



**splunk®**

# ITSI'ing ITSI: How to leverage the internal ITSI indices to extend your service capabilities

Chris Crocco | Lead Solutions Engineer ViaSat, Inc.

August 2018 | Version 2.0

# Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

Splunk, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2018 Splunk Inc. All rights reserved.

# CHRIS CROCCO

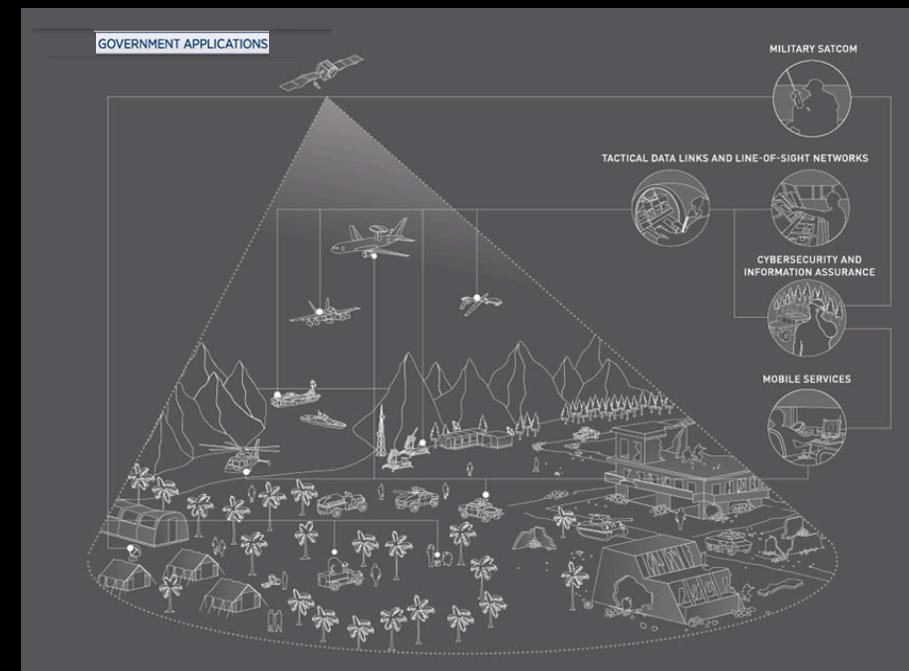
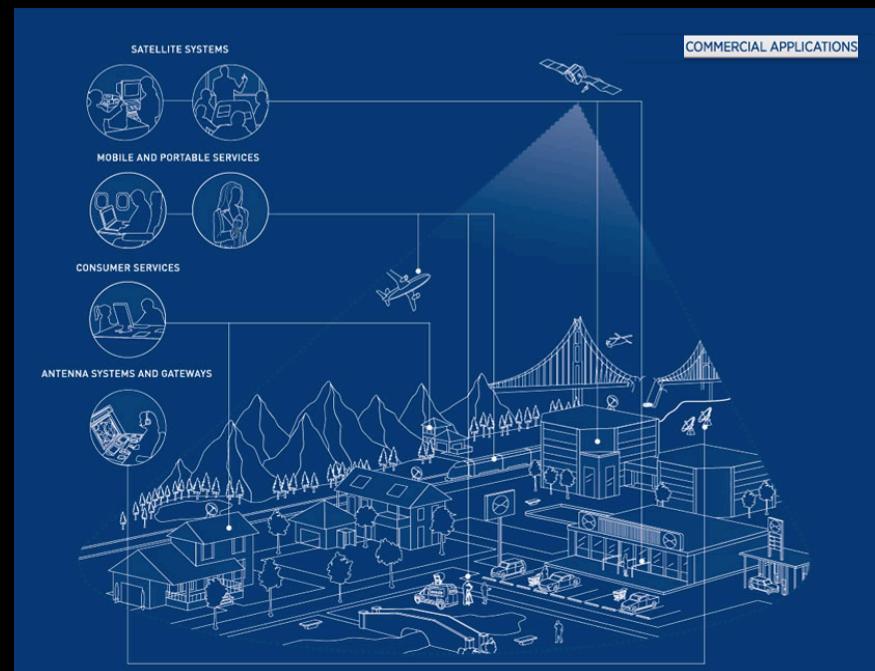
Lead Solutions Engineer, ViaSat, Inc



# About Viasat

## ViaSat: Connecting the World is Our Mission

- ▶ Global communications company that believes everyone and everything in the world can be connected
- ▶ More than 4,500 employees across 26 offices



# The Do's and Don'ts of ITSI

---

## Knowing Your Use Case for Initial Success



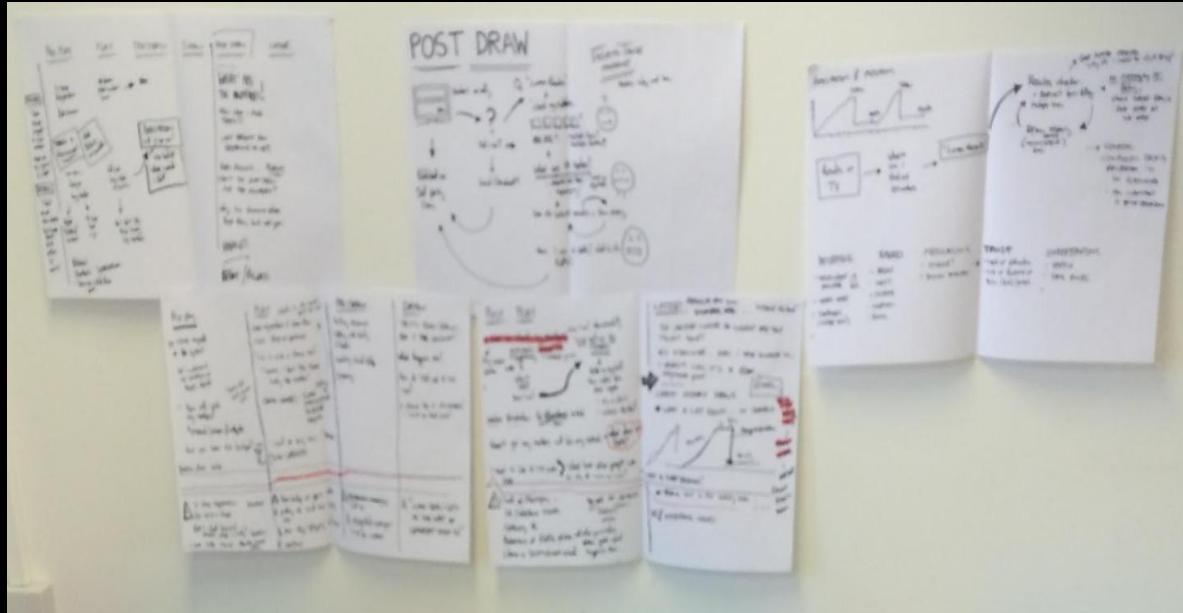
# Know Your User Requirements

## Don't Use the Ferrari if They Only Need a Bicycle

- ▶ If all they need is one function of Splunk, ITSI might not be the right fit
  - Scheduled Reports
  - Static alerts
  - Dashboards that never change
  
- ▶ If they need actual performance management (not just alerts) than you do!
  - Aggregated performance over time
  - Predicting future performance
  - Impacts of one part of your environment on another
  - Anomalies in normal behavior
  - Service lens

# Know and Agree on What Healthy Means

AND Make Sure Everyone Else Does Too!



► Know all of the components of your service

- KPI's
- Entities
- Dependencies

► Make sure cross functionally everyone is on the same page

- KPI Calculation
- Service Definition
- Search Schedule
- Thresholds

# Be Willing to Stay Engaged

## Both With Your ITSI Deployment and Your Users

# Services Are Needy!

- ▶ Adaptive Thresholding
  - ▶ Environment expansion
  - ▶ Entity discovery

# The NOC is Needy Too!

- ▶ They need this information to do their job
  - ▶ Introducing a lot of change to a change-averse culture
  - ▶ Alert conditions are a moving target

# Be Patient When Building Your First ITSI Service

# **Build- Re-Evaluate- Modify!**

# Factors for Getting ITSI Right

- ▶ Good KPI Base Searches
  - ▶ Correct Thresholds
  - ▶ ....and we haven't even talked about entities yet!

# Be Okay With Iterating!

- ▶ Learn from your mistakes and user feedback
  - ▶ Let changes soak
  - ▶ If all else fails...backup and restore



# ITSI Internal Index Overview

What ITSI is Doing in the Background



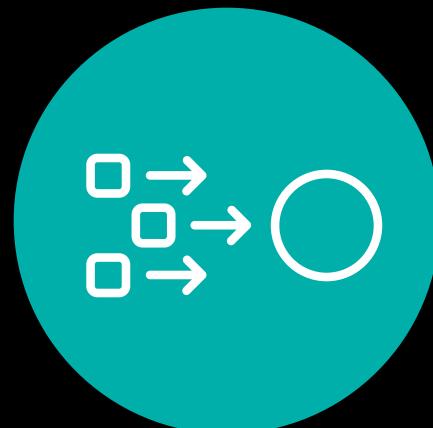
# The Big 4

# Where Your Most Important ITSI Data is Located



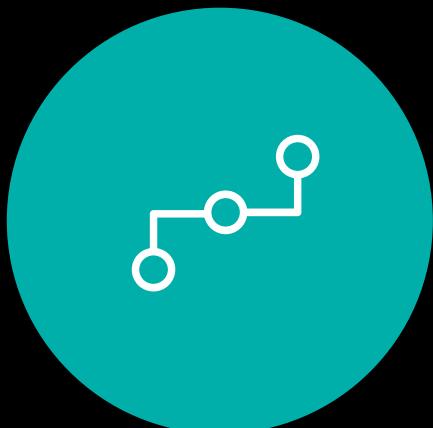
# itsi\_summary

# Service and KPI information



## itsi\_tracked\_alert

# Active Notable Events



## itsi\_notable\_audit

## Notable Event Action Details



itsi\_notable\_archive

# Historical event metadata

# Other Important Data Sets



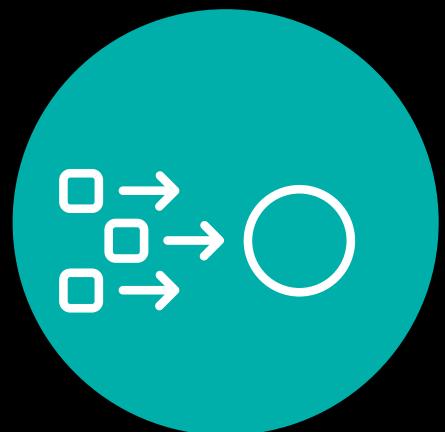
# service\_kpi\_lookup

## Service Metadata lookup



# index=anomaly\_detect

## KPI anomaly detection from services



## index=itsi\_grouped\_alerts

### Active notable event groups

# Scenario 1: Better Multi-KPI Alerts



# The Problem

## Entities and Stuff...

- ▶ What Multi-KPI alerts are good for off the shelf
  - Website Performance
  - User impact
  - General Cloud Tenancy/VPC degradation

- ▶ What am I supposed to do with this?

```
gs_kpi_id: 25e9ae45126874c4e8af5bf2
kpibasesearch: 5a594ba490a7c0c74849bef
alert_value: 100
alert_color: #F26A35
status: 1
percentage: 100
all_info: Ping Packet Loss had severity value high 1 times in Last 15 minutes
is_service_max_severity_event: 1
event_description: Ping Packet Loss had severity value high 1 times in Last 15 minutes
entity_key: service_aggregate
indexed_itsi_kpi_id: 25e9ae45126874c4e8af5bf2
alert_period: 5
```

# The Solution: Part 1

## Find Your Entities

- ▶ Creating new Nested Macros that are applied in conjunction to the base multi-KPI macro's

New Search		Save As
<pre>'composite_health_data' ("composite_kpi_id"="TEST MULTIPLE ENTITITES ISSUE" AND health_score&lt;=40)   join [search `composite_health_data` ("composite_kpi_id"="TEST MULTIPLE ENTITITES ISSUE" AND health_score&lt;=40)   stats latest (alert_level) as latest_alert_level]   search ((latest_alert_level != -2) AND (alert_level != -2))   reverse   suppressalert is_consecutive=False count=1 suppression_period=15 `associate_kpi_entities`</pre>		
Last 60 minutes		
56 events (1/29/18 7:59:00.000 PM to 1/29/18 8:59:51.000 PM) No Event Sampling ▾		
Events	Patterns	Statistics (5)
Events	Patterns	Visualization
20 Per Page	Format	Preview
entity_title	composite_kpi_id	composite_kpi_name
mgtr01-san0096.nav.spprod.viasat.io_Cellular0_1_0	TEST MULTIPLE ENTITITES ISSUE	TEST MULTIPLE ENTITITES ISSUE
aggs01-san0001.nav.spprod.viasat.io_Ethernet1	TEST MULTIPLE ENTITITES ISSUE	TEST MULTIPLE ENTITITES ISSUE
aggs01-san0096.nav.spprod.viasat.io_Ethernet1	TEST MULTIPLE ENTITITES ISSUE	TEST MULTIPLE ENTITITES ISSUE
mgtr01-san0001.nav.spprod.viasat.io_Cellular0_1_0		
mgtr01-san0096.nav.spprod.viasat.io_Cellular0_1_0		
asla01-san0053.nav.spprod.viasat.io	TEST MULTIKPI SAN0053 RTT AND LATENCY	TEST MULTIKPI SAN0053 RTT AND LATENCY
mgtr01-san0096.nav.spprod.viasat.io_Cellular0_1_0	TEST COMPOSITE SCORE NEW SAN AVAILABILITY	TEST COMPOSITE SCORE NEW SAN AVAILABILITY
aggs01-san0001.nav.spprod.viasat.io_Ethernet1	TEST COMPOSITE SCORE NEW SAN AVAILABILITY	TEST COMPOSITE SCORE NEW SAN AVAILABILITY
aggs01-san0096.nav.spprod.viasat.io_Ethernet1		
mgtr01-san0001.nav.spprod.viasat.io_Cellular0_1_0		
mgtr01-san0096.nav.spprod.viasat.io_Cellular0_1_0		

# Use Cases



# Network Alerting

- Link Flaps, IS IS Adjacencies, etc.



- Database to order provisioning correlations



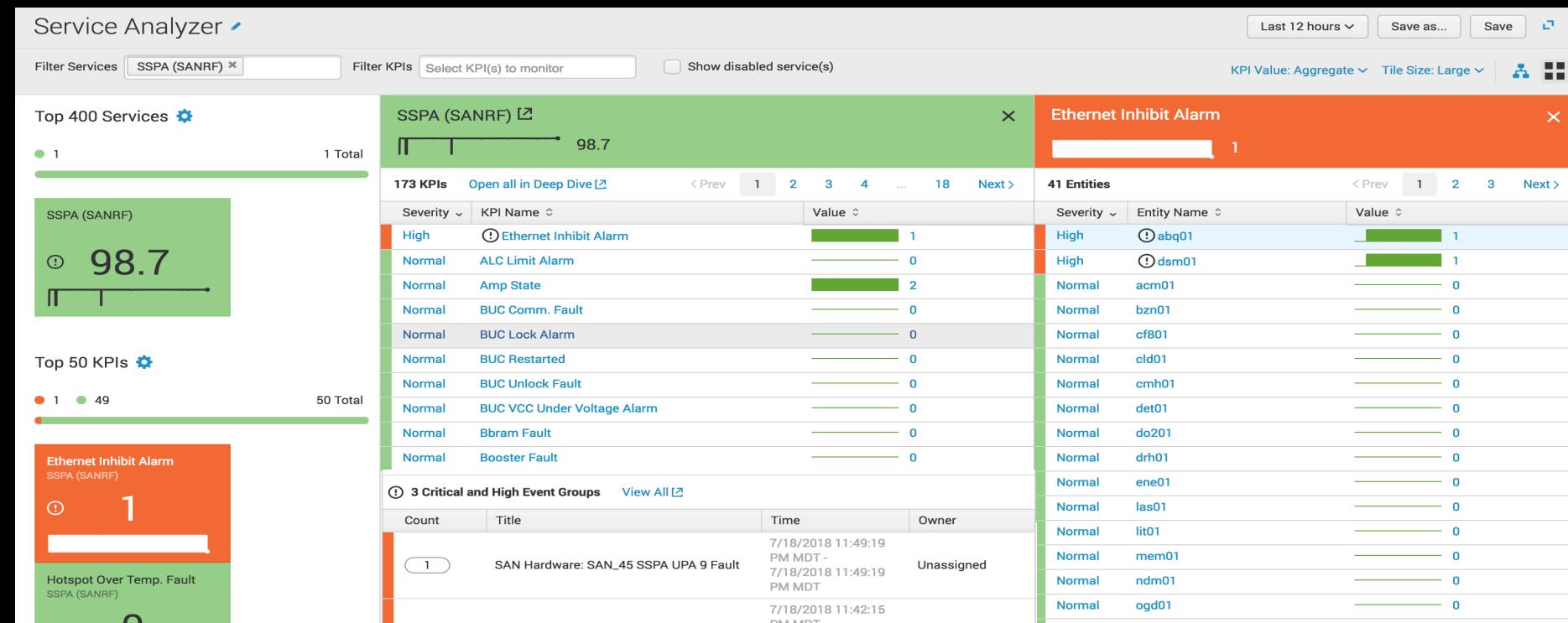
## Airlines

- Tail to ground segment hosts

# The Solution: Part 2

## ITSI Summary in Correlation Searches

- ▶ Use the service information in the `itsi_summary` index to create rich Notable events

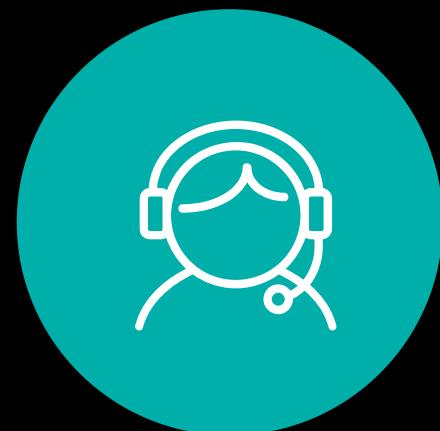


# Use Cases



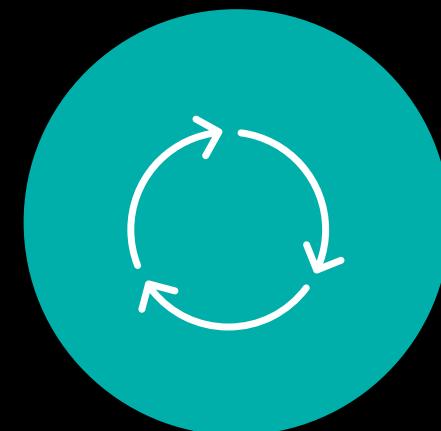
## Hardware Alerting

- Same hardware in different locations



## NOC Alerting

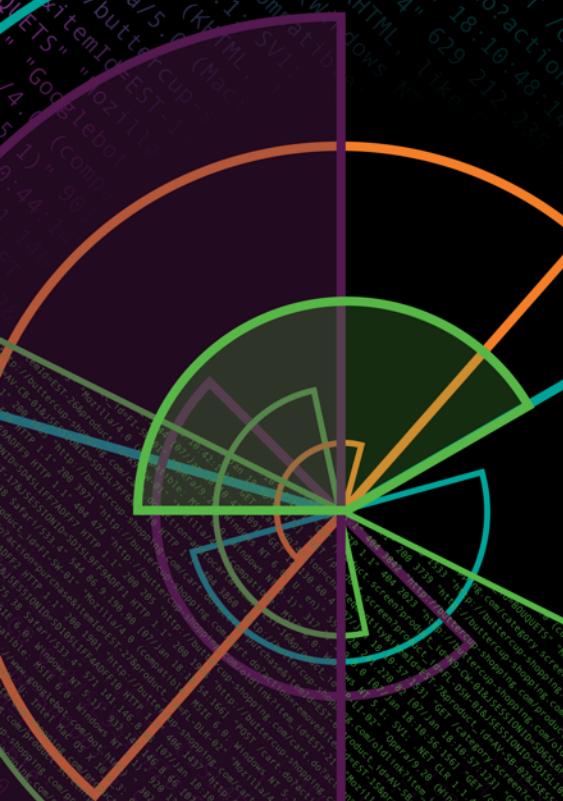
- Operator information



# DevOps Incident Management

- xMatters notifications,  
automation variables

# Scenario 2: Event Orchestration



# The Problem

## Validating an Issue is Real Before Getting Humans Involved

- ▶ Many events can self-recover
    - Link Flaps
    - CPU/Memory Spikes
    - Order processing backlogs
  - ▶ This pulls resources away from other tasks

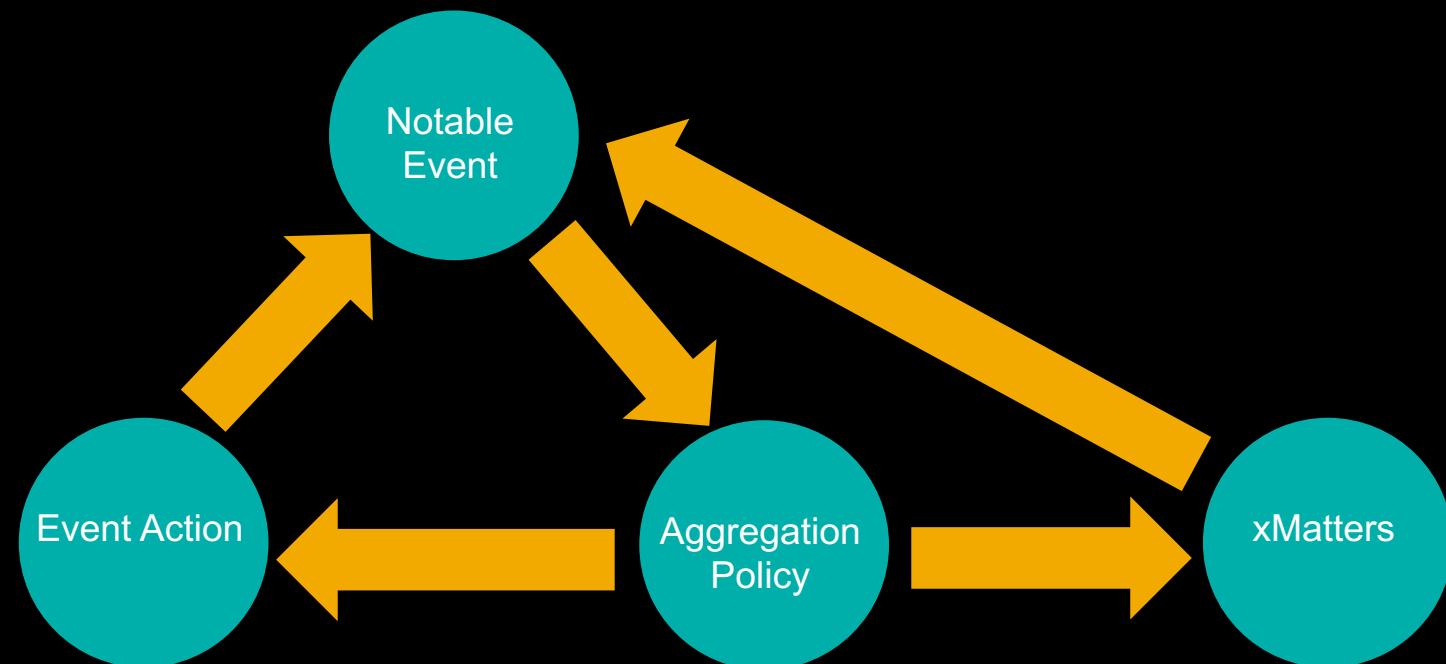
# Don't wake me up for this...

KPIs				
Severity	KPI	Service	Sparkline	
High	CPU Load	aggs01-san0006.naw.spprod...		
High	CPU System	aggs01-san0006.naw.spprod...		
Low	CPU User	aggs01-san0006.naw.spprod...		

# The Solution

# Aggregation Policies to the Rescue!

- ▶ By having aggregation policies do some validation steps, you can reduce alert fatigue and make your services better!



# The Solution

## Looping Notable Events

- ▶ Use the output of aggregation policy action rules to make new KPI's and alerts

The screenshot shows the Splunk IT Service Intelligence interface. On the left, a sidebar titled 'SAN Down xMatters' displays 'Notable Event Aggregation Policy description' and 'Action Rules'. The main area is titled '(x) matters' and shows a 'New Notable Event Alert from Splunk ITSI'. The alert details are as follows:

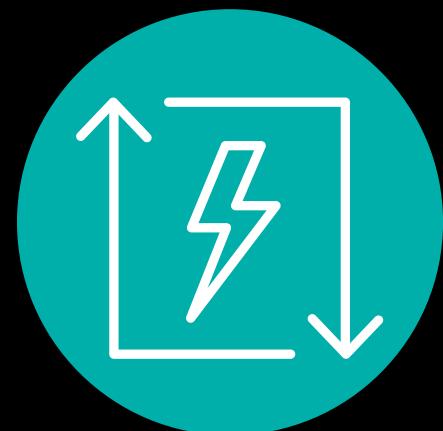
- Title:** mgts01:iasat.io has failed availability ping tests
- Description:** mgts01:viasat.io has failed availability ping tests
- Host:** mgts01:asat.io
- Owner:** unassigned
- Severity:** Medium
- Splunk Server:** splindawsprd08.splunk.viasat.io
- Event Severity Breakdown:** This notable event contains (1) Medium
- Grouped Events**

Below the alert details, there is a table with one row:

mgts01	viasat.io has failed availability ping tests	.spprod.viasat.io
Medium		

At the bottom of the main window, there is a footer with the 'splunk>' logo and a toolbar with buttons for 'Title', 'Threshold Field', 'Entity Calculation', 'Service Calculation', 'Unit', and 'Actions'.

# Use Cases



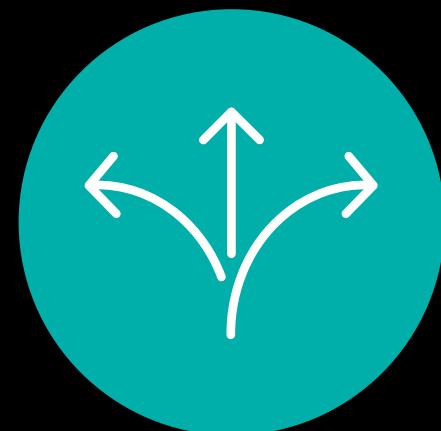
# DevOps Alerting

- Only notify engineers when there is a real issue



# Maintenance Validation

- Confirm services are working following a deployment



# Auto-Remediation

- Send a webhook to Auto-remediation orchestrator

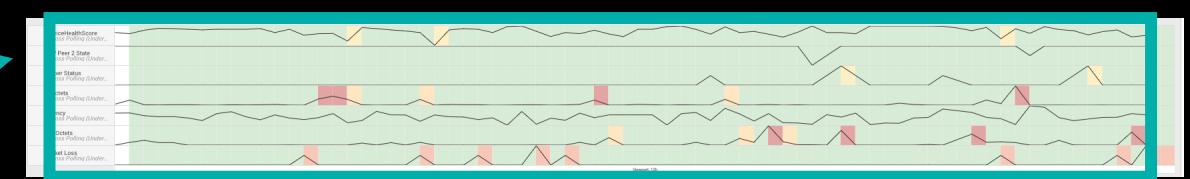
# Scenario 3: ITSI and ML Toolkit

# The Problem

## How Do I Discover Patterns in my ITSI Notable Events?

- ▶ Deep dives are good for seeing variations in KPI's over time
  - Threshold breaches that happen in conjunction
  - Time series patterns in KPI data
  - Operator level analysis
- ▶ No mechanism for pattern matching Notable events

What should I care about here?



# The Solution

# Use the ML Toolkit to do event clustering

- ▶ Piping your alert values through the clustering algorithms allows you to see patterns in the thresholds



# The Solution

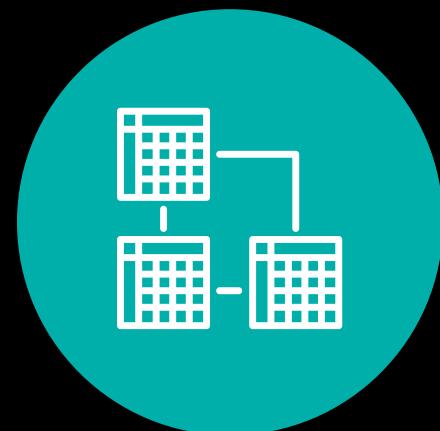
## Cluster Notable events

- ▶ Use the output of the `itsi_summary` index to identify patterns in your service data



Fields Set of Fields which are used together to identify if notable event is unique or not.  
Drill-down link title? Hardware Ops Runbooks

# Use Cases



# Resource prioritization

- What to fix first



## Impact assessment

- Which of my customers is having the worst experience



# Predictive Operational insight

- Know what you didn't know before

# Predictive Analytics Resources

- ▶ **Blog Post by Nate Smalley and Andrew Stein at Splunk: ITSI and Sophisticated Machine Learning**
- ▶ **ITSI Prediction Conf Sessions:**
  - Session IT 1676: Splunk IT Service Intelligence (ITSI) Not Just for IT Operations! How to Monitor a National Power Grid Using ITSI : Wednesday, Oct 03, 11:30 a.m. – 12:15 p.m.
  - Session IT1396 Transunion and a Time Traveling Delorean: MTTR Fading Like Marty McFly: Wednesday, Oct 03, 3:15 p.m. - 4:00 p.m.

# Scenario 4: ITIaaS



# The Problem

## ITSI isn't in the Monitoring Console

- ▶ Several factors can impact the performance of ITSI
  - Upgrades to the environment
  - Bad base searches and correlation searches
  - Service Templates
  
- ▶ You need a way to monitor ITSI like the rest of your infrastructure



# Key Takeaways

## How to build a better ITSI

1. Make your base ITSI deployment as good as you can through best practices
2. Leverage the summary and notable event indices for better alerting, actions, and context for your Services and Events
3. ITSI and ML Toolkit are best friends

# Join the Pony Poll



[ponypoll.com/\\*\\*\\*](http://ponypoll.com/)

# Thank You

**Don't forget to rate this session  
in the .conf18 mobile app**

