



splunk>

Anatomy of a Successful Event Analytics Implementation

Ross Lazerowitz | ITOA-PM
Martin Wiser | ITOA-Practitioner

October 2018 | Version 2.0

Our Speakers



ROSS LAZEROWITZ

**Splunk
ITOA Product Management**



MARTIN WISER

**Splunk
ITOA Practitioner**

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.

Key Takeaways

In today's session,
you'll learn

1. What is Event Analytics
 - Demo
2. How to Get Data In
3. Event Reduction/Correlation
4. Implementation Plan
 - Implementation Activities
 - Project Timeline/Schedule
 - Deployment Steps
5. Tuning and Troubleshooting
6. Q&A

You Need an Approach That...

Provides easy and seamless access to all data of any type and volume

1 Delivers **service context** to prioritize investigation



2 Understands **time-based behavior** based on historical patterns



Splunk IT Service Intelligence™



3 Helps you find what's broken quickly with human-scale actionable alerts



Today We Are Going to Focus on Events

ITSI needs to be able to handle all of this in order to be “The Backbone of IT Monitoring”



Logs



Metrics



Events

```
138.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 404 728 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=63-5w-03"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=SD5SL7FF6ADFF0 HTTP 1.1" 404 322 "http://buttercup-shopping.com/category.screen?category_id=01&product_id=63-5w-03"
191.317.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&SESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-1B&product_id=AV-CB-016.1&SESSIONID=SD5SL7FF6ADFF0"
191.317.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&SESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-1B&product_id=AV-CB-016.1&SESSIONID=SD5SL7FF6ADFF0"
191.317.27.160.0 - - [07/Jan 18:10:56:156] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=SD5SL7FF6ADFF0 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/category.screen?category_id=01&product_id=63-5w-03"
191.317.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&SESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-1B&product_id=AV-CB-016.1&SESSIONID=SD5SL7FF6ADFF0"
191.317.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&SESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-1B&product_id=AV-CB-016.1&SESSIONID=SD5SL7FF6ADFF0"
191.317.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&SESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-1B&product_id=AV-CB-016.1&SESSIONID=SD5SL7FF6ADFF0"
191.317.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&SESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-1B&product_id=AV-CB-016.1&SESSIONID=SD5SL7FF6ADFF0"
191.317.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&SESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-1B&product_id=AV-CB-016.1&SESSIONID=SD5SL7FF6ADFF0"
191.317.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&SESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-1B&product_id=AV-CB-016.1&SESSIONID=SD5SL7FF6ADFF0"
```


Example Event

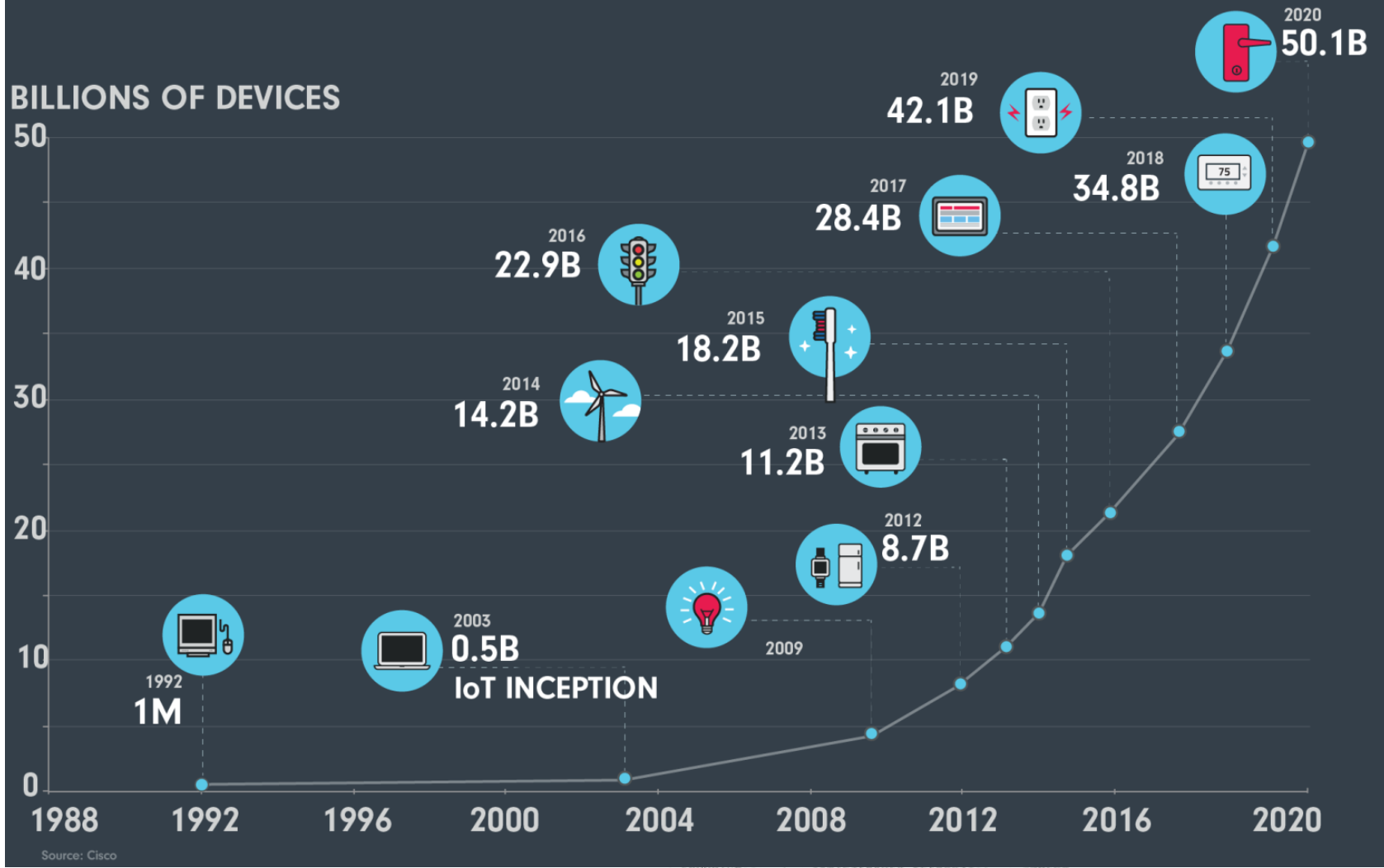
Nagios Health Check

```
1502642822 src_host="splunk_sh-01" omd_site="SJC"  
perfddata="SERVICEPERFDATA name="check_dhcp" severity="OK" attempt="1"  
$statetype="HARD" executiontime="0.000" latency="0.000" reason="OK: Received  
1 DHCPOFFER(s), max lease time = 600 sec." result="OK"
```

It's Only Getting Worse

GROWTH IN THE INTERNET OF THINGS

THE NUMBER OF CONNECTED DEVICES WILL EXCEED 50 BILLION BY 2020



138.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=5D15L9FF10ADFF10 HTTP 1.1" 404 728 "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 14.10.10.10

The Road to ITSI Event Analytics

ITSI 2.1

ITSI supports Notable Events.

.conf 2017

ITSI releases Smart Mode. ITSI can now use machine learning to reduce noise in events.

.conf 2016

ITSI releases the Policy Engine. Users can curate policies that reduce the noise in events and take automated action.

.conf 2018

ITSI introduces impact console an alert timeline. Bringing analytics driven context to alarms.

Splunk ITSI for Event Analytics

Simplify Your Operations With Artificial Intelligence and Service Context

Service Context

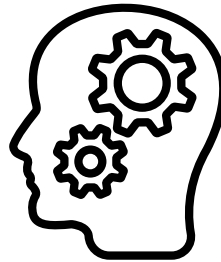


Find and fix the most important issues

Contextualize and prioritize

Reduce time-to-resolution on business-critical services

Artificial Intelligence



Transform IT operations with machine learning

Separate valuable signal in noise

Enable IT with intelligence for data-driven decisions

Scalable Platform



Get a full view of your IT environment

Respond collaboratively and simplify operations

Share customized insights across the enterprise to enable business-centric IT





Demo

Talk is cheap. Demonstrations are where it's at

How to Onboard Data

- ▶ **ITSI Native**
 - Anomaly Detection
 - Multi-KPI Alerts
- ▶ **Splunk Native**
 - Correlation Searches
 - Enrichment, Suppression
- ▶ **External Sources**
 - HTTP Event Collector



How to Onboard Data

Multi KPI Alerts
Create Correlation Search based upon selected KPIs

Service Analyzer | Notable Events Review | Glass Tables | Deep Dives | Multi KPI Alerts | Search | Configure | IT Service Intelligence

Composite score | Status over time | Last 15 minutes

1. Services

Select services that contain KPIs for your alert. Include service dependencies?

search

Deselect All

- Database Service
 - Depends on
 - Impacts
- Network Service
- Website service
 - Depends on
 - Impacts

2. KPIs in Selected Services

+Add Selected | *View Selected in Deep Dive | filter | 10 Per Page

i	+	Add	KPI	Service	Percentage Status Breakdown	Latest Status
>	<input type="checkbox"/>	+ Add	DB response time	Database Service	<div style="width: 100%;"><div style="width: 100%; background-color: #c00000;"></div></div>	High
>	<input type="checkbox"/>	+ Add	mem_free	Website service	<div style="width: 100%;"><div style="width: 100%; background-color: #008000;"></div></div>	Normal
>	<input type="checkbox"/>	+ Add	error count	Website service	<div style="width: 100%;"><div style="width: 100%; background-color: #c00000;"></div></div>	Critical
>	<input type="checkbox"/>	+ Add	response time	Website service	<div style="width: 100%;"><div style="width: 100%; background-color: #ff8c00;"></div></div>	High
>	<input type="checkbox"/>	+ Add	cpu_load_percent	Website service	<div style="width: 100%;"><div style="width: 100%; background-color: #008000;"></div></div>	Normal

3. Selected KPIs

The associated correlation search runs when severity-level thresholds exceed trigger conditions

Composite Score: 35 ■ Medium
Range: Critical 0-10, High 10-30, Medium 30-50, Low 50-70, Normal 70-90, Info 90-100

-Remove Selected | *View Selected in Deep Dive | filter | 10 Per Page

i	Remove	KPI	Service	Latest Status	Importance
>	<input type="checkbox"/> - Remove	response time	Website service	High	<input type="range" value="9"/>
>	<input type="checkbox"/> - Remove	cpu_load_percent	Website service	Normal	<input type="range" value="5"/>
>	<input type="checkbox"/> - Remove	DB response time	Database Service	High	<input type="range" value="9"/>

Multi KPI Alerts

are designed for users to be able to identify multiple interrelated problems that result in KPI statuses becoming unfavorable across Services and get alerted on such issues. They are great in identifying service degradation across multiple counters and alerting on them prior to the issues reaching a critical state. The user creates these alerts through a visual interface.

Correlation Search

SPL to pull events from index into Notable Events
Enrichment & Deduplication
Suppression & Change Windows

Token Replacement
%fieldname%

Drill downs allow you to open the raw events in search or launch any URL (dashboard, 3rd party)

Search Properties

Search Name*

Description?

Search Type

Search*

[Run Search](#)

Time range

Association

Service

Entity Lookup Field?

Schedule

Schedule Type

Run Every

Notable Events

Notable Event Title?*

Notable Event Description?

Owner? [Advanced Mode](#)
In advanced mode, use tokens like %fieldname% to use result field values to set owner

Severity? [Advanced Mode](#)
In advanced mode, use tokens like %fieldname% to use result field values to set severity

Status? [Advanced Mode](#)
In advanced mode, use tokens like %fieldname% to use result field values to set status

Drill-down Name?

Drill-down Search?

Drill-down earliest offset?

Drill-down latest offset?



Getting Data in (HTTP Event Collector)

► HEC Example

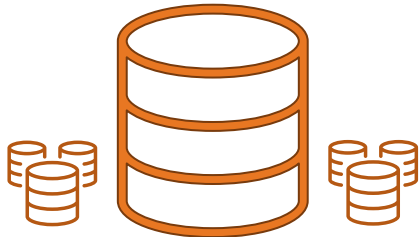
- HEC enabled by default (**needs to be working** for Notable Events to work)

The screenshot shows the 'HTTP Event Collector' configuration page in Splunk. It displays a list of 5 tokens. The table below represents the data shown in the screenshot.

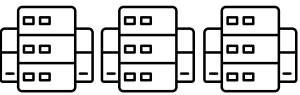
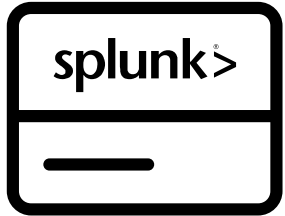
Name	Actions	Token Value	Source Type	Index	Status
Auto Generated ITSI Event Management Token	Edit Disable Delete	DB6C9B5D-1970-4BE4-8B13-3185B6C63075	stash	itsi_tracked_alerts	Enabled
Auto Generated ITSI Notable Event Retention Policy Token	Edit Disable Delete	F62402D3-2757-49CE-A55F-788DECBF2CBE	stash	itsi_notable_archive	Enabled
Auto Generated ITSI Notable Index Audit Token	Edit Disable Delete	FBB49534-CE9E-4320-BA26-C2A6ABEC80DC	stash	itsi_notable_audit	Enabled

- Need to generate GUID for event ID
- `curl -k https://localhost:8088/services/collector/event -H "Authorization: Splunk DB6C9B5D-1970-4BE4-8B13-3185B6C63075" -d '{"event" : {"event_id" : "d65600d-8669-4903-8a14-af88203add38", "title" : "Disk 90% Full", "status" : "4", "severity" : "6", "owner" : "unassigned", "description": "Disk is almost full", "other_field" : "more stuff"}'}`

Common Data Onboarding Use Case



Persistent Storage



Core Splunk



Event Management



Infrastructure Alerts
(SNMP, Monitors, Etc.)

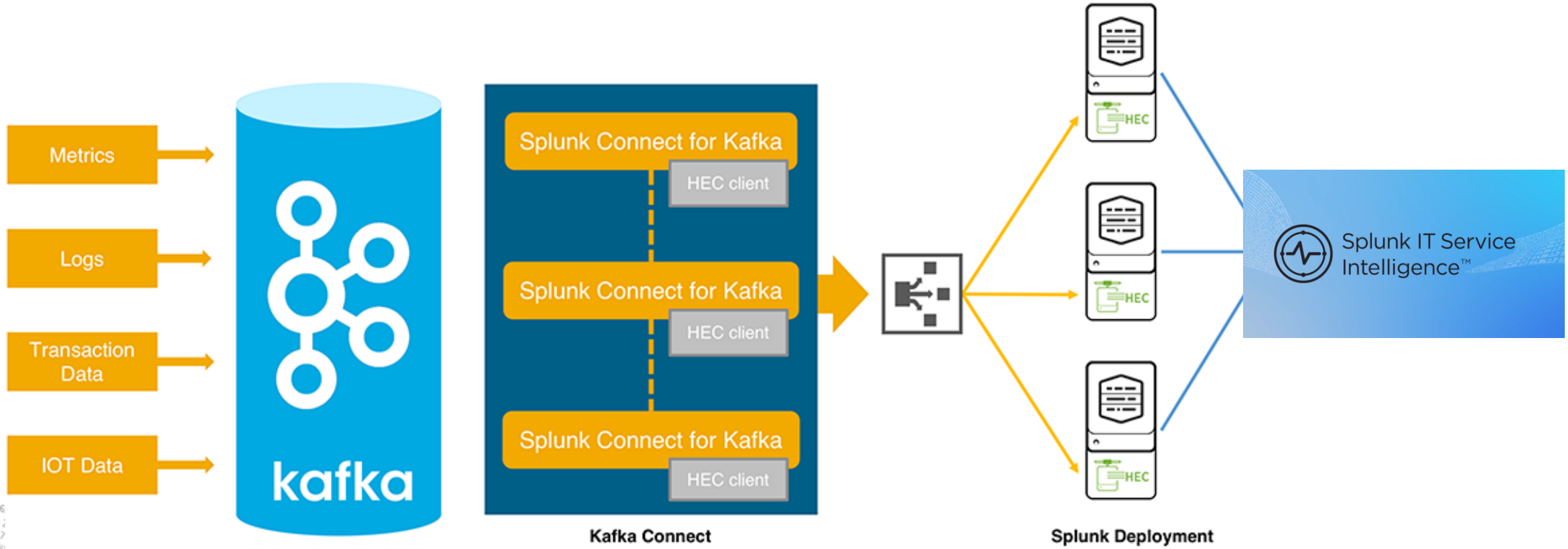
(Correlation Search → HEC)



Splunk IT Service Intelligence™



Large Scale Telco Data Pipeline



138.6
128.1
i= 317
ows N
-:0 @ - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GLFTS&JSESSIONID=5D15L9FF1ADFF3 HTTP 1.1" 404 728 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-66&product_id=63_5w-03"
-:1: 5VI: - [07/Jan 18:10:57:123] "GET /category.screen?category_id=GLFTS&JSESSIONID=5D15L9FF1ADFF3 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/category.screen?category_id=63_5w-03"
:/buttercup-shopping.com/product_id=RP-LI-02" 468 125.17 14.1.4322" "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=63_5w-03"
:/buttercup-shopping.com/product_id=RP-LI-02" 468 125.17 14.1.4322" "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=63_5w-03"
:/buttercup-shopping.com/product_id=RP-LI-02" 468 125.17 14.1.4322" "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=63_5w-03"
:/buttercup-shopping.com/product_id=RP-LI-02" 468 125.17 14.1.4322" "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=63_5w-03"

Event Reduction

► Aggregate Notable Events into Event Groups

- Roll Up Duplicate Events
- Clear Noise
 - Suppress Alerts (Per Node/Per Region/Site)
 - Close Events based on Clearing Event
- Perform Automated Actions
 - Create IT Service Management Ticket
 - Page On-Call Staff

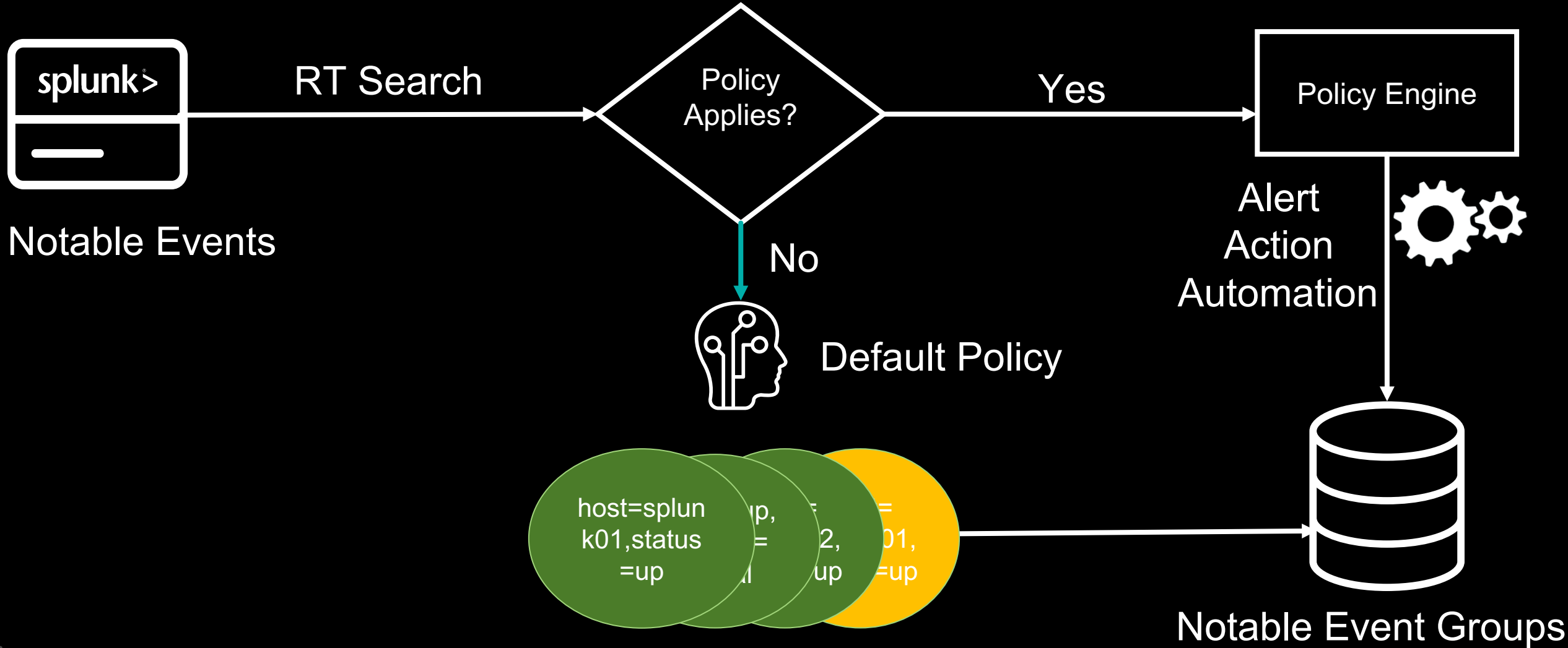


- splkhst38 Node Down
- snowhst01 Node Down
- splkhst38 Node Up



Should Clear Event
from Console

Let's Run In Real Time!



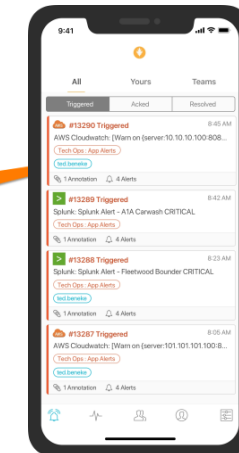
```

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD5L9FF1ADFF3 HTTP/1.1" 404 720
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-D5H-01&JSESSIONID=SD5L9FF1ADFF3 HTTP/1.1" 200 1318
317.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5L9FF1ADFF3 HTTP/1.1" 200 3865
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD5L9FF1ADFF3 HTTP/1.1" 404 720
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-D5H-01&JSESSIONID=SD5L9FF1ADFF3 HTTP/1.1" 200 1318
317.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5L9FF1ADFF3 HTTP/1.1" 200 3865
  
```

Common Operations Flow



Service Now, BMC Remedy, Cherwell
Service Management
ITIL/Incident Management



On Call Management
Routing/Notification Preferences
Mobile Interface
Escalation

Monitor

On-Premises: Containers, Servers, Security, Storage, Shopping Cart, Smartphones and Devices

Private Cloud: Online Services, Packaged Applications, Web Services, Location, Networks, Desktops, Firewalls, Intrusion Prevention, Databases

Public Cloud: Telecommunications, Call Detail Records

Detect/Analyze WHY

Splunk IT Service Intelligence™

splunk >

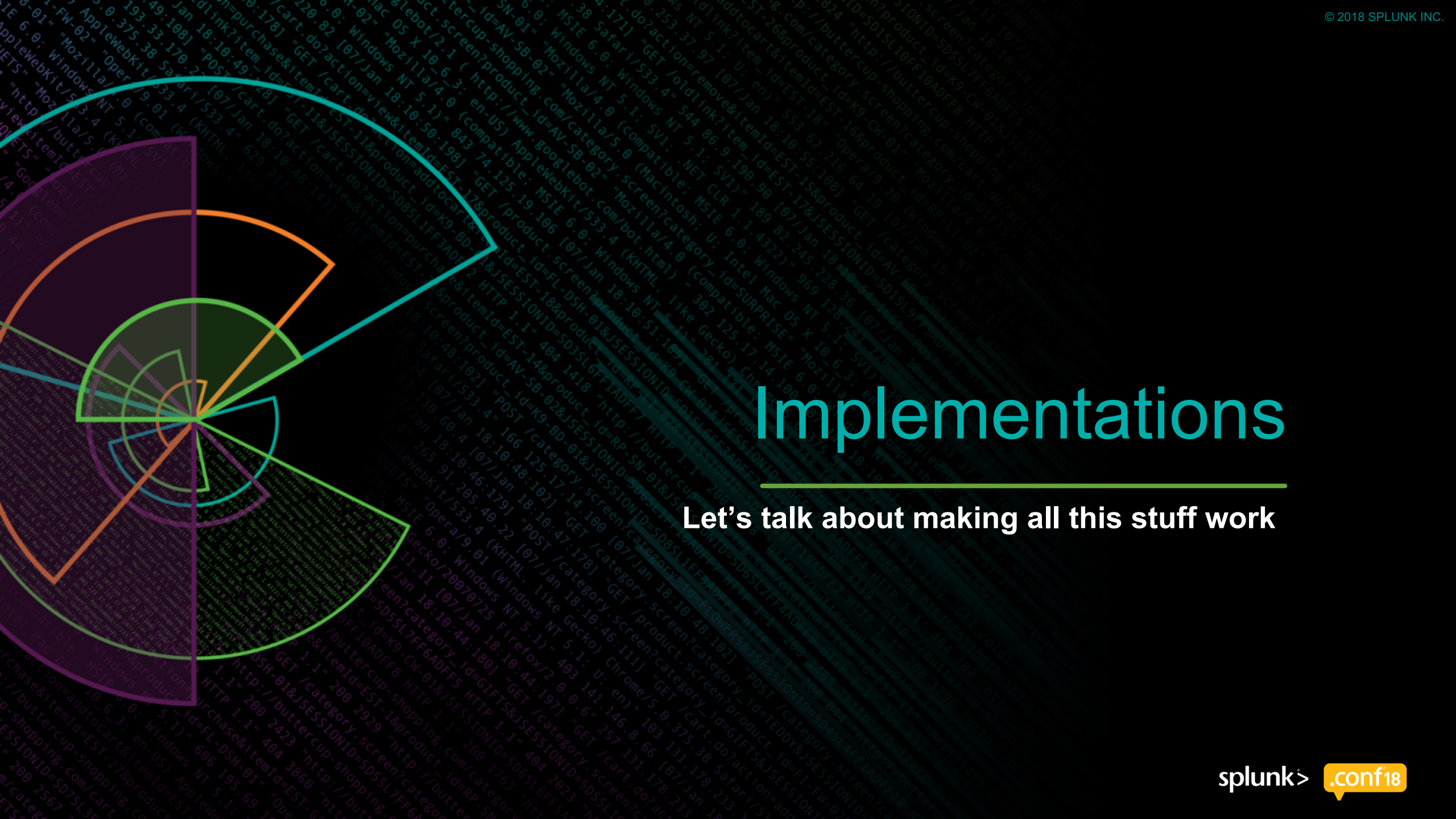
- Add to Triggered Alerts**
Add this alert to Triggered Alerts list
- Log Event**
Send log event to Splunk receiver endpoint
- Run a script**
Invoke a custom script
- Send email**
Send an email notification to specified recipients
- VictorOps**
Send a customized message to VictorOps on a triggered alert action in Splunk.
- Webhook**
Generic HTTP POST to a specified URL

+ Add Actions ▾

```

138.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 404 728 "http://buttercup-shopping.com/cart.do?action=view&item_id=EST-66&
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/category.screen?category_id=
ows NY 5-1: 5V1: - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 404 728 "http://buttercup-shopping.com/cart.do?action=view&item_id=EST-66&
item_id=EST-16&product_id=RP-LI-02" 468 125.17 14. - - [07/Jan 18:10:57:156] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS&SESSIONID=
shopping.com/cart.do?action=purchase&item_id=EST-26&SESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS&SESSIONID=
//buttercup-shopping.com/cart.do?action=purchase&item_id=EST-26&SESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS&SESSIONID=

```



Implementations

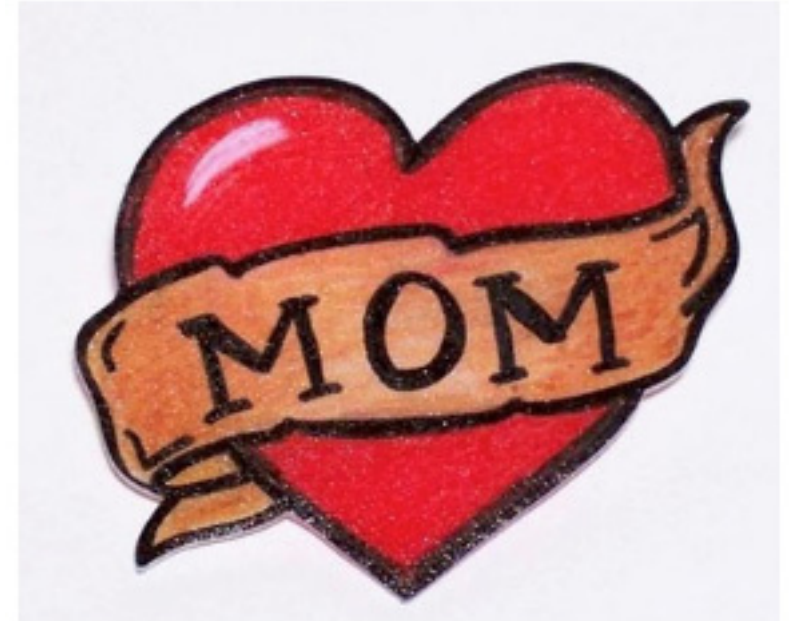
Let's talk about making all this stuff work

Review Existing MoM Architecture

- ▶ What DataSources do exist?
 - SNMP (Traps, Polling)
 - Performance Monitoring
 - 3rd Party Monitoring Packages

- ▶ Event Aggregation/Correlation
 - How complex are the rules
 - Event Suppression (Maintenance Windows, Deduplication)

- ▶ Reporting Gateways?
 - Ticketing Integration into Service Management Tools



```

138.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15L9FF10ADFF10 HTTP 1.1" 404 728 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-66&product_id=FI-SW-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"
ows NY 5-1: 5VI: - - [07/Jan 18:10:56:156] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D55L7FF6ADFF0 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=KQ-CW-06"
:/buttercup-shopping_id=RP-LI-02" 468 125.17 14. - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF10ADFF10 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS&JSESSIONID=5D55L7FF6ADFF0 HTTP 1.1"
do?action=purchase&itemId=EST-26&product_id=KQ-CW-06" 468 125.17 14. - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF10ADFF10 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS&JSESSIONID=5D55L7FF6ADFF0 HTTP 1.1"
opping.com/category.screen?category_id=FLOWERS&JSESSIONID=5D55L7FF6ADFF0 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS&JSESSIONID=5D55L7FF6ADFF0 HTTP 1.1"

```

Migration Approach

▶ Minimize Risk

- Implement "along side" existing MoM environment
 - no rip-and-replace, Provide a graceful migration process from <insertyourlegacytoolhere>

▶ Involve (NOC) in all phases

- They have deep SME in how valuable the event reduction truly is
- Adjust Alert Grouping based on feedback

▶ Implementation

- Proof of Concept/Pilot
 - Validate basic Event Management capabilities
- Minimum Viable Deployment
 - Partial User Migration/Hybrid Operations

Common Event Analytics Technology Add ons

▶ SNMP Traps

- <https://docs.splunk.com/Documentation/Splunk/7.0.3/Data/SendSNMPeventstoSplunk>

▶ Nagios

- <https://splunkbase.splunk.com/app/2703/>

▶ Service Management: BMC Remedy, Service Now, Cherwell

- <https://splunkbase.splunk.com/app/3087/>
- <https://splunkbase.splunk.com/app/1928/>

▶ App Dynamics

- <https://splunkbase.splunk.com/app/3471/>

▶ Other Common TAs

- AWS, Azure, GCP, Solarwinds, SCOM, Network Devices, *Nix, Windows

Putting it all together

- ▶ Review and Onboard Data Sources
- ▶ Identify Aggregation Logic and External Integrations
- ▶ Operational Analysis -> Design Future state Workflows
- ▶ Infrastructure and Workflow Build Out
- ▶ Pilot/POC
- ▶ Incorporate Stakeholder Feedback & Schedule Production Deployment
- ▶ Production Infrastructure Build Out
- ▶ Alert Accuracy Validation
- ▶ Operation Team Onboarding

Common Tuning and Troubleshooting

► Tuning

- Change Aggregation Policies to Real Time
 - http://docs.splunk.com/Documentation/ITSI/3.1.4/User/Managenotableeventindexes#Notable_event_real-time_search_optimization
- Adjust timeframe for Notable Event Console
- Publish pre-built views for different Operations Teams

► Troubleshooting

- Ensure Java is installed on ITSI SH – Aggregation Policies depend on it
- Index=_internal source="<install folder>/var/log/splunk/itsi_event_management.log"

Key Takeaways

- ▶ We learned why “Event Analytics” is so important
- ▶ We reviewed how to get your data into Splunk ITSI
- ▶ We demonstrated how to reduce event noise and automate recovery actions with curated policies and Artificial Intelligence/Machine Learning
- ▶ We discussed what operational models typically look like
- ▶ Finally, we examined how to implement ITSI Event Analytics and migrate off a legacy platform to take advantage of these noise reduction features



Q&A

Try and stump us. I dare you.

Thank You

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



Step 1 – POC/Pilot

- ▶ Show basics of Event Analytics
 - In you environment
 - Using your actual Events
 - APM, Network, SNMP, Performance Management, Backup, Power, Virtualization, ...
- ▶ Event Analytics Exercise
 - Prep remote (Infrastructure/Install)
 - 2-3 days on site
- ▶ Event Correlation
 - Manual Correlation Policies/Aggregation Policies
 - Smart Mode

Step 2 - Minimum Viable Deployment

▶ Operational Analysis

- Review current state capabilities, workflow, and key metrics
- Discuss future state workflow, Process and key metric improvement
- Deliverable: workflow diagram, capabilities diagram, value case

▶ Data and Architecture Analysis

- Review current state data sources and architecture
- Document and discuss methods for Splunk to ingest those data sources
 - Many will yield more granular input than existing methods
- Document and discuss replacement methods for current state architecture components
- Deliverable: categorized and prioritized data source listing, methods of data ingest into Splunk, future state logical architecture

Step 2 - Minimum Viable Deployment (continued)

- ▶ **Infrastructure and Workflow Build out**
 - Provision Compute Infrastructure/Software Installation
 - Perform Data Onboarding Activities
 - Various (Technology Add-Ons)
 - Replicate Impact Enrichment capabilities(e.g. CMDBs, Maintenance Windows)
- ▶ **Alert Accuracy Validation**
 - Legacy MoM and Splunk should closely mirror enrichment rules, Alert Counts
 - External Alert Actions (e.g. Service Management Ticketing)
 - Allow Data Consumers to switch to new Repository
- ▶ **Operation Team Onboarding**