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

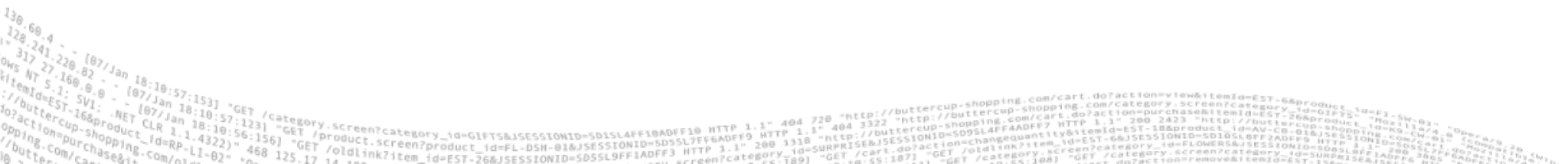
Splunk
ITOA Practitioner

splunk> .conf18

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.



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

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

The Three Pillars of Monitoring Data

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

Logs

Metrics

Events

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

What the Heck is an (IT) Event Anyway?

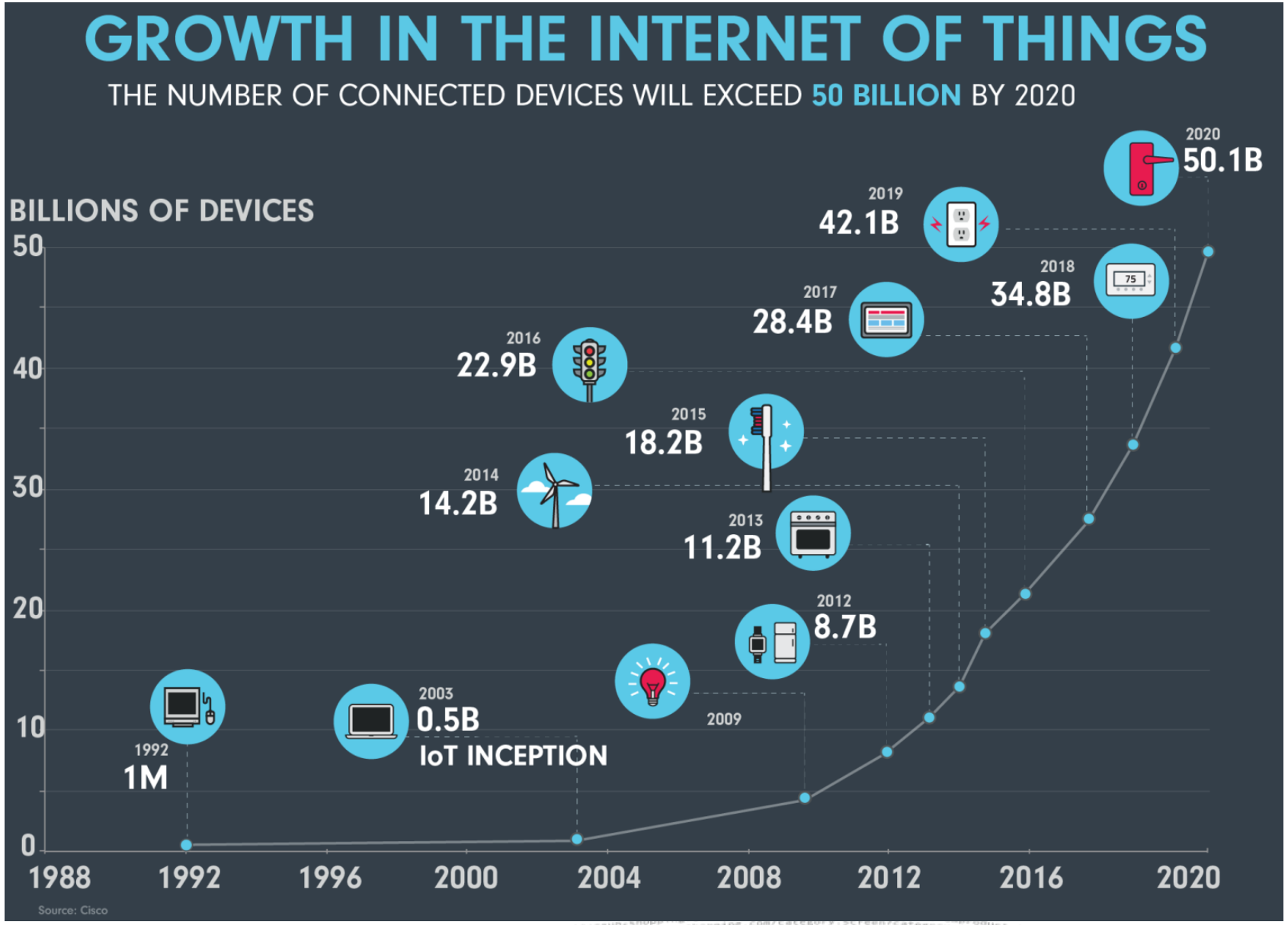
- For the purposes of this talk when we say “Event” we are referring to Events in the IT sense not the Splunk sense.
- Self descriptive message that tells a user that something happened.
- Usually contain some sort of title, severity, and description.
- Used to determine in the moment health.
- Often very noisy.
- Think alarm data coming out of tools like Nagios, Solarwinds, APM, Netcool, etc.

Example Event

Nagios Health Check

1502642822 src_host="splunk_sh-01" omd_site ="SJC" perfdata="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



From NCTA: https://www.ncta.com/positions/internet-of-things

The Road to ITSI Event Analytics

ITSI 2.1

ITSI supports Notable Events.

.conf 2016

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

.conf 2017

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

.conf 2018

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

splunk> .conf18

Splunk ITSI for Event Analytics

Simplify Your Operations With Artificial Intelligence and Service Context

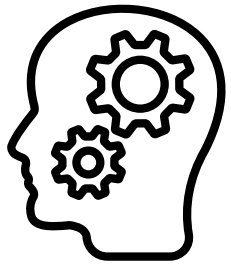
Service Context

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**

splunk> .conf18

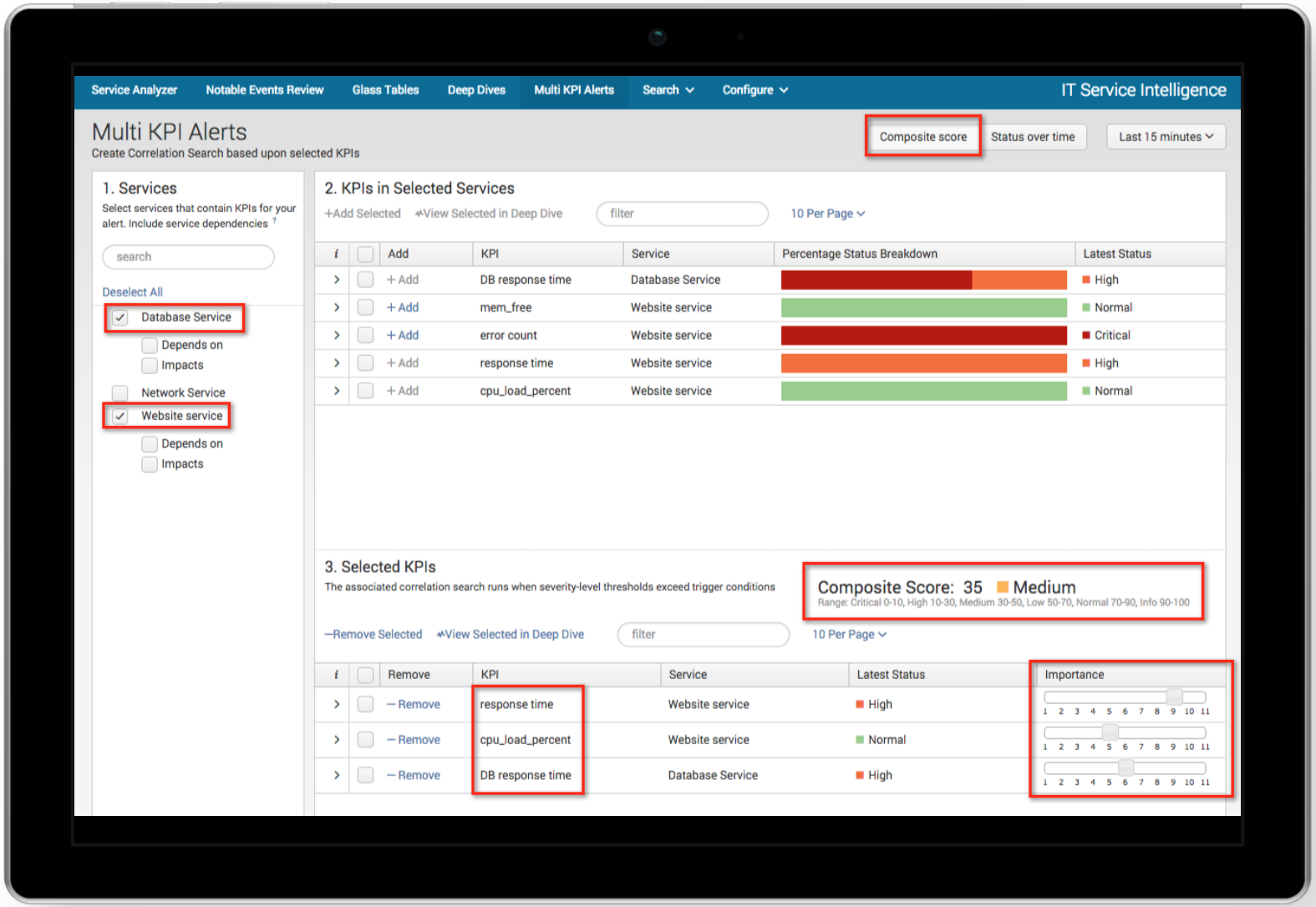
Demo

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 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.

splunk> .conf18

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* Events

Description? Pull data into Notable Events

Search Type Data Model | Ad hoc

Search* index="sourcedata"

Run Search

Time range Last 1 minute

Association

Service Select service(s)

Entity Lookup Field?

Schedule

Schedule Type Basic | Cron

Run Every minute

Notable Events

Notable Event Title?* %message%

Notable Event Description? %message%

Owner? unassigned Advanced Mode
In advanced mode, use tokens like %fieldname% to use result field values to set owner

Severity? Info Advanced Mode
In advanced mode, use tokens like %fieldname% to use result field values to set severity

Status? New Advanced Mode
In advanced mode, use tokens like %fieldname% to use result field values to set status

Drill-down Name? Test1

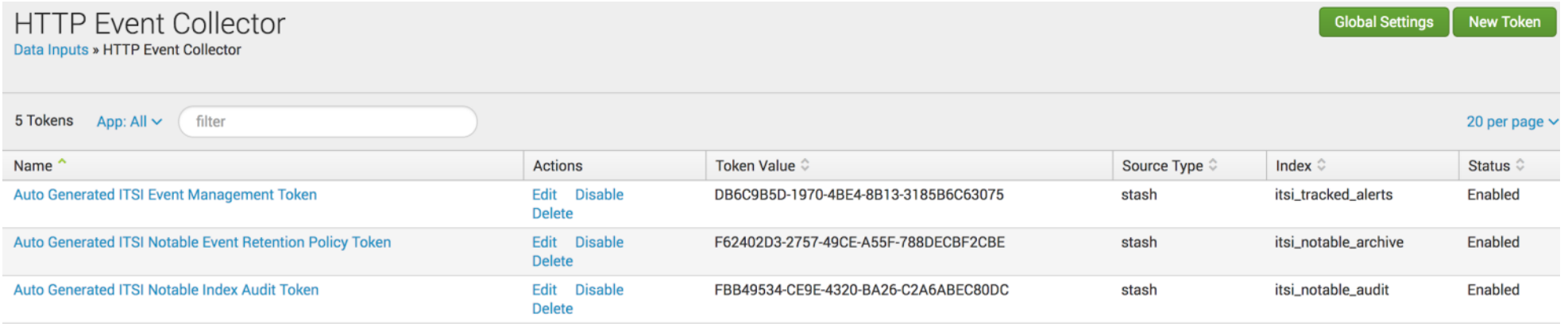
Drill-down Search? index="sourcedata"

Drill-down earliest offset? Last 5 minutes

Drill-down latest offset? Next 5 minutes

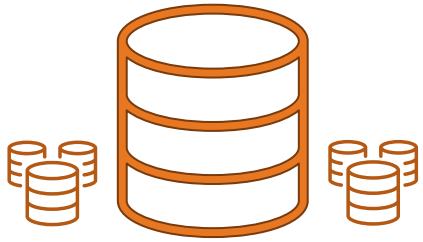
Getting Data in (HTTP Event Collector)

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

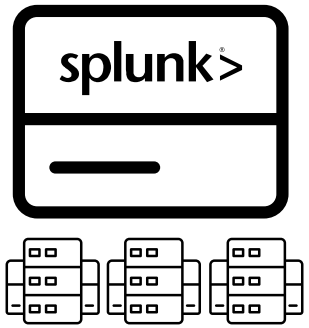


  - Need to generate GUID for event ID
  - curl -k https://localhost:8088/services/collector/event -H "Authorization: Splunk DB6C9B5D-1970-4BE4-8B13-3185B6C63075" -d '{"event" : {"event_id" : "d65600d-8669-4903-8a14-af88203add38", "title" : "Disk 90% Full", "status" : "4", "severity" : "6", "owner" : "unassigned",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

Common Data Onboarding Use Case



Persistent Storage



Core Splunk

(Correlation Search → HEC)

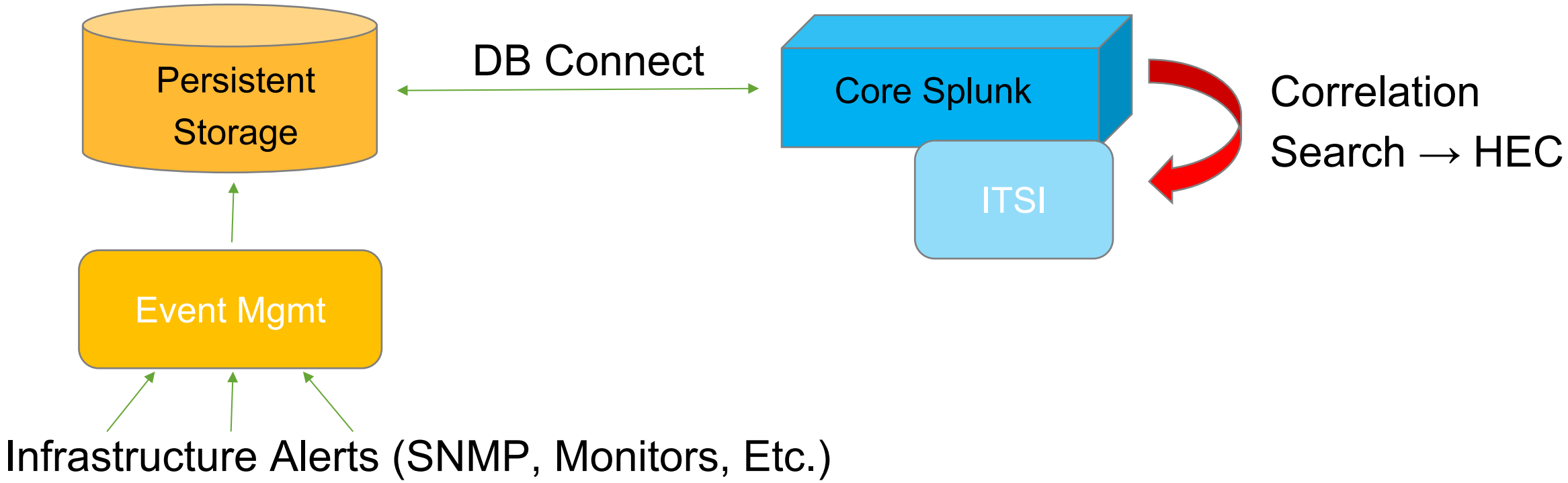
Event Management

Splunk IT Service Intelligence™

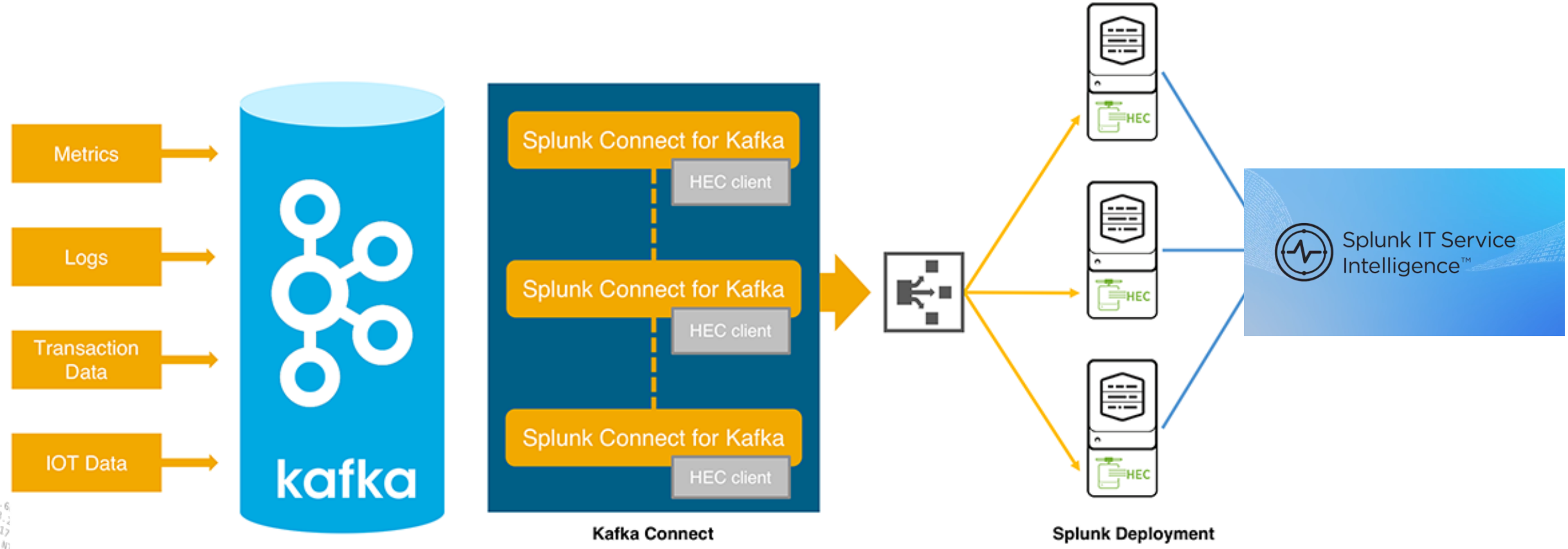
Infrastructure Alerts

(SNMP, Monitors, Etc.)

Common Data Onboarding Use Case



Large Scale Telco Data Pipeline



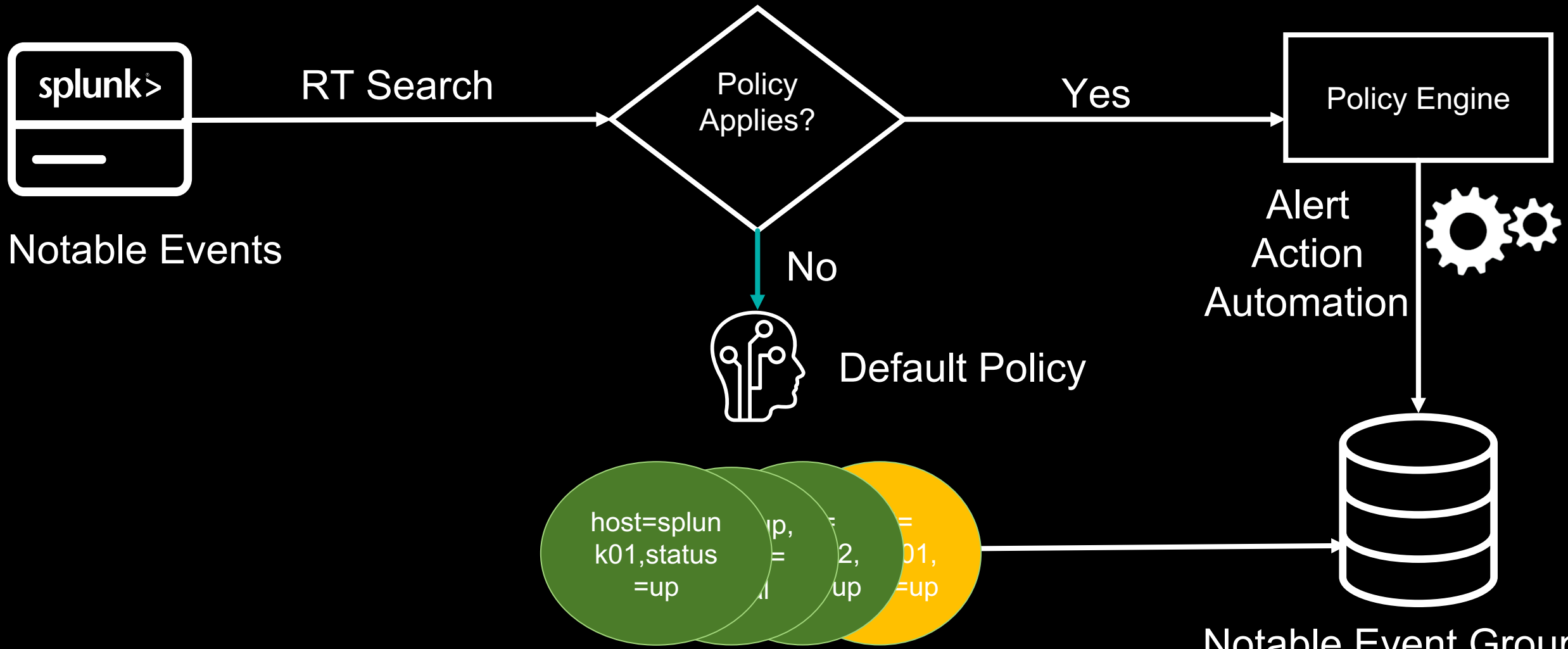
Event Reduction

- 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!



Common Operations Flow

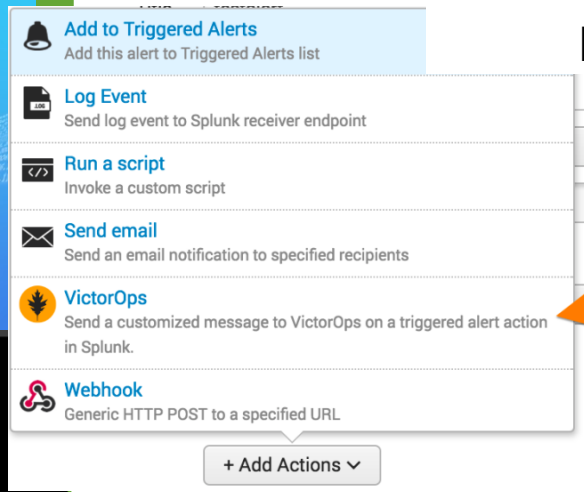
Monitor

Detect/Analyze

WHY

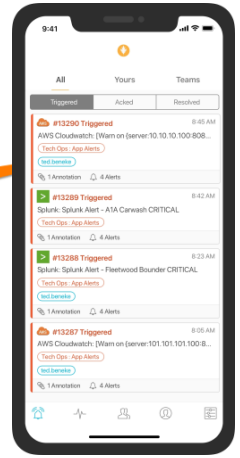
Splunk IT Service Intelligence™

splunk>



ITSM

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



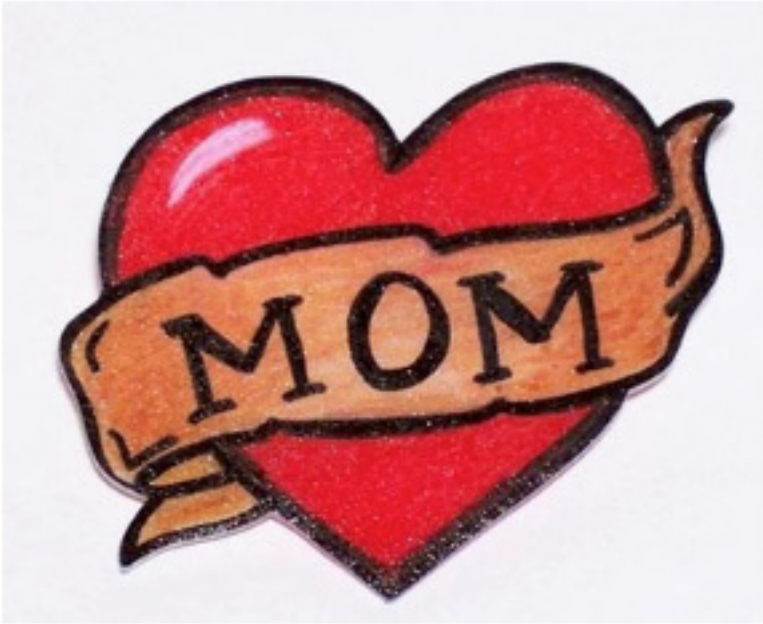
On Call Management
Routing/Notification Preferences
Mobile Interface
Escalation

Implementations

Let’s talk about making all this stuff work

Review Existing MoM Architecture

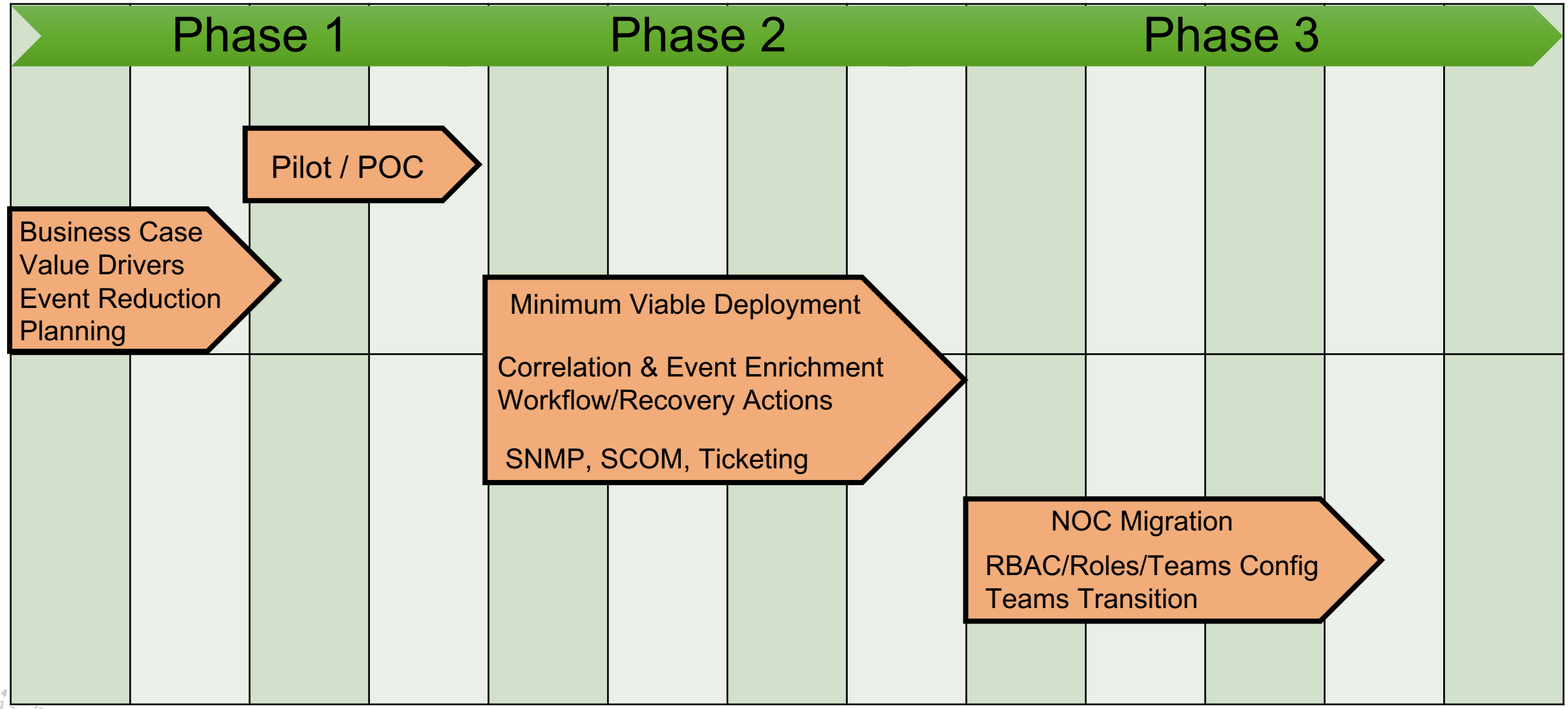
- What DataSources do exist?
  - SNMP (Traps, Polling)
  - Performance Monitoring
  - 3rd Party Monitoring Packages
- Event Aggregation/Correlation
  - How complex are the rules
  - Event Suppression (Maintenance Windows, Deduplication)
- Reporting Gateways?
  - Ticketing Integration into Service Management Tools



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

High Level Timeline



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

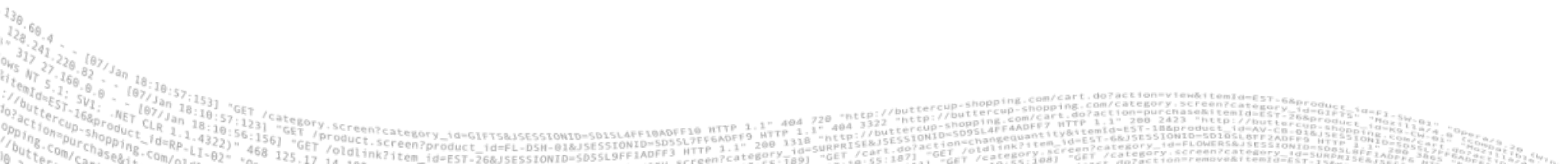
- Change Aggregation Policies to Real Time
  - http://docs.splunk.com/Documentation/ITSI/3.1.4/User/Managenotableeventindexes#Notable_event_real-time_search_optimization
- Adjust timeframe for Notable Event Console
- Publish pre-built views for different Operations Teams

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 Analystics” 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**