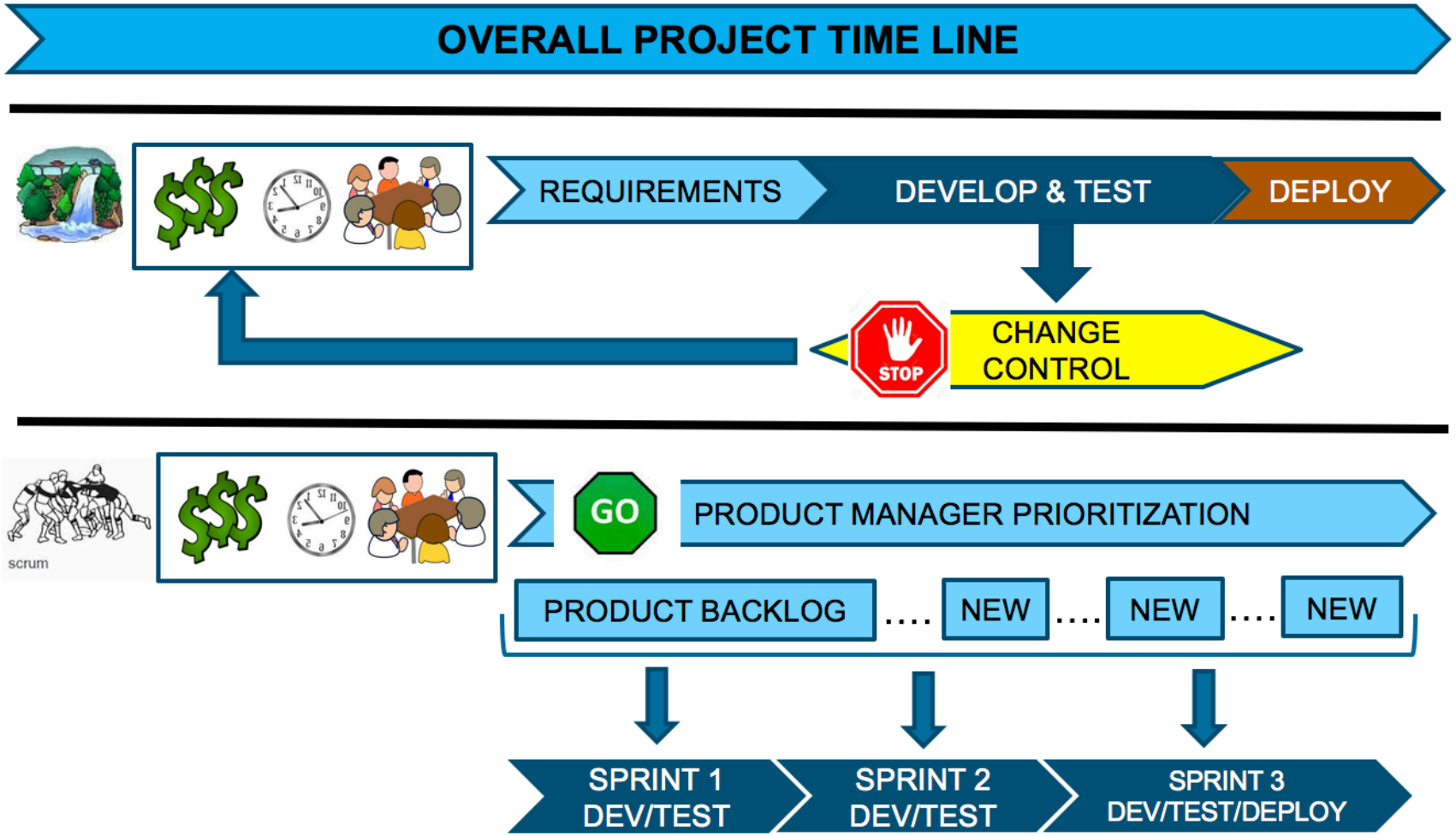
# What does a Scrum look like?




splunk> .conf2017

© 2017 SPLUNK INC.

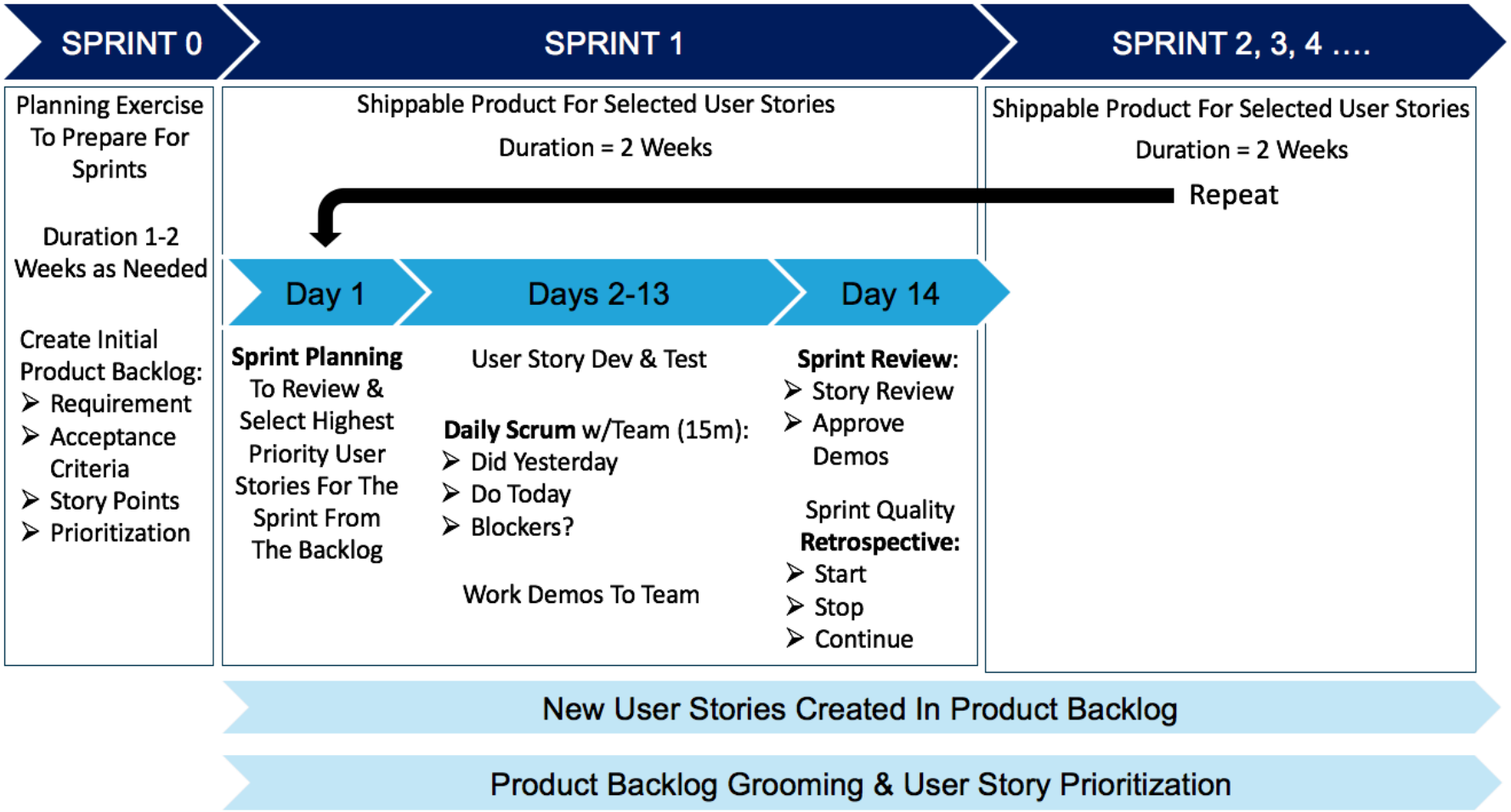
# The Scrum Advantage




splunk> .conf2017

© 2017 SPLUNK INC.

# Scrum Framework Process




splunk> .conf2017

© 2017 SPLUNK INC.

# Example Story

Summary* MW ·Attacking IP High Data Rate Outbound

Issue Type* Story

Reporter*

Start typing to get a list of possible matches.

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

Start typing to get a list of possible matches or press down to select.

Priority ↑ Medium

Attachment Drop files to attach, or browse.

Linked Issues relates to

Issue

Begin typing to search for issues to link. If you leave it blank, no link will be made.

Assignee Matt Parks

Assign to me

Epic Link Security Analytics Operations

Choose an epic to assign this issue to.

Sprint

JIRA Software sprint field

Completed sprints **Use Case Content Sprint 9**

Story Points 13

Measurement of complexity and/or size of a requirement.

CRDC Tag MW × SA × es ×

Use the "CRDC Tag" field as a replacement for the default "Label" field. CRDC Tag uses the Label Manager Plugin.

Actual Work 13

TL; DR Alert for attackers with high volume outbound

Short summary of what was actually done - keep to 30 words or less.

splunk> .conf2017

© 2017 SPLUNK INC.

# So what do we do with all this JIRA Data?

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

© 2017 SPLUNK INC.

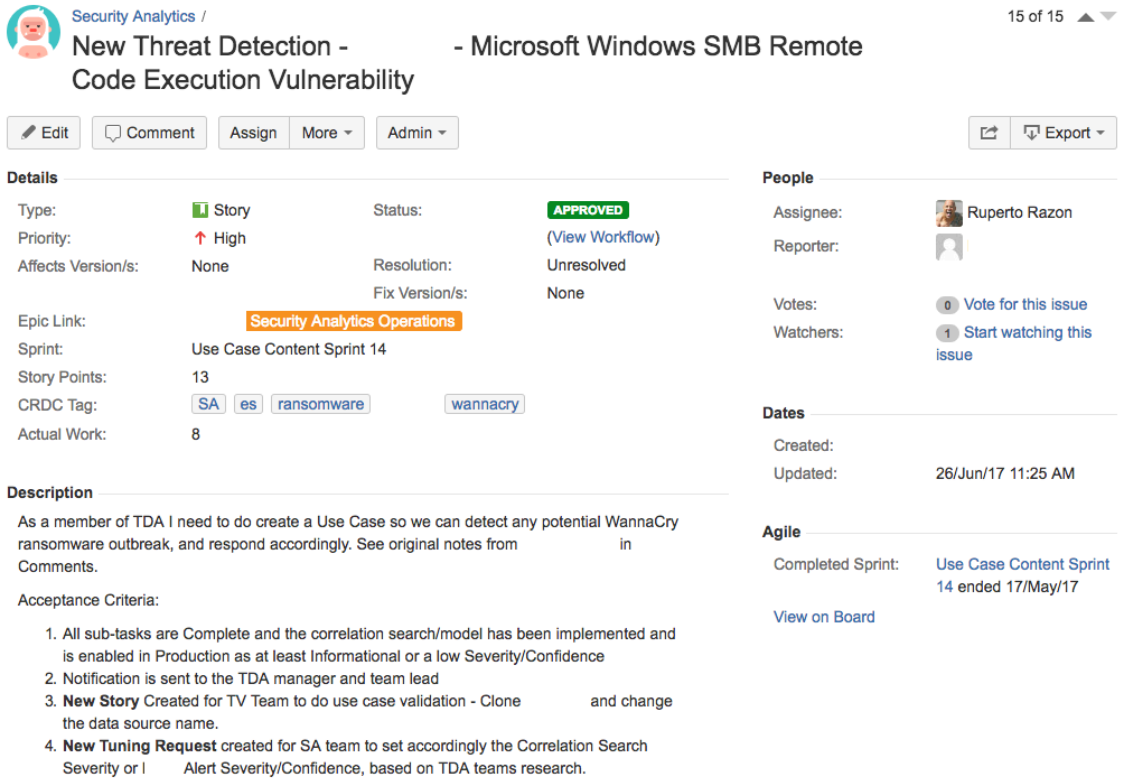
# Bob in accounting was infected by <insert-threat-of-the-day-here>, who else was infected?

splunk> .conf2017

© 2017 SPLUNK INC.

# 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 - - Microsoft Windows SMB Remote Code Execution Vulnerability

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: 0 Vote for this issue

Watchers: 1 Start watching this issue

**Dates**

Created:

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 in 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 and change the data source name.
4. **New Tuning Request** created for SA team to set accordingly the Correlation Search Severity or l Alert Severity/Confidence, based on TDA teams research.

splunk> .conf2017

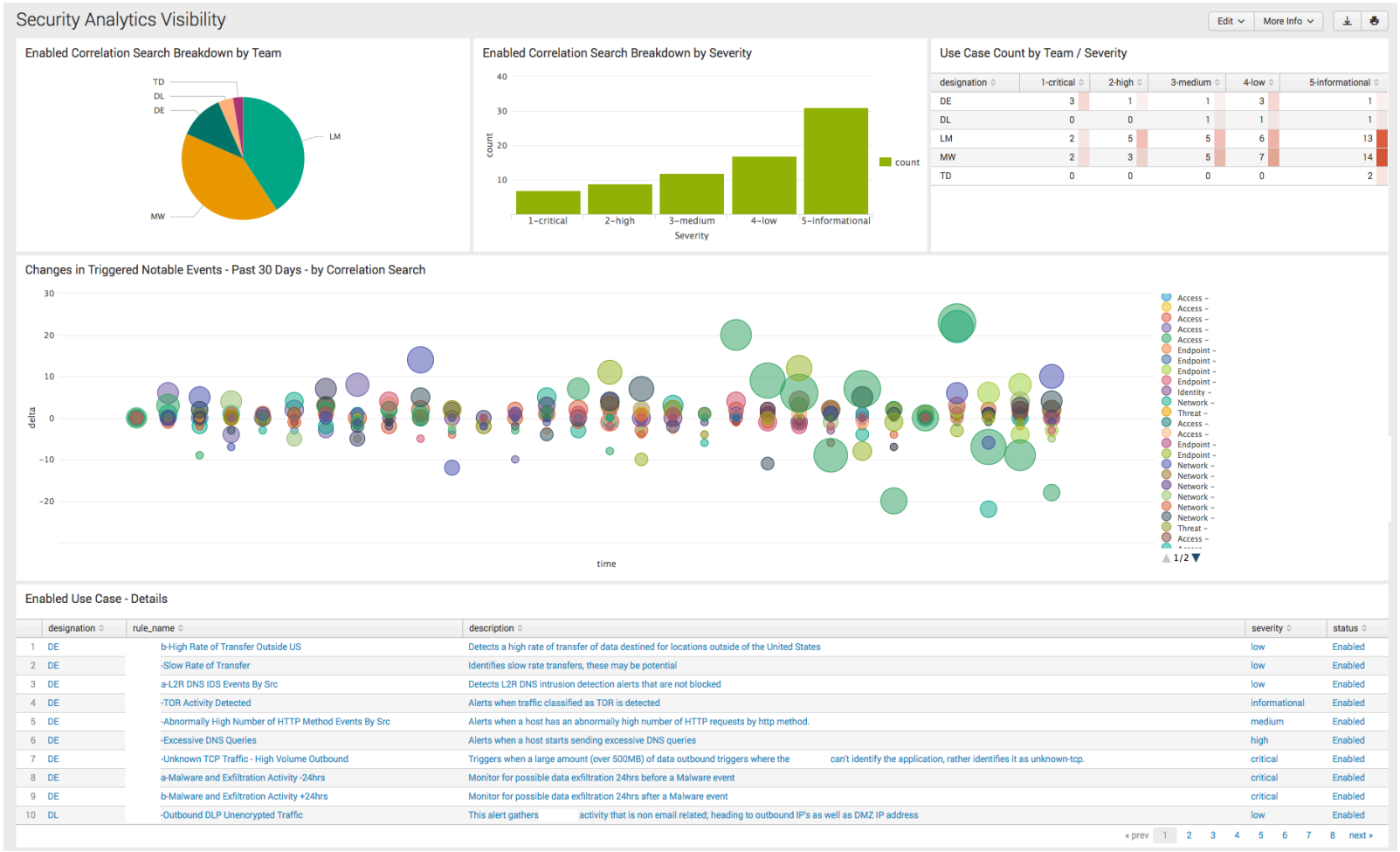
© 2017 SPLUNK INC.

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

splunk> .conf2017

© 2017 SPLUNK INC.

# Deployed Use-Case Visibility




splunk> .conf2017

© 2017 SPLUNK INC.

# 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

splunk> .conf2017

© 2017 SPLUNK INC.

# 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

splunk> .conf2017

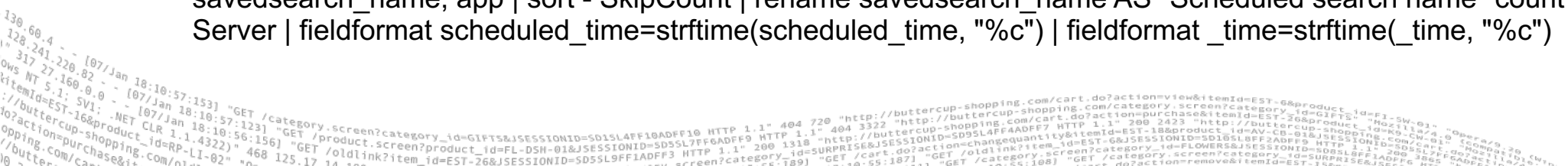
© 2017 SPLUNK INC.

# 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")



splunk> .conf2017

© 2017 SPLUNK INC.

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

splunk> .conf2017

© 2017 SPLUNK INC.

# Status Metricization

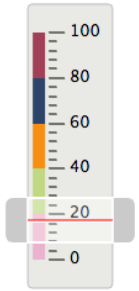
Used to show completeness of status regardless of velocity in a given Scrum related to Epic that have heretofore been unaccomplished but are tied to the current Sprint.

Edit | More Info

### Percent Completometer

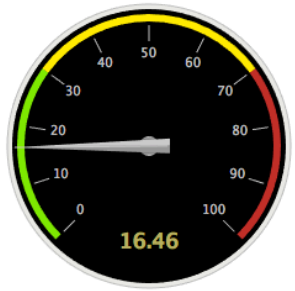
12.17 %

### Truthiness

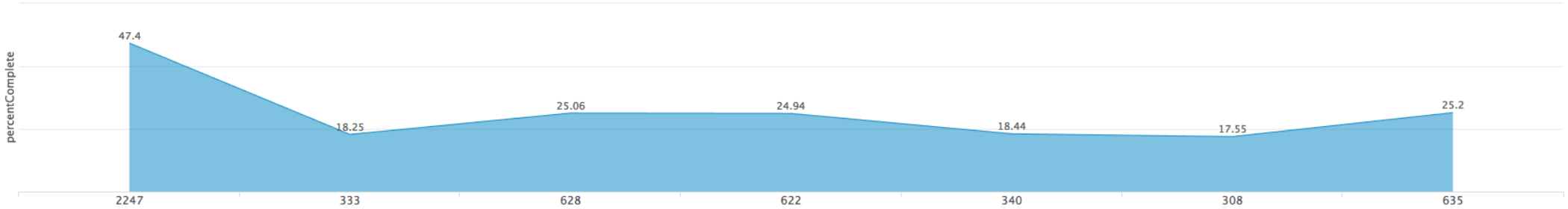



### Number of


### 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

splunk> .conf2017

© 2017 SPLUNK INC.

# 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
- CompleteTruthiness
  - 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"

splunk> .conf2017

© 2017 SPLUNK INC.

# 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

splunk> .conf2017

© 2017 SPLUNK INC.

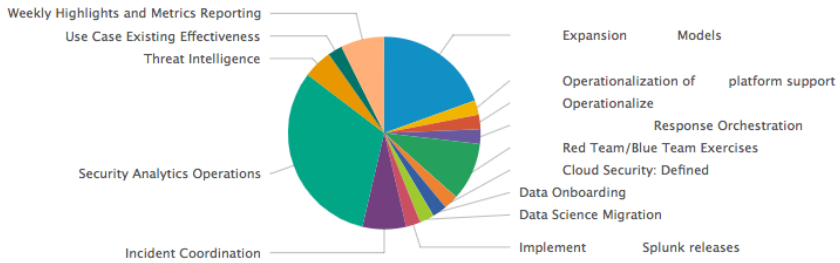
# JIRA Epic Tracking

## Demo JIRA Epic Tracking

demo jira epic tracking

Edit | Export | ...

### Stories Completed By Epic 2017




### Story Summaries by Epic

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

splunk> .conf2017

© 2017 SPLUNK INC.

# 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

splunk> .conf2017

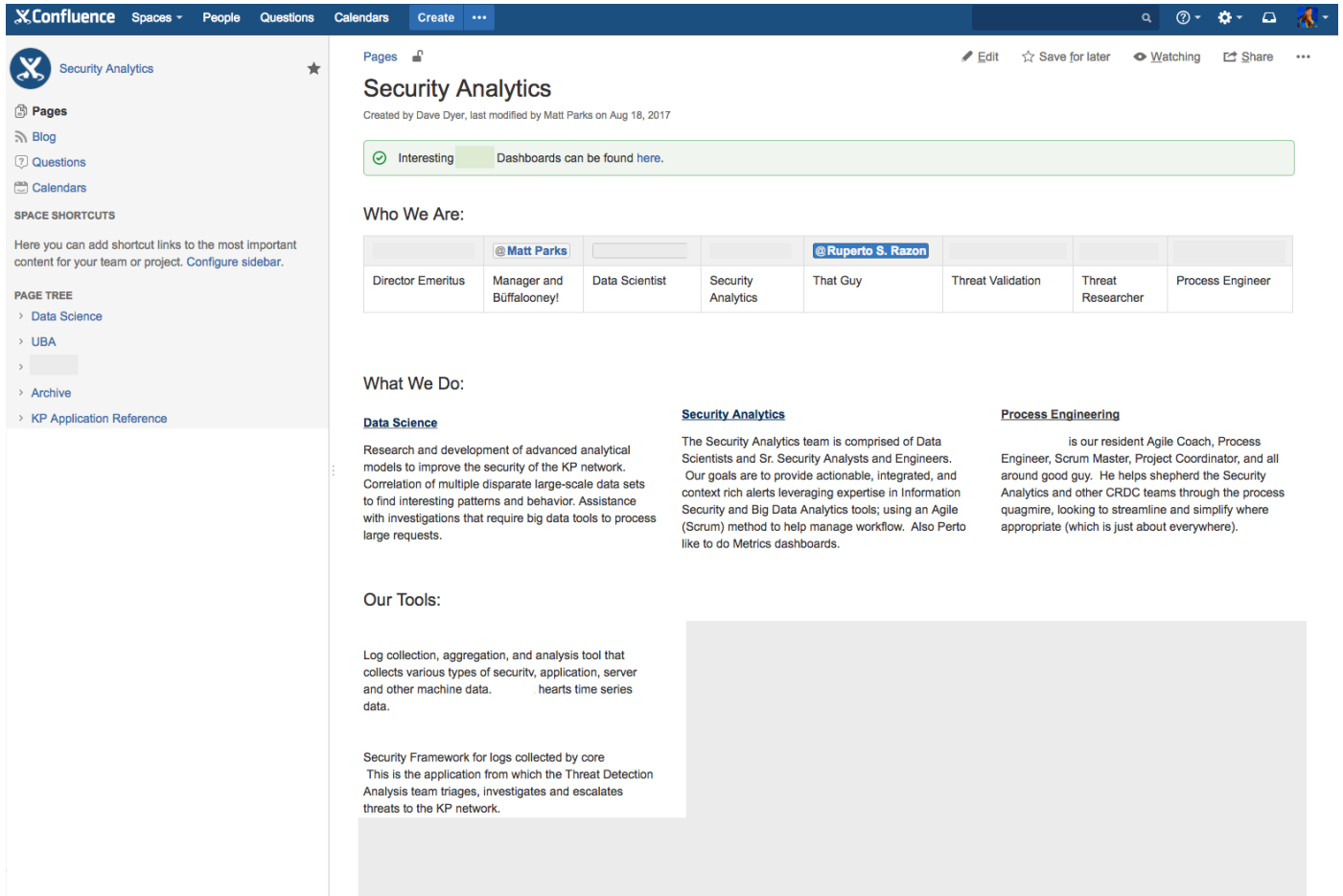
© 2017 SPLUNK INC.

# What does your development team do all day?

splunk> .conf2017

© 2017 SPLUNK INC.

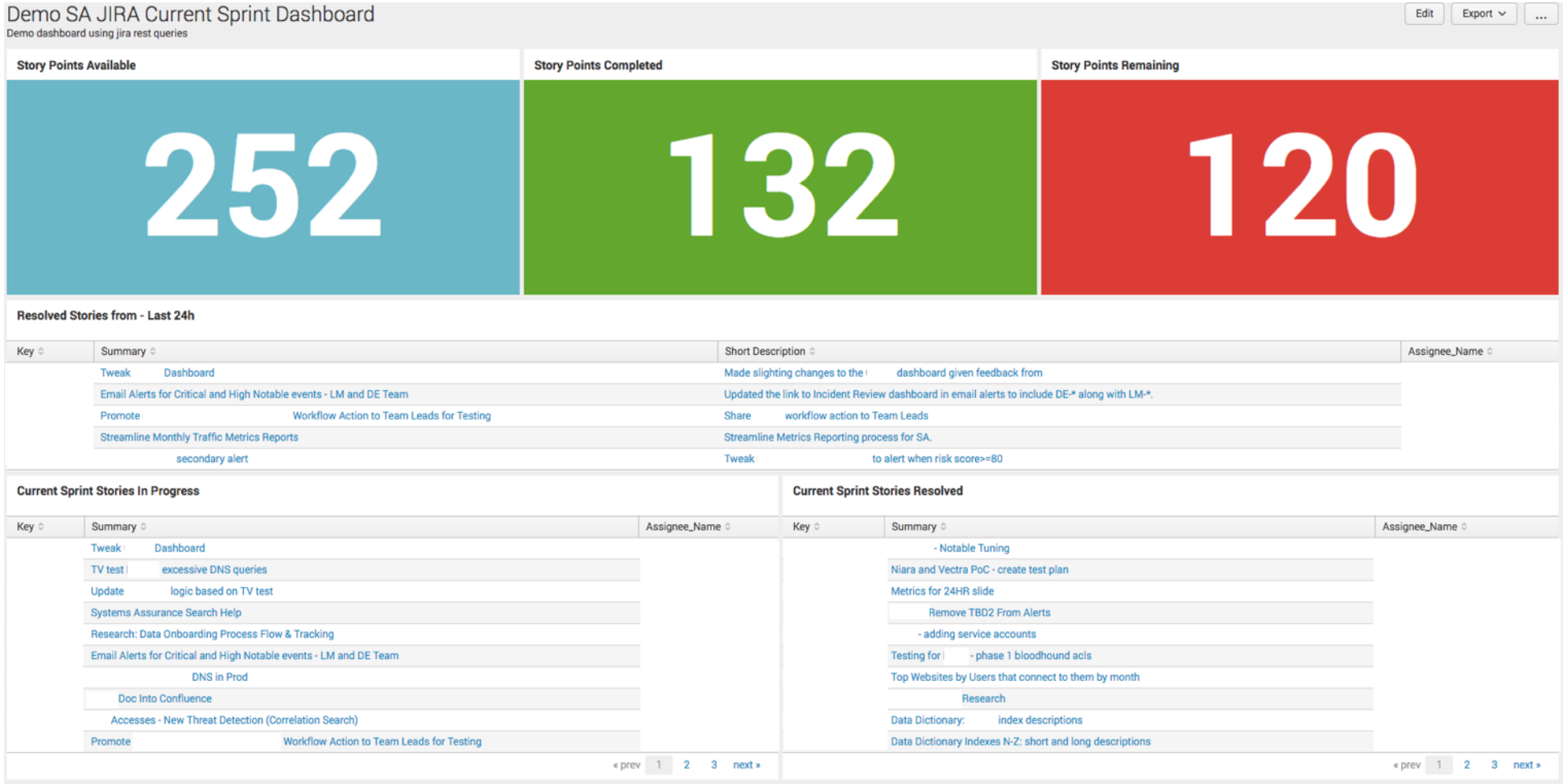
# In General, This Is What We Do…




splunk> .conf2017

© 2017 SPLUNK INC.

# This Is What We're Doing Right Now



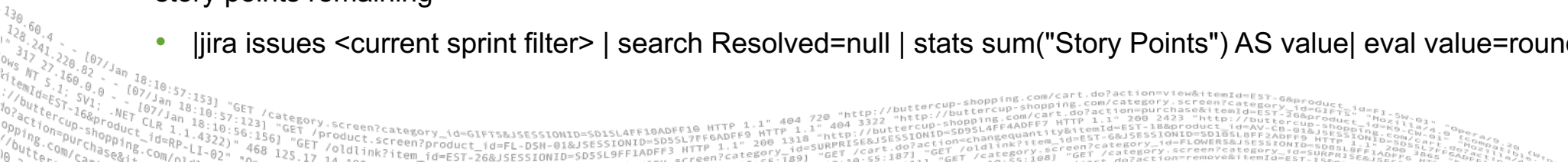

splunk> .conf2017

© 2017 SPLUNK INC.

# 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)



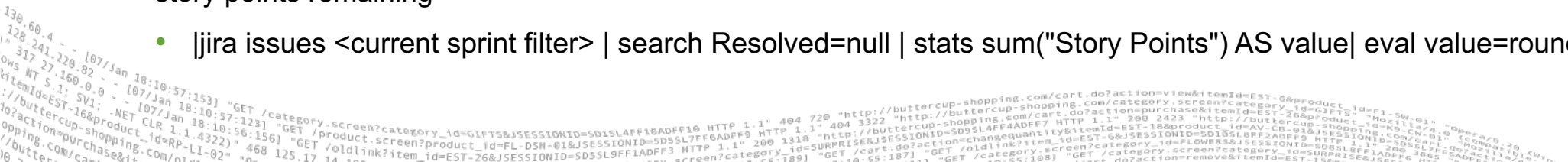
splunk> .conf2017

© 2017 SPLUNK INC.

# 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)



splunk> .conf2017

© 2017 SPLUNK INC.

# 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 |

splunk> .conf2017

© 2017 SPLUNK INC.

# Recap

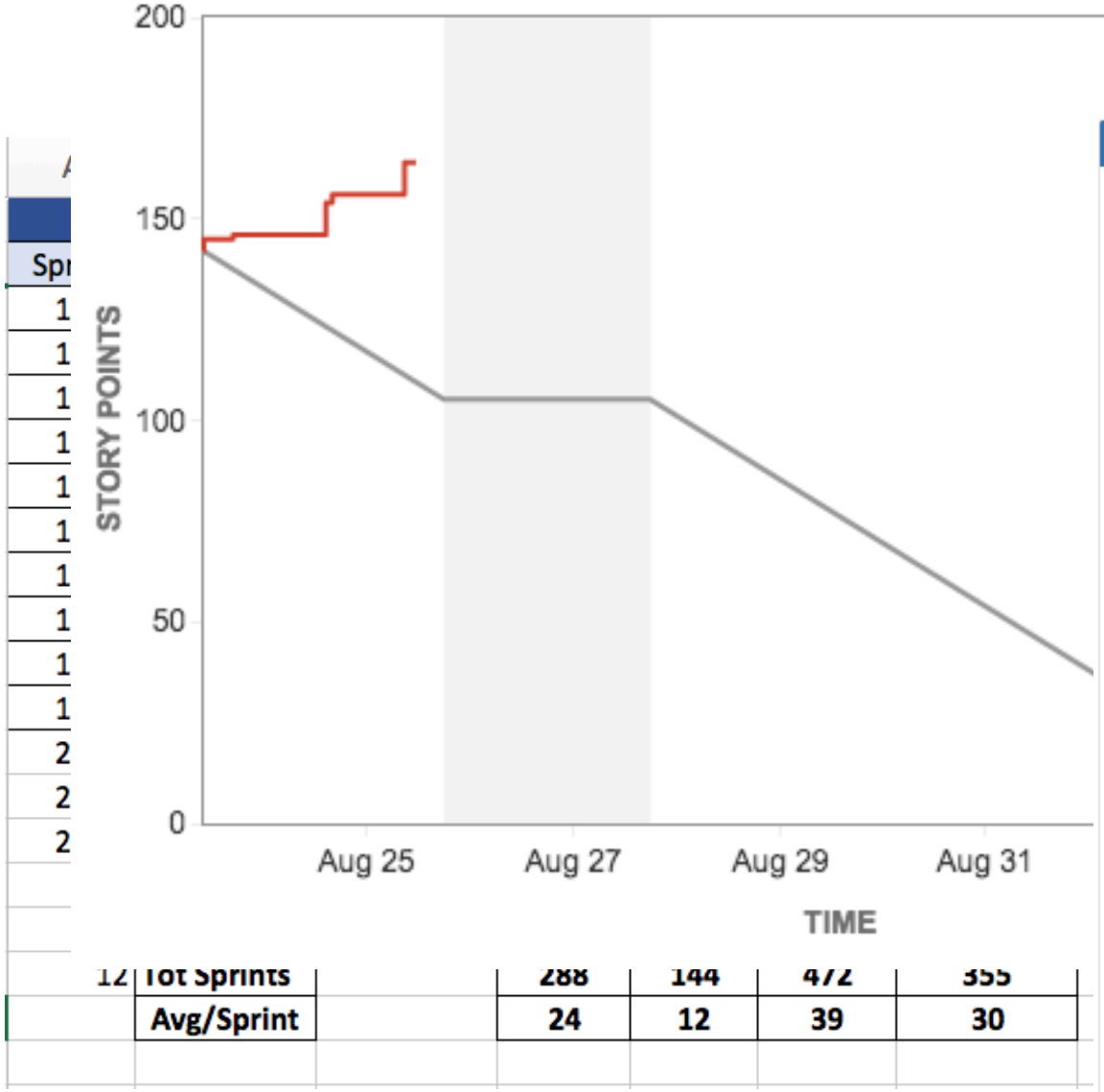
- Gave you tips on how you can build a flexible content development process
- Shared with you a real-world example of how this flexible process works in practice
- Provided you with dashboards and searches that will improve visibility of your security posture, high-level goal tracking and content dev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

© 2017 SPLUNK INC.

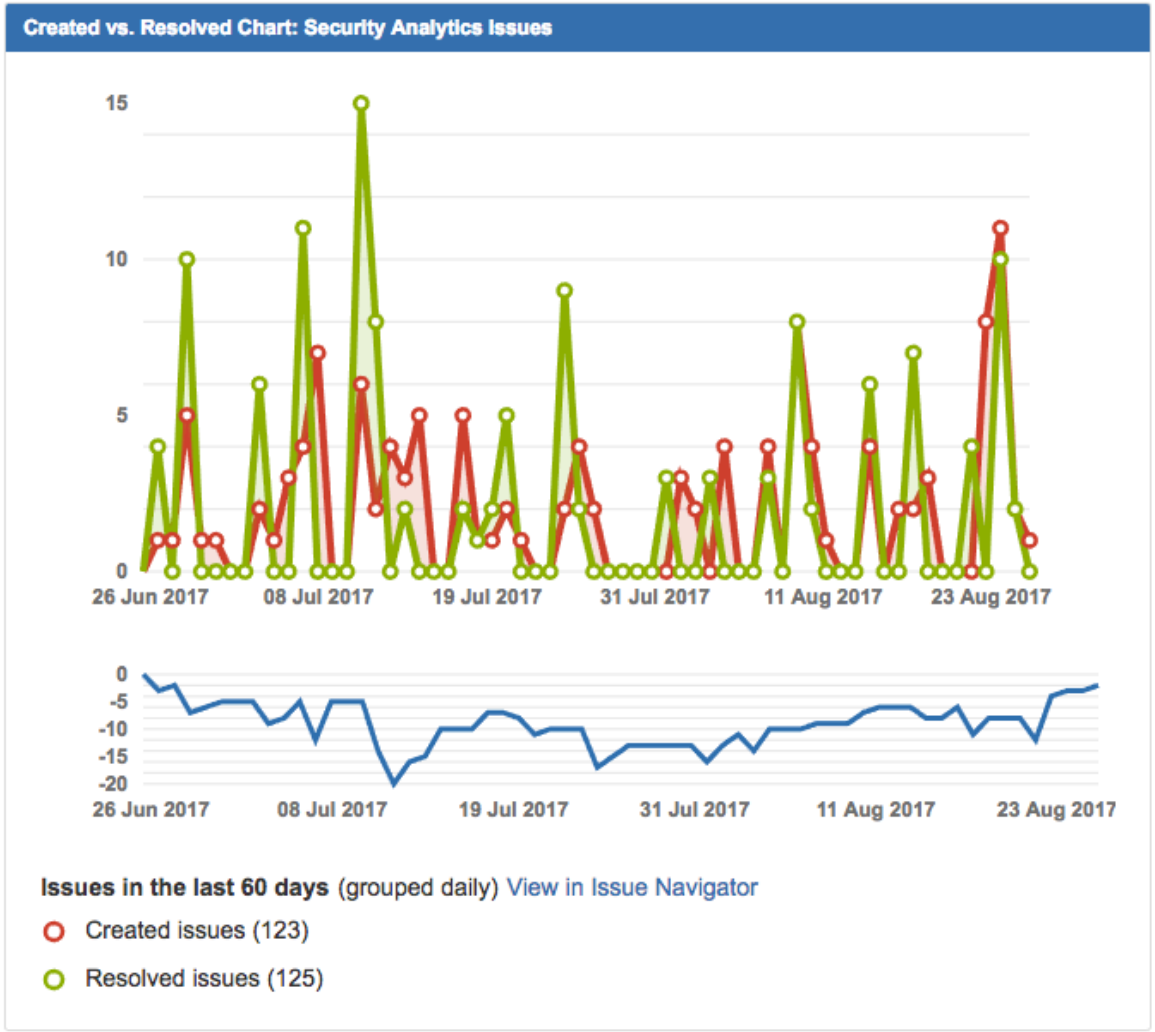
# What will we do in the next 12 months?

splunk> .conf2017

© 2017 SPLUNK INC.




| | | | | | | |
|---|---|---|---|---|---|---|
| 12 | Tot Sprints | | 288 | 144 | 472 | 355 |
| | Avg/Sprint | | 24 | 12 | 39 | 30 |




splunk> .conf2017

© 2017 SPLUNK INC.

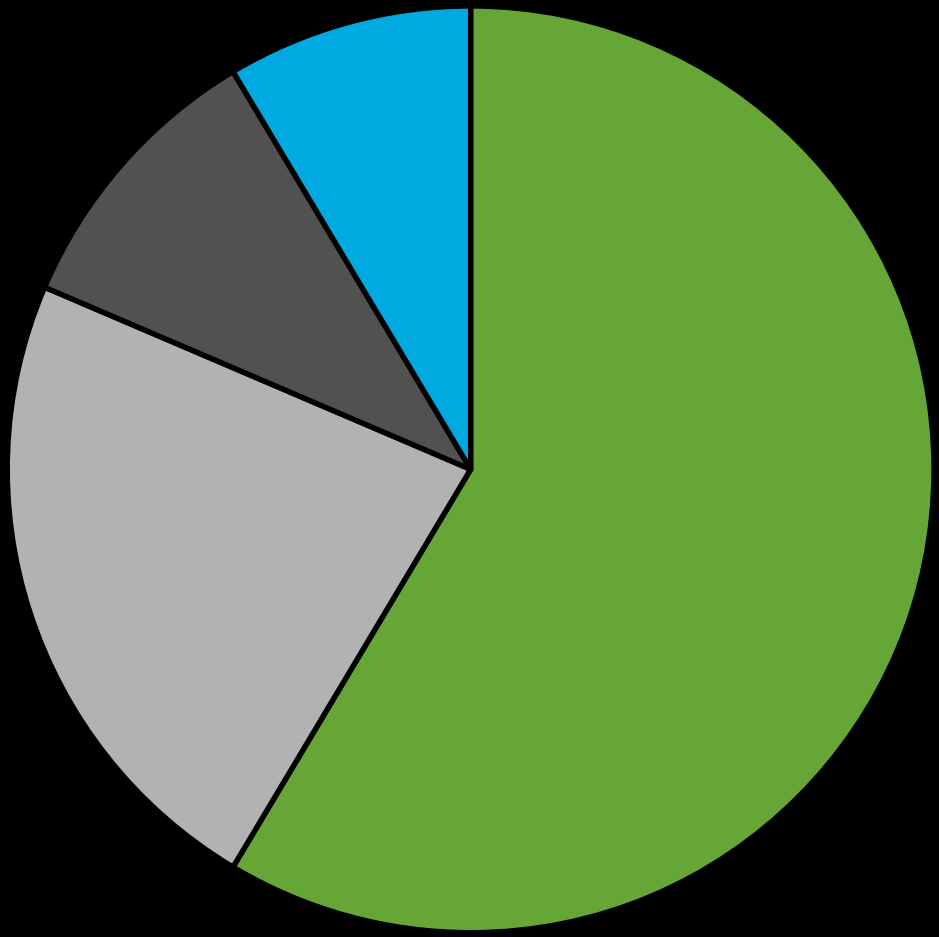
# What can you do in the next 12 months?

- 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)

© 2017 SPLUNK INC.

# 96%

© 2017 SPLUNK INC.



© 2017 SPLUNK INC.

© 2017 SPLUNK INC.

# Do or do not, there is no try.

- Abraham Lincoln

© 2017 SPLUNK INC.

splunk> .conf2017

© 2017 SPLUNK INC.

# 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/

© 2017 SPLUNK INC.

# Questions?

splunk> .conf2017