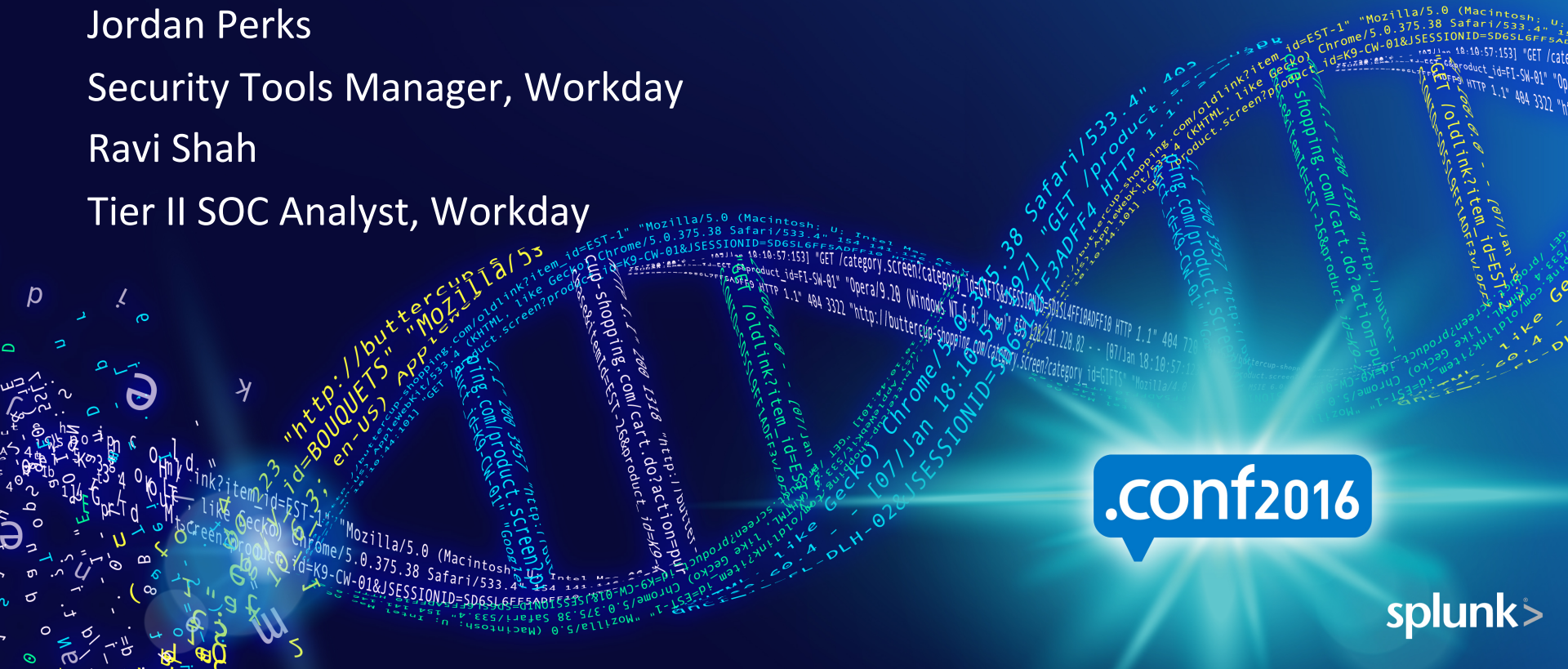
Maturing Workday's SOC With Splunk

Jordan Perks

Security Tools Manager, Workday

Ravi Shah

Tier II SOC Analyst, Workday



.conf2016

splunk>

Disclaimer

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 the 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.

Agenda

- How Workday matured its SOC with Splunk as our ”Tier-0” security tool
- Workday’s Method
  - Process/People
  - Splunk searches and visualizations
  - Documentation
  - Automation

Legacy SIEM

Shallow Skillset
One Engineer
Took over w/ no training

Unstable
History of outages

"Clunky"
Not Customizable

Inflexible
Mostly Firewall

High False Negative/ Positive

A Few Use Cases

Port Scanning	- A rule-set that detects various types of port scanning activity. - Large number of targets (Single Port) - Large number of ports (Single Target)
Suspicious Access Attempts	- Logging into the network from 2+ places faster than one can travel. - Multiple users logging in from the same IP that is not in their known home region.
Malware Suite	A large suite of malware rules. Enables Workday to identify risky users and take immediate action on severe malware.

Risk Based Alerting

Why	- Non-actionable, low-risk behavior - Eliminate high volumes of incidents - Identify patterns of risky behavior
How	- Assign risk score to items such as accessing an IOC or commodity malware that was handled - Alert on a “high” value of risk score assigned
Results	- Enables SOC to identify patters of behavior in a single event rather than be bombarded by thousands of low-value incidents.

How Did We Do It?

Who

- Analysts
- Engineers
- Management
- Data Owners

Process

- Training
  - Engineers > Architect
  - Analysts > Power User
  - Management > Admin
- Feedback Loop
- Documentation
- Customization
  - Low False positive/negative rate
  - Specific to Workday

Results

- Deep Skillset
- Knowing the right questions
- Rapid delivery
- More Secure Workday!

Feedback Loop

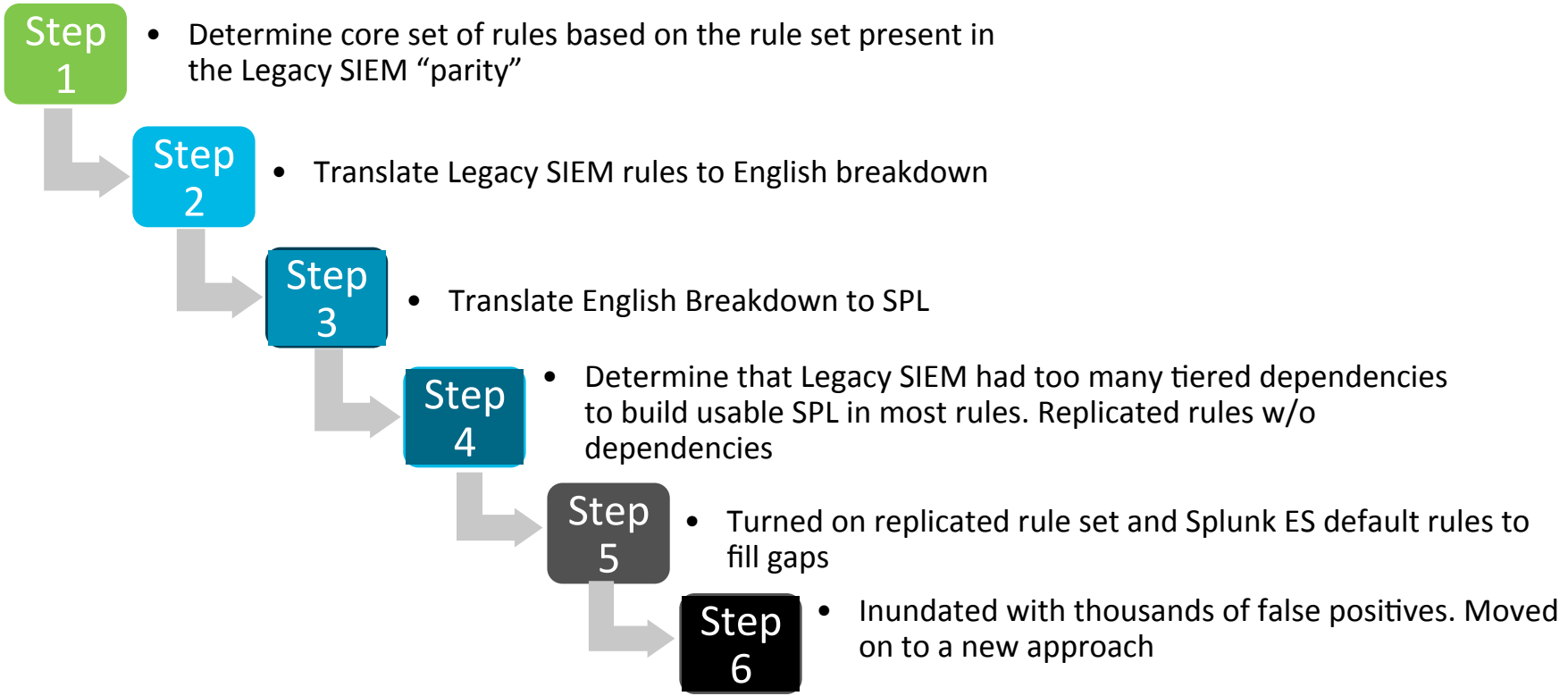
Engineers
Use Case Creation
Rule Development
Gap Analysis
Rule Tuning

Data Owners
Use Case Creation
Provide Content

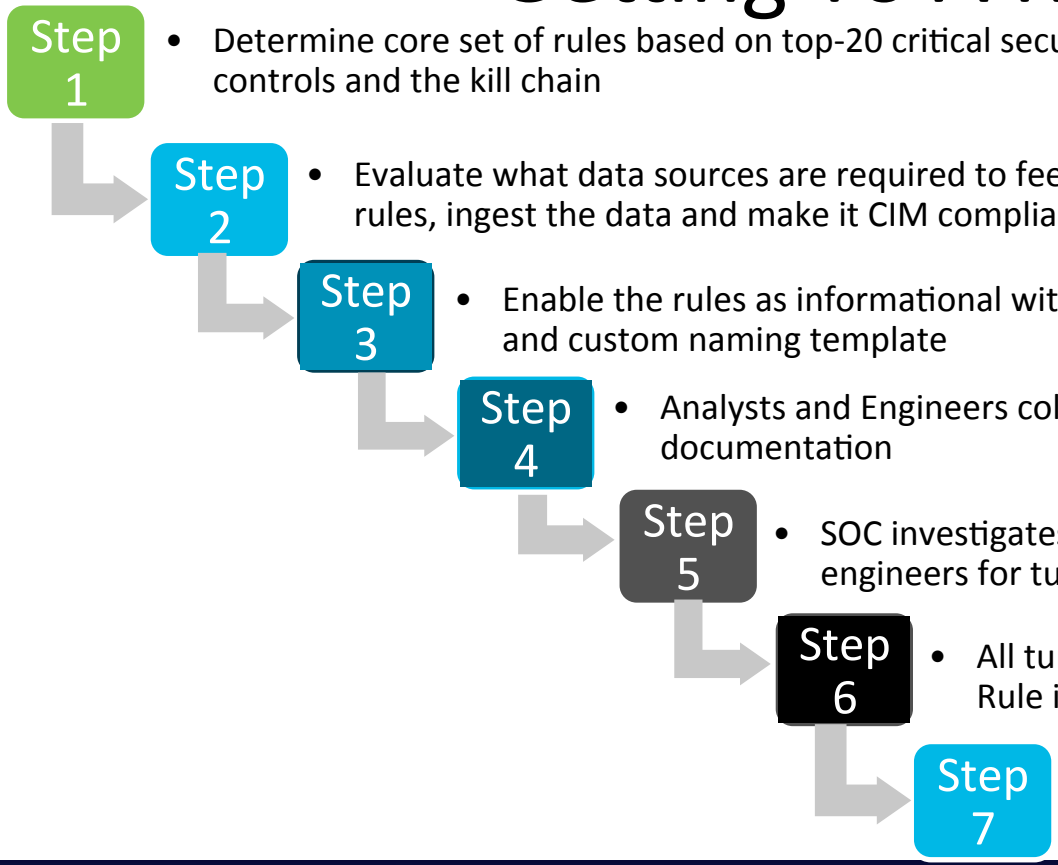
Analysts
Incident Investigation
False Positive/Negative Reporting
Tuning Requests
Use Case Creation
Rule Development (SOC SMEs)

Management
Set Policy
Gap Analysis
Executive Sponsors

First Attempt At A Rule Set



Getting To A Rule Set



Naming The Rules

- 4002-EXP-Host with same recurring malware infection
- 4-002 “4” Indicates it is in the 4th stage of the kill chain
- 4-002 ”002” Indicates it is the 2nd rule written in ”4” category
- “EXP” Indicates it is in the ’Exploit’ category
- Lastly, the name of the rule
- When conversing about a rule, using this 4-digit unique identifier has been very efficient
- It has been a small effort that has made an enormous impact

The SOC Process

- Writing Playbook
- ES Rules Training Sessions
  - What the rule detects and how it works
  - How the drill down works
  - Other Notable Event details (throttling, schedule, time ranges, risk modifiers) and reason for them
  - Walk thru of a True Positive alert (round table)
  - Walk thru of False Positive / non-issue alert
  - Questions/comments about rule or improving the rule

4002-EXP-Host with Same Recurring Malware Infection

Contents [hide]

Rule State	Rule Acceptance
Disabled	**Disabled**

1 Rule Basics

Rule Name	4002-EXP-Host with Same Recurring Malware Infection													
Kill Chain/Category	REC	WEA	DEL	EXP	INS	CAC	DEX	MISC	ACC	END	NET	IDT	THR	HEA
App	SA-EndpointProtection													
Data Feeds	**Indexes**	mcafee_epo												
	Data Models	Malware												

2 Query

Description	Alerts when a host has an infection that has been re-infected remove multiple times over multiple days.	
Search	`| tstats allow_old_summaries=true dc(Malware_Attacks.date) as "day_count",count from datamodel=Malware where nodename=Malware_Attacks by "Malware_Attacks.dest","Malware_Attacks.signature" | rename "Malware_Attacks.dest" as "dest","Malware_Attacks.signature" as "signature" | where 'day_count'>3`	
Query Description	An English breakdown of the query	
Time Range	**Earliest**	-10085m@m
	Latest	-5m@m
Schedule	45 * * * *	

3 Throttling

Throttle?	**TRUE**[Collapse]
Throttling Period	86300s
Throttling Fields	dest,signature

4 Notable Event Details

Create Notable?	**TRUE**				**[Collapse]**
Title	4002-EXP-Host With Same Recurring Malware Infection ($signature$ On $dest$) - WIP				
Description	The device $dest$ was detected with malware '$signature$' that has been detected as active for day_count days in a row. AV has successfully removed the infection each time but the system is continually reinfected; this may indicate the presence of another form of malware is on the system that is prompting the download of '$signature$'.				
Severity	Informational	Low	Medium	High	Critical
Drilldown	`| datamodel Malware Malware_Attacks search | search Malware_Attacks.dest="$dest$" Malware_Attacks.signature="$signature$"`				
Drilldown Time Range	**Earliest**				
	Latest				

5 Risk Modifier

Assign Risk?	**FALSE[Expand]**

6 Workfow/Testing

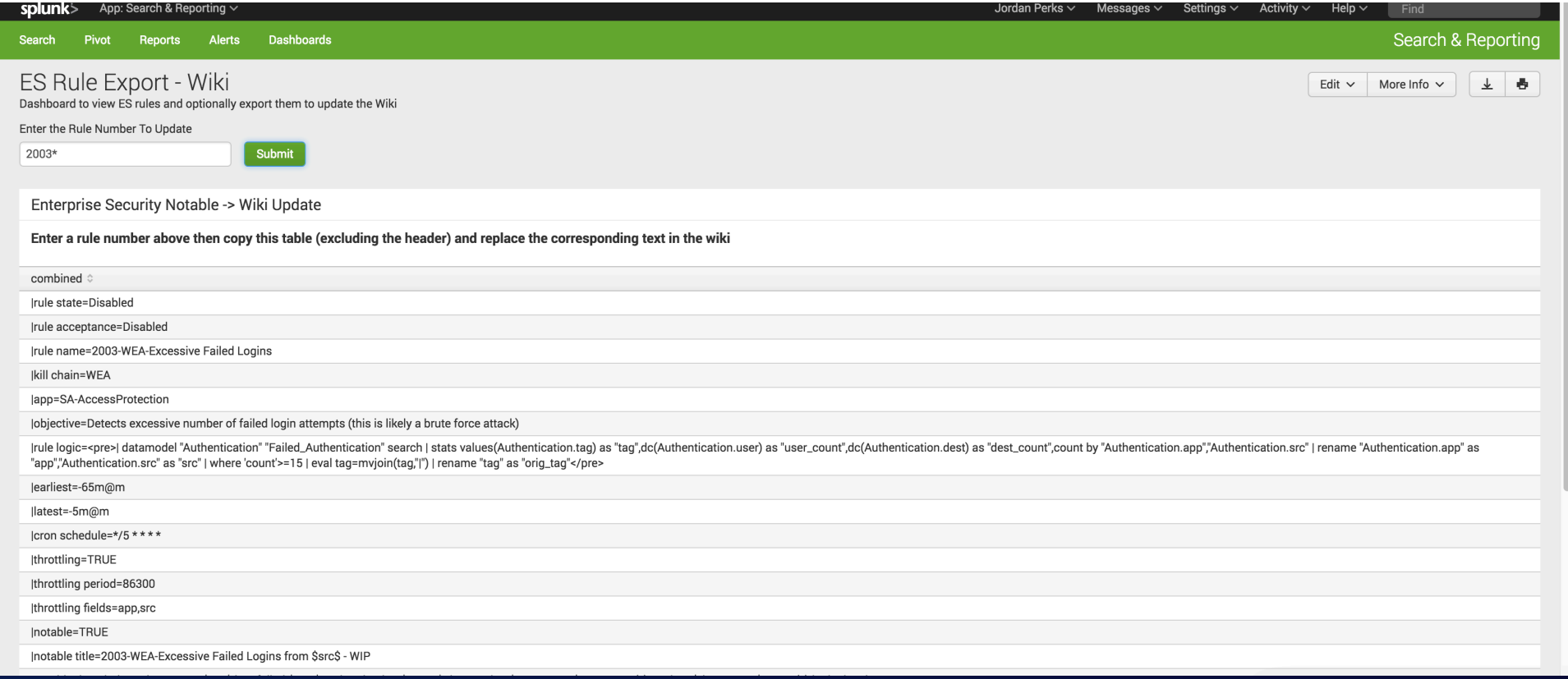
Workflow	• Create a Jira with the following information
	  • Identify the User & User's Risk Value User Risk Determination
	  • Hostname and IP of the affected device(s)
	• Edit the ES notable event by checking the checkbox and clicking "Edit all selected". Change Status to "In Progress", Owner to yourself, and copy the JIRA URL in Comment section.
	• Investigate the severity of the malware Malware Research Wiki
	• Attempt to clean the infection with EPO
	  • If cleaning is unsuccessful, create ServiceNow ticket for IT to nuke the workstation. Depending on the threat, this may not be always the case.
	• Once all followup is complete, close the JIRA and ES notable alert.

Testing Procedure	*Download EICAR on any single machine that has EPO installed every day for three days in a one week span.

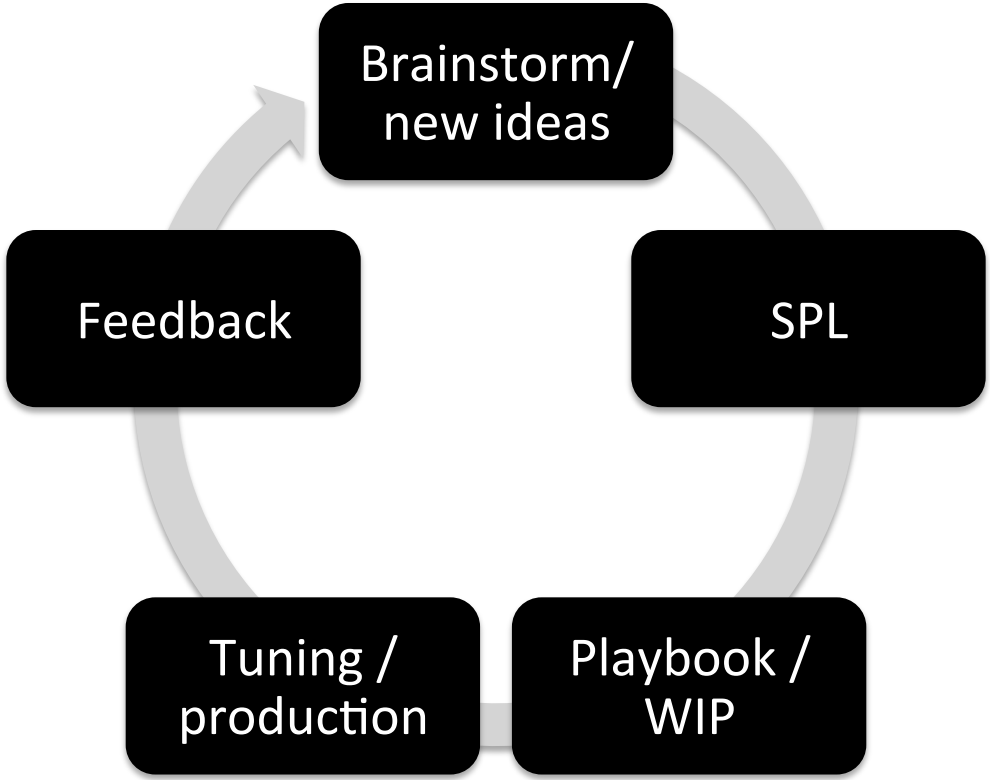
7 Links

Links	JIRA
	Splunk
Dev Contact	Jordan Perks

Automated Documentation



ES Rules Lifecycle



Notable Metrics

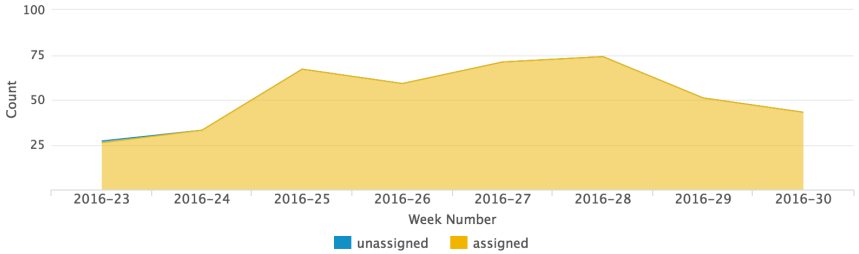
Notables

43 -8

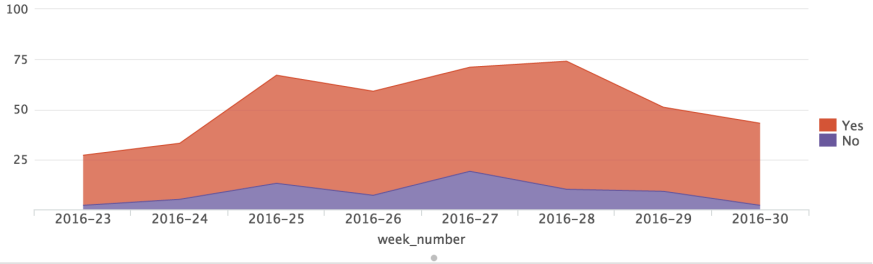
Total Events

Splunk Enterprise Security

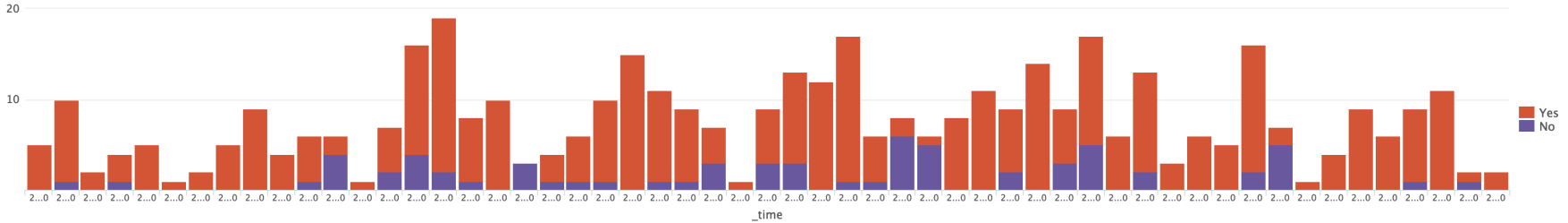
Count of Notable Events By Assigned Status and Week Number



Count of Notable Events By Met SLA and Week Number

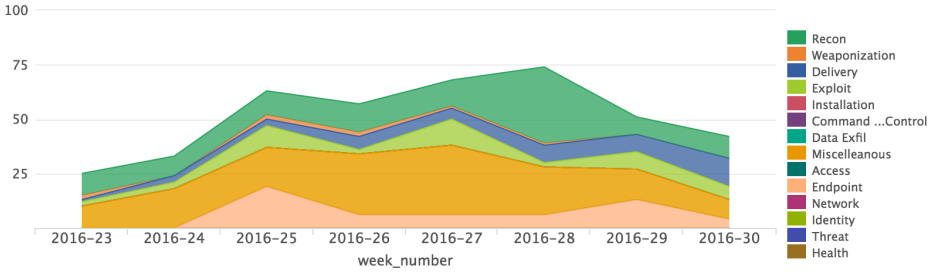


Count of Notable Events By Met SLA and Day

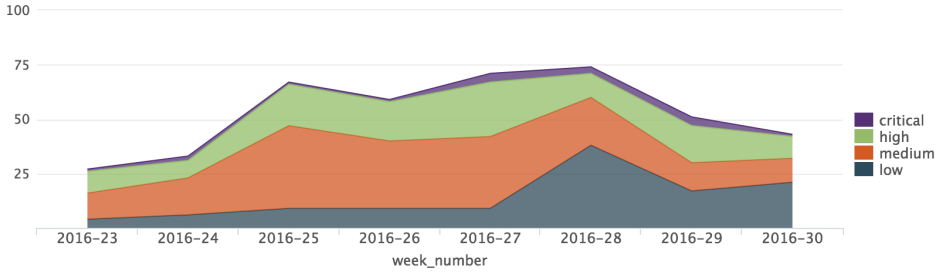


Notable Metrics Continued

Count of Notable Events By Kill Chain Stage and Week Number

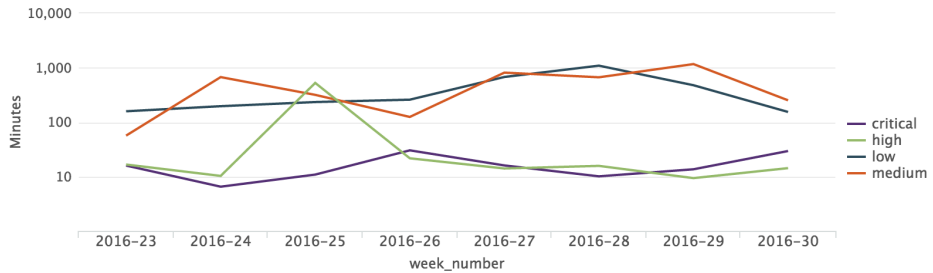


Count of Notable Events By Urgency and Week Number



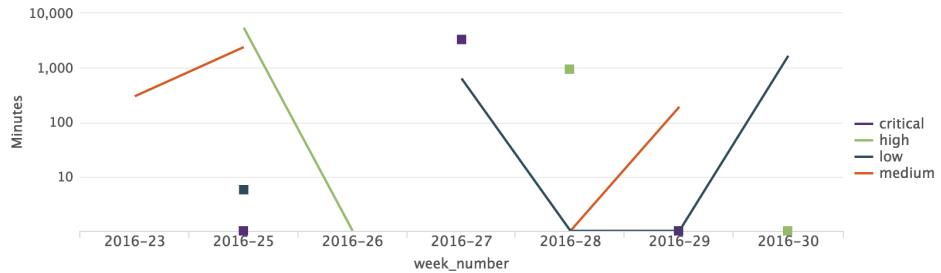
Average Time in Minutes To Acknowledge By Week Number and Urgency

All Urgency



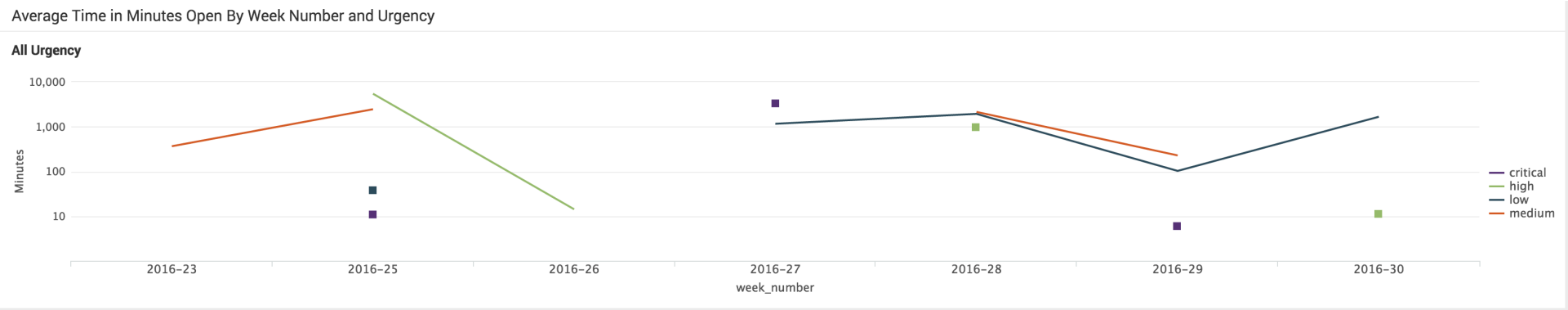
Average Time in Minutes To Resolve By Week Number and Urgency

All Urgency

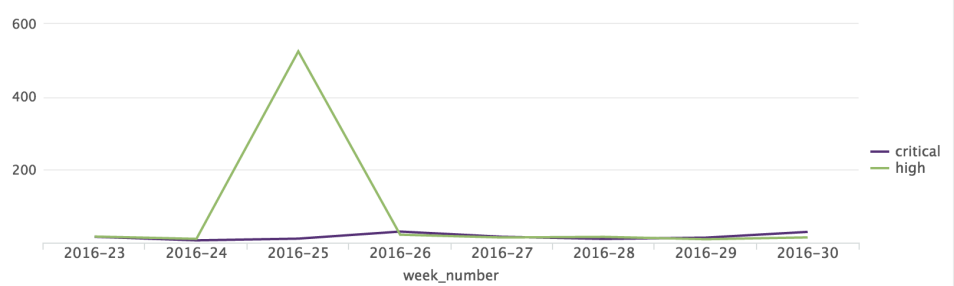


Notable Metrics Continued

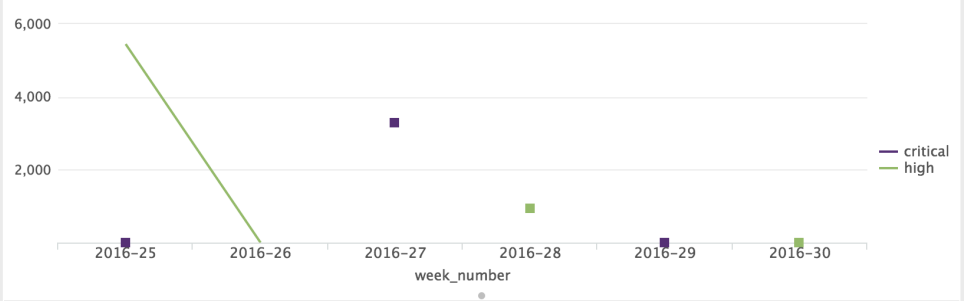
Average Time in Minutes Open By Week Number and Urgency



Average Time in Minutes To Acknowledge By Week Number and Urgency

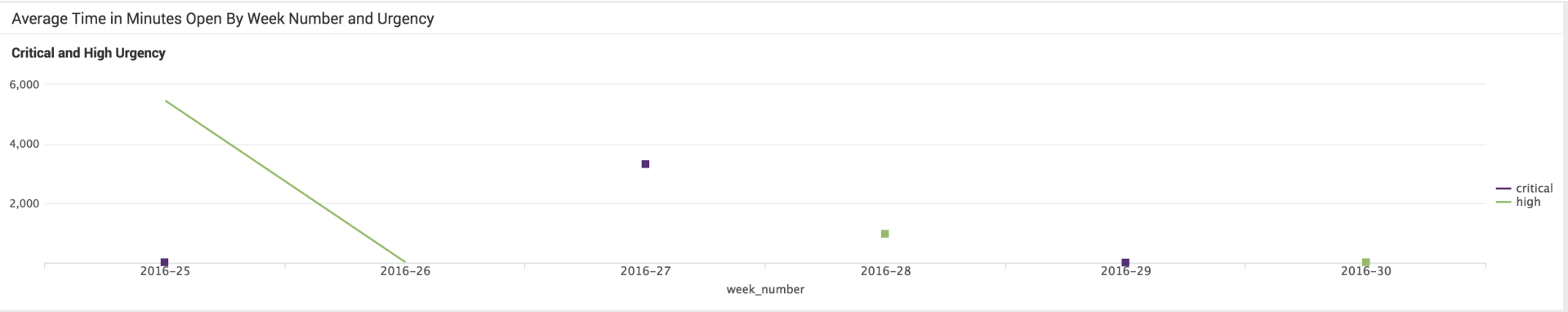


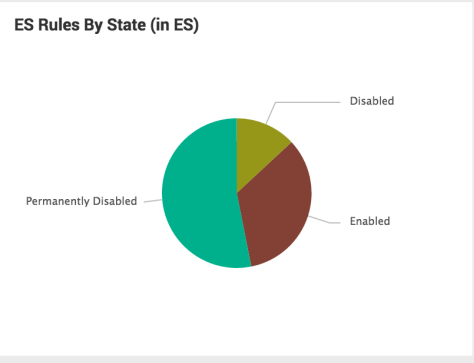
Average Time in Minutes To Resolve By Week Number and Urgency

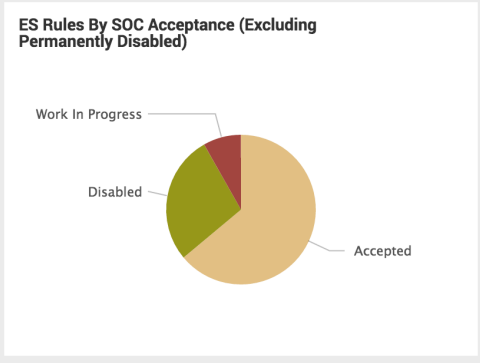


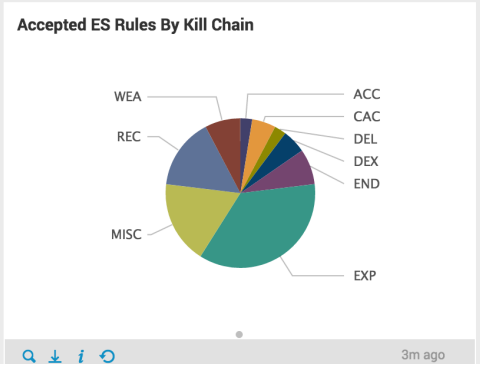
Average Time in Minutes Open By Week Number and Urgency

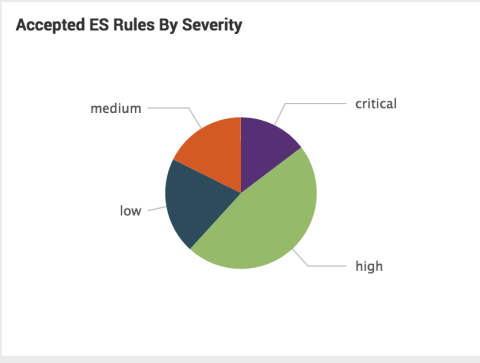
Notable Metrics Continued











Questions?

THANK YOU

splunk>