© 2017 SPLUNK INC.

splunk> .conf2017

# An Enterprise as Nimble as a Fighter Jet

## Building the Instrumented Enterprise at Lockheed Martin

Robert Frazier | Senior Manager for Cyber Architecture

Date | Washington, DC

© 2017 SPLUNK INC.

# 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. © 2017 Splunk Inc. All rights reserved.

splunk> .conf2017

© 2017 SPLUNK INC.

# Introduction

- What is an instrumented enterprise?
- How we started out
- Hurdles to Implementation
- Building the Instrumented Enterprise
- Digital Transformation

splunk> .conf2017

© 2017 SPLUNK INC.

# What is an Instrumented Enterprise?

SPAD VII (single logs)

Modern Aircraft (Splunk >)

splunk> .conf2017

© 2017 SPLUNK INC.

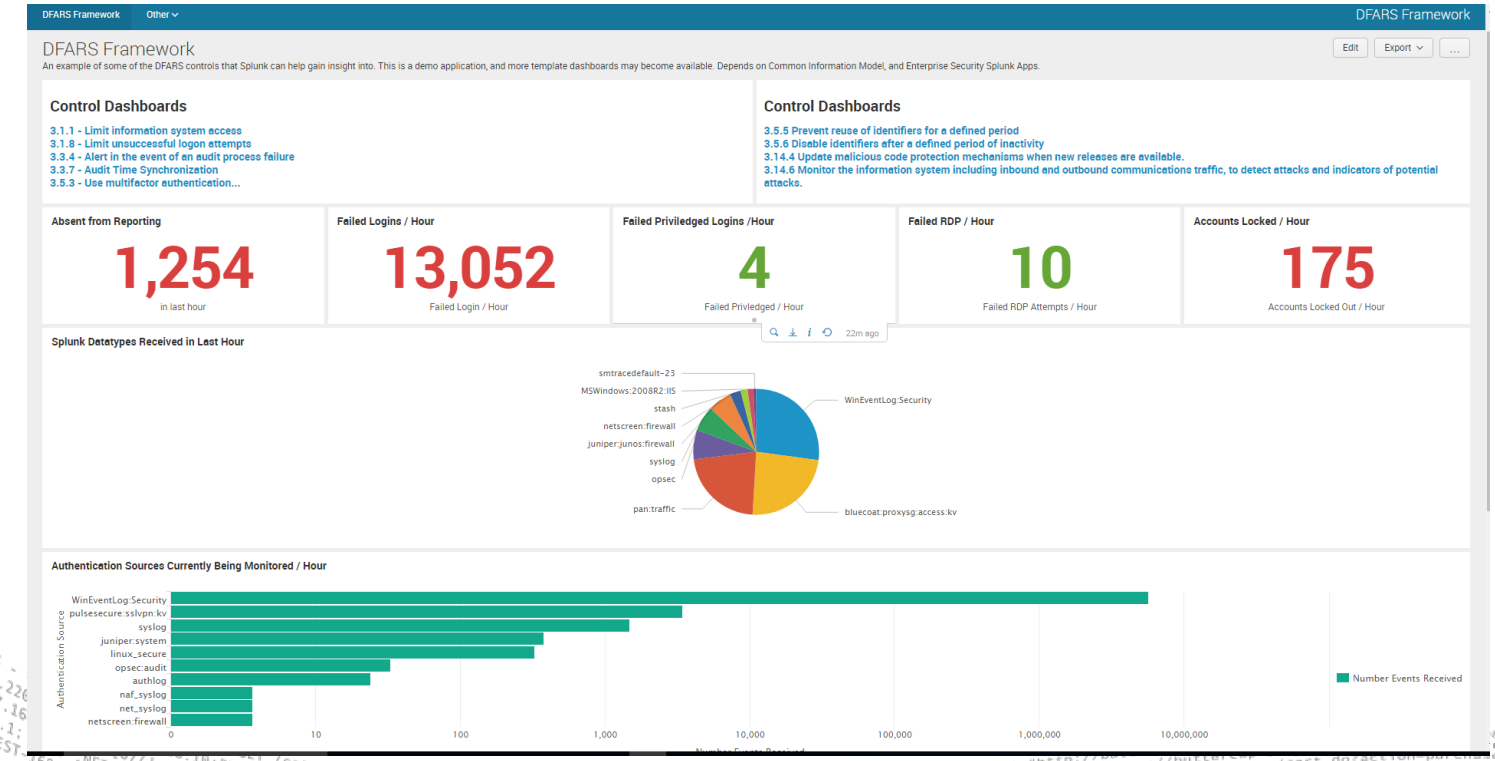
# In the beginning....

- Splunk for logging
- Core Splunk for security correlation
- F-35 program (https://www.splunk.com/blog/2015/04/08/splunk-lockheed-f-35-lightning.html)

© 2017 SPLUNK INC.

# Then Came DFARS

- Systems with Defense Information had to be logged
- Data from logging started being useful in other areas
- Lockheed Martin Security became interested




Splunk logging and reporting became the choice for DFARS compliance

splunk> .conf2017

© 2017 SPLUNK INC.

# Lockheed Martin CIRT

- World Famous Lockheed Martin Computer Incident Response Team (CIRT)
- Cyber Kill Chain
- Laika Boss
- International Reputation as a Security Thought Leader

**What could Splunk do to support top gun security?**

© 2017 SPLUNK INC.

# Splunk and Expanding the Knowledge Base

- Greater breadth of insight from broader range of collection
- More data points, more data correlation
- Splunk and CIRT tools side by side, greater insight
  - FISMA App
  - Machine Learning Tool Kit
  - Apps from Splunkbase
  - Home Grown Apps
- Splunk ES (under construction)
- **Splunk as a force multiplier**

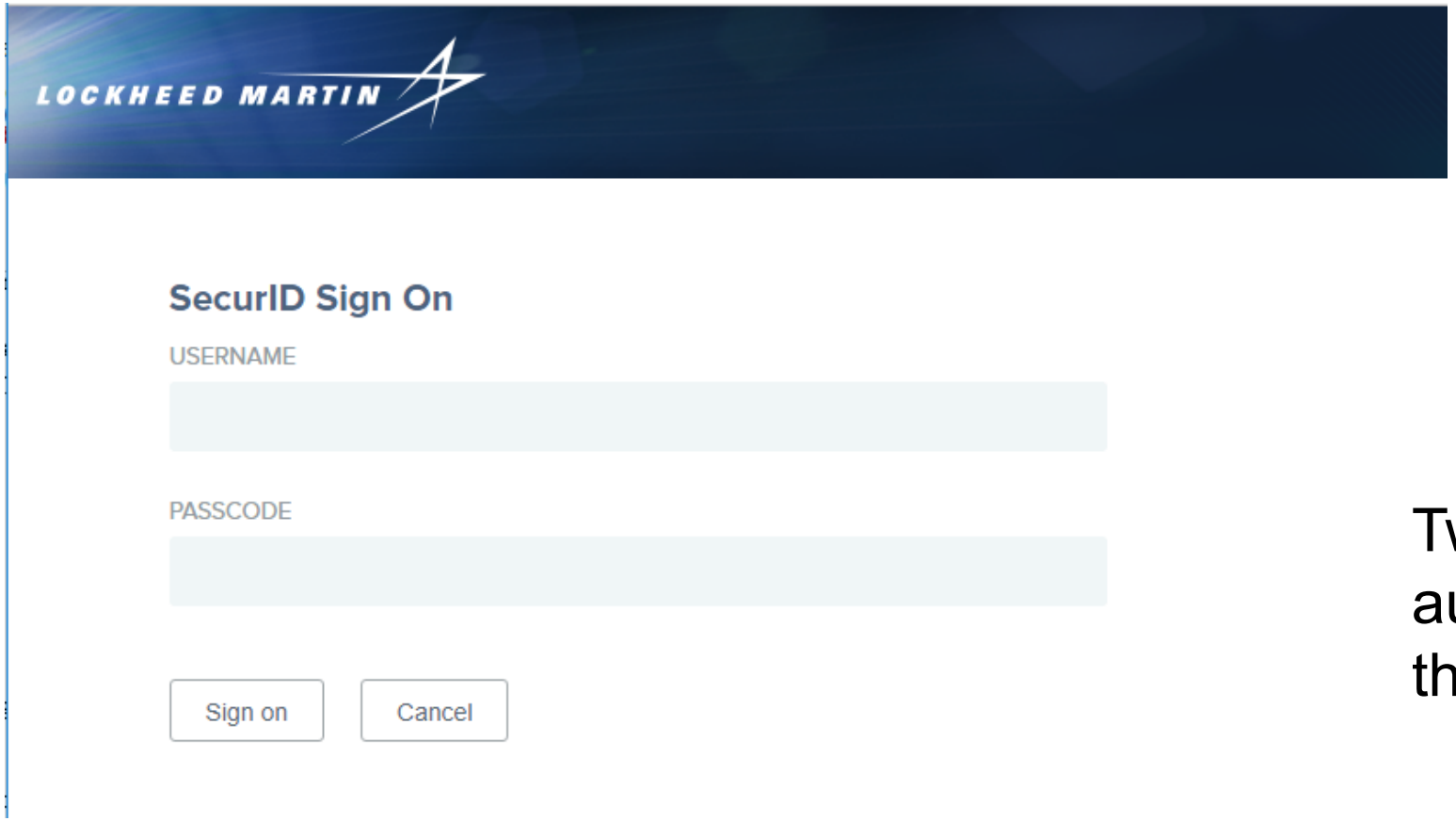
© 2017 SPLUNK INC.

# Organizational Issues

- Who pays for what?
- Who owns the data?
- Who controls access to Indexes?
- Who decides?

© 2017 SPLUNK INC.

# Two Factor Authentication




Two Factor authentication to access the search heads

splunk> .conf2017

© 2017 SPLUNK INC.

# Who pays for what?

- Several Options
  - Use charge back system (cumbersome overhead)
  - Use licensing pools (distribute the per day license overrun risks)
  - Limit usage (innovation killer)
- Use per-seat tax
  - Providing IT services on a per seat basis (email, network, office applications, etc.)
  - Encourages “citizen data scientists”
  - Control data ingest at the Splunk administrator level
- Unlimited License
  - True up at end of the year (budget uncertainty, but encourages innovation)

© 2017 SPLUNK INC.

# Who owns the data?

- Splunk service owner ultimately owns all indexes and data
- Data generators, i.e. network, server, manufacturing, etc. co-own their data

- Bigger question: What data do you want in Splunk?
  - What kinds of knowledge do you need from your data
  - What kinds of data will provide that kind of knowledge
  - How much is needed to be ingested? All of it? Extracts? Parts of the logs?

- Requires finesse between data generators and Splunk administrators to balance cost and benefits, remembering that what is not collected is lost.

© 2017 SPLUNK INC.

# Who controls access to Indexes?

- Privacy concerns
- Security data
- Proprietary data
- Control by Indexes
  - Create user roles and access to indexes
  - Some roles may need access to all indexes (Security)
  - Other roles can be limited (just network, just manufacturing, etc.)
  - What indexes can your Apps see/use?
- Good Index, data, and knowledge object management helps control costs, indexing/search performance, etc.

© 2017 SPLUNK INC.

# Who decides?

- Organizational issue
- Splunk Drawback:  Easy to use and set up and get started
- Gartner:  develop a corporate data plan, collect data, choose analytics tool
- Which approach is more rational?
- Which do you think will be accomplished faster?

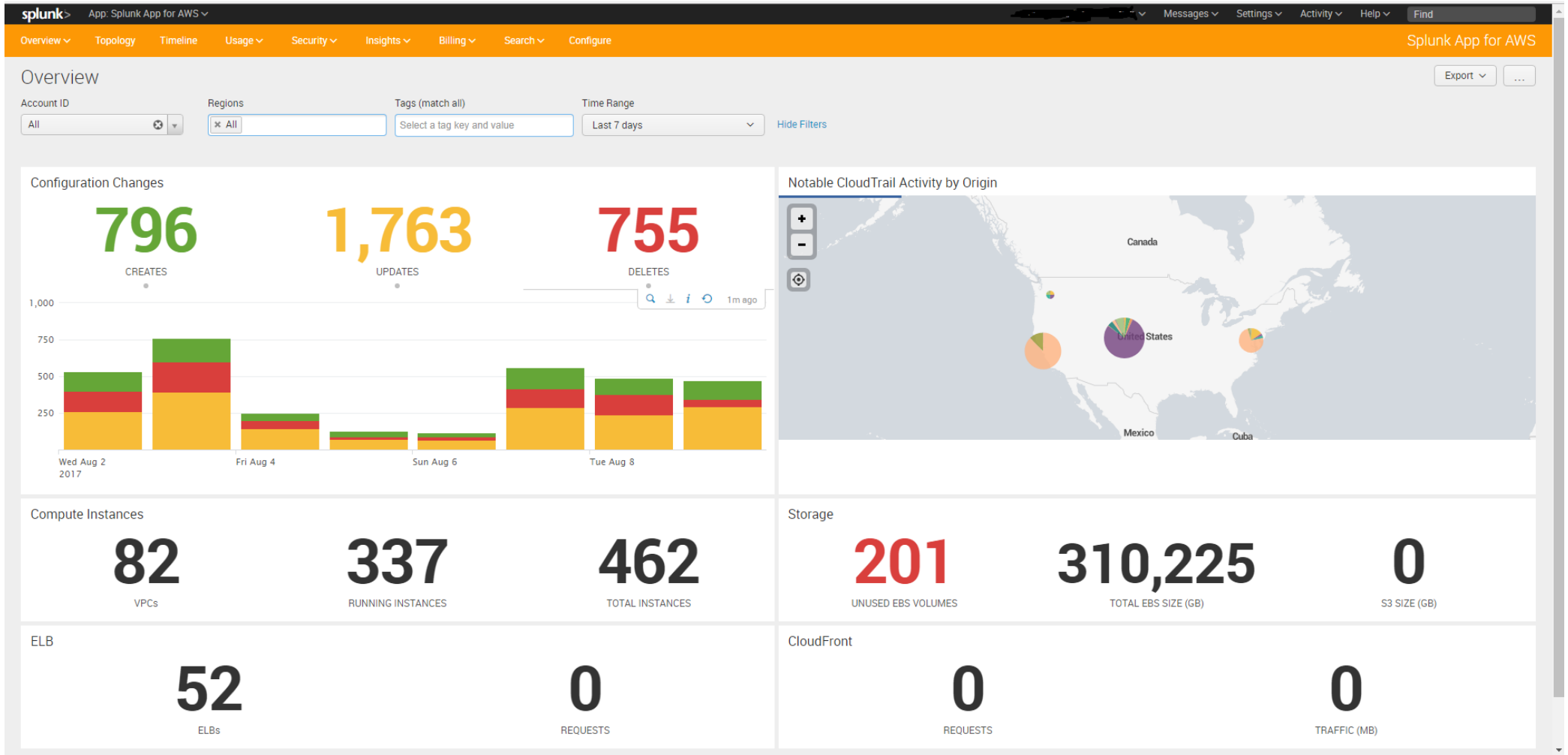
© 2017 SPLUNK INC.

# Splunking the Enterprise

- AWS (Government)
  - Splunk for AWS to manage our cloud infrastructure
  - Splunk is also on AWS
  - Used the AWS App and Splunk to look for ethereal machines and compliance
- Network
  - Manage network traffic and operations
  - Significant savings from mean-time to resolution, efficient use of resources, etc.
- ITSI
  - Newest installation
  - Under development to manage service infrastructure and supported business processes

© 2017 SPLUNK INC.

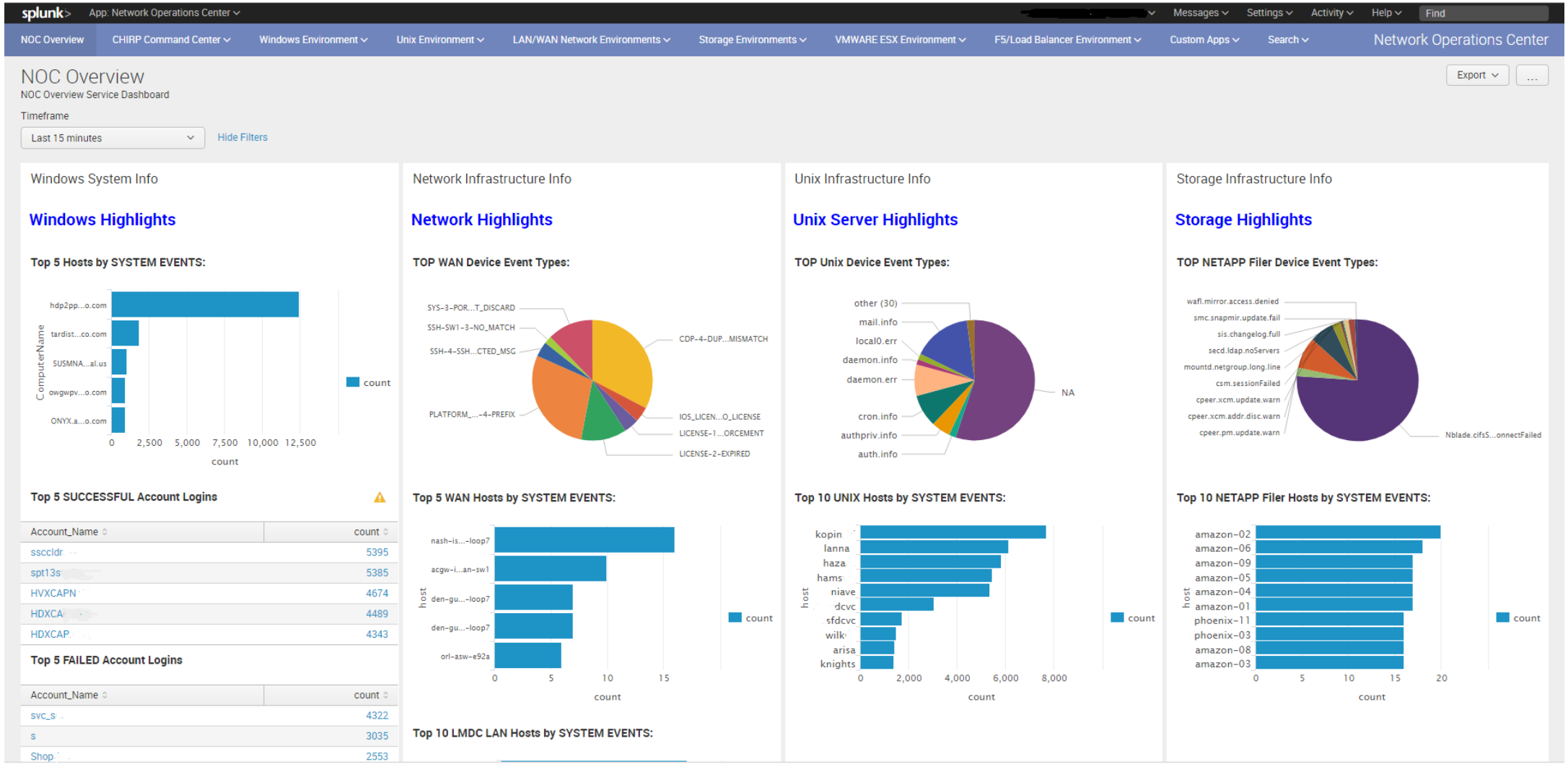
# AWS and Splunk




splunk> .conf2017

© 2017 SPLUNK INC.

# Network and Splunk




splunk> .conf2017

© 2017 SPLUNK INC.

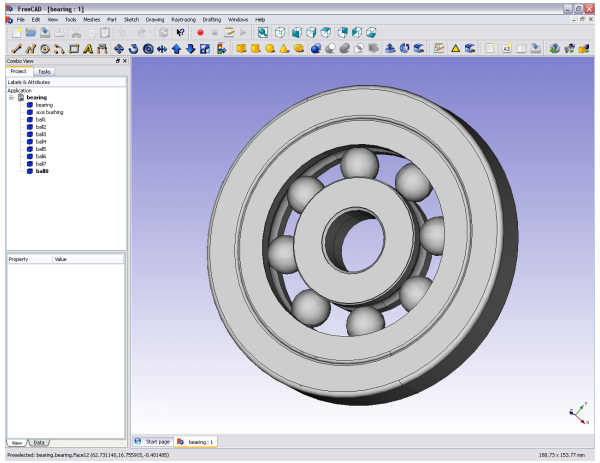
# Splunk is a data platform, not tool.

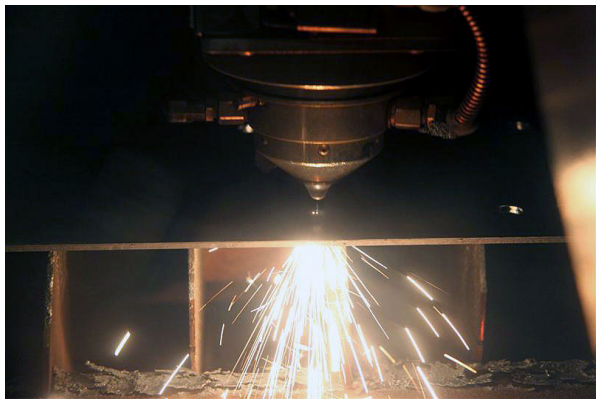
- Start small, plan for big, then expand.
- Like chess, keep planning two or three moves ahead
- Splunk **WILL** grow and expand. (You can quote me)

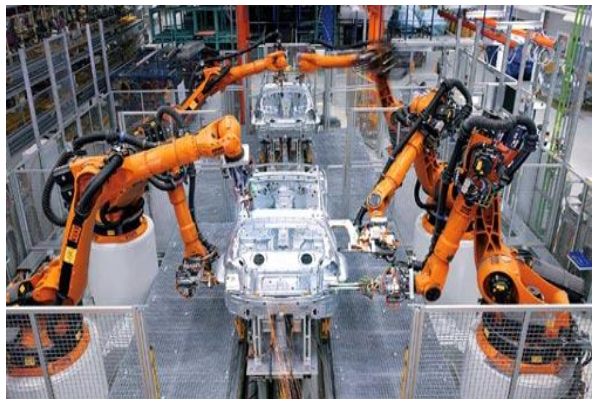
© 2017 SPLUNK INC.

# Digital Transformation

- Data is Essential to Digital Transformation
  - Digital manufacturing
  - From Art to Part
  - Internet of Things
  - Operational Technology





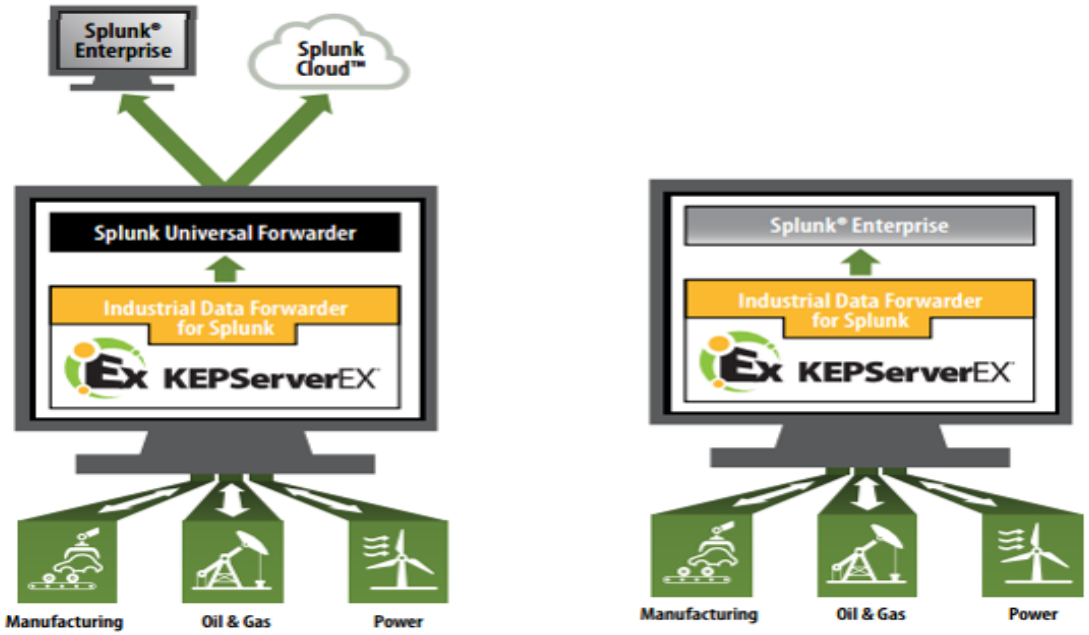


splunk> .conf2017

© 2017 SPLUNK INC.

# Expanding the Knowledge Base

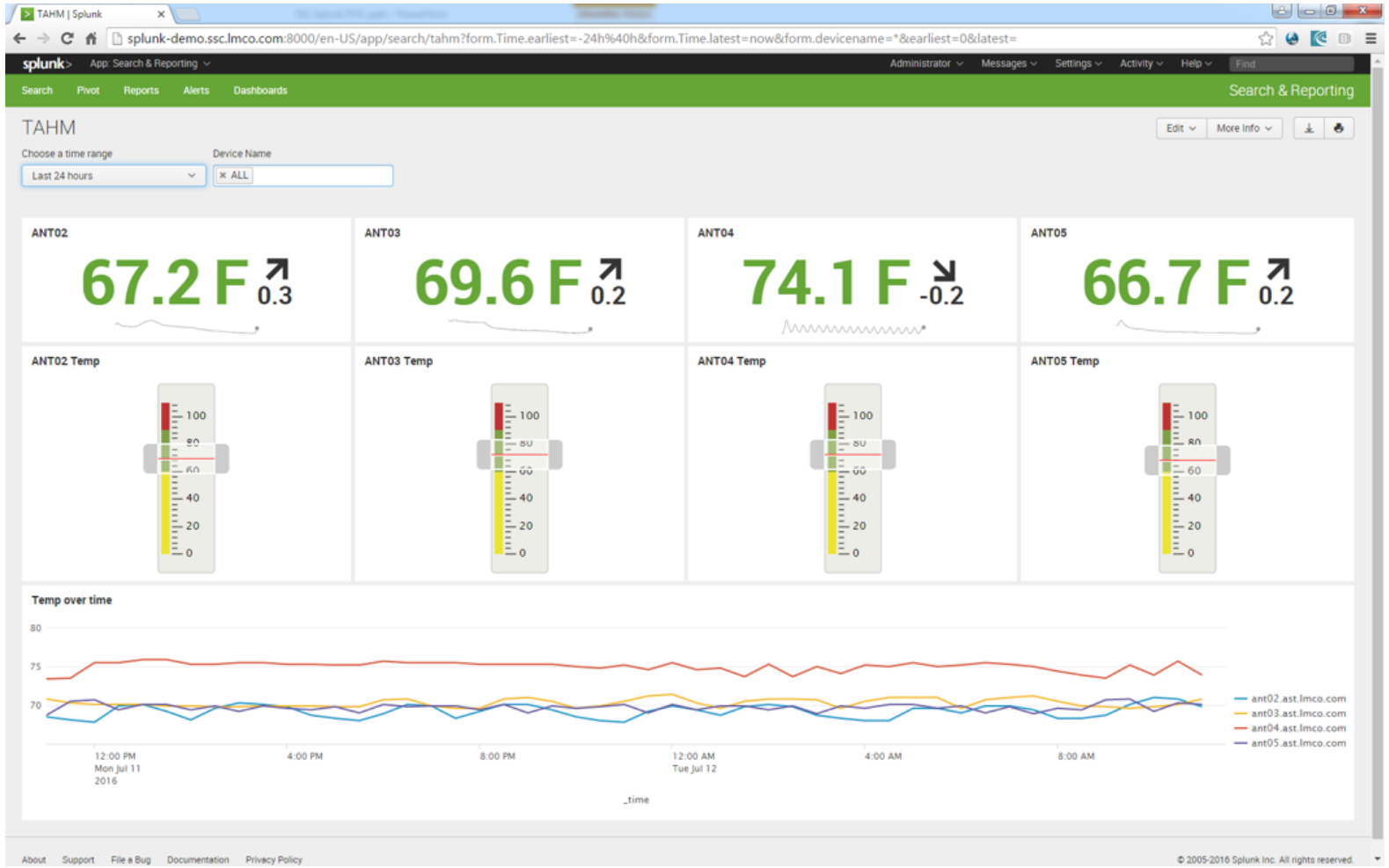
- Getting data from OT systems
- Using data from manufacturing to be more secure, plan for digital resiliency
- Using data to manufacture better, smarter




splunk> .conf2017

© 2017 SPLUNK INC.

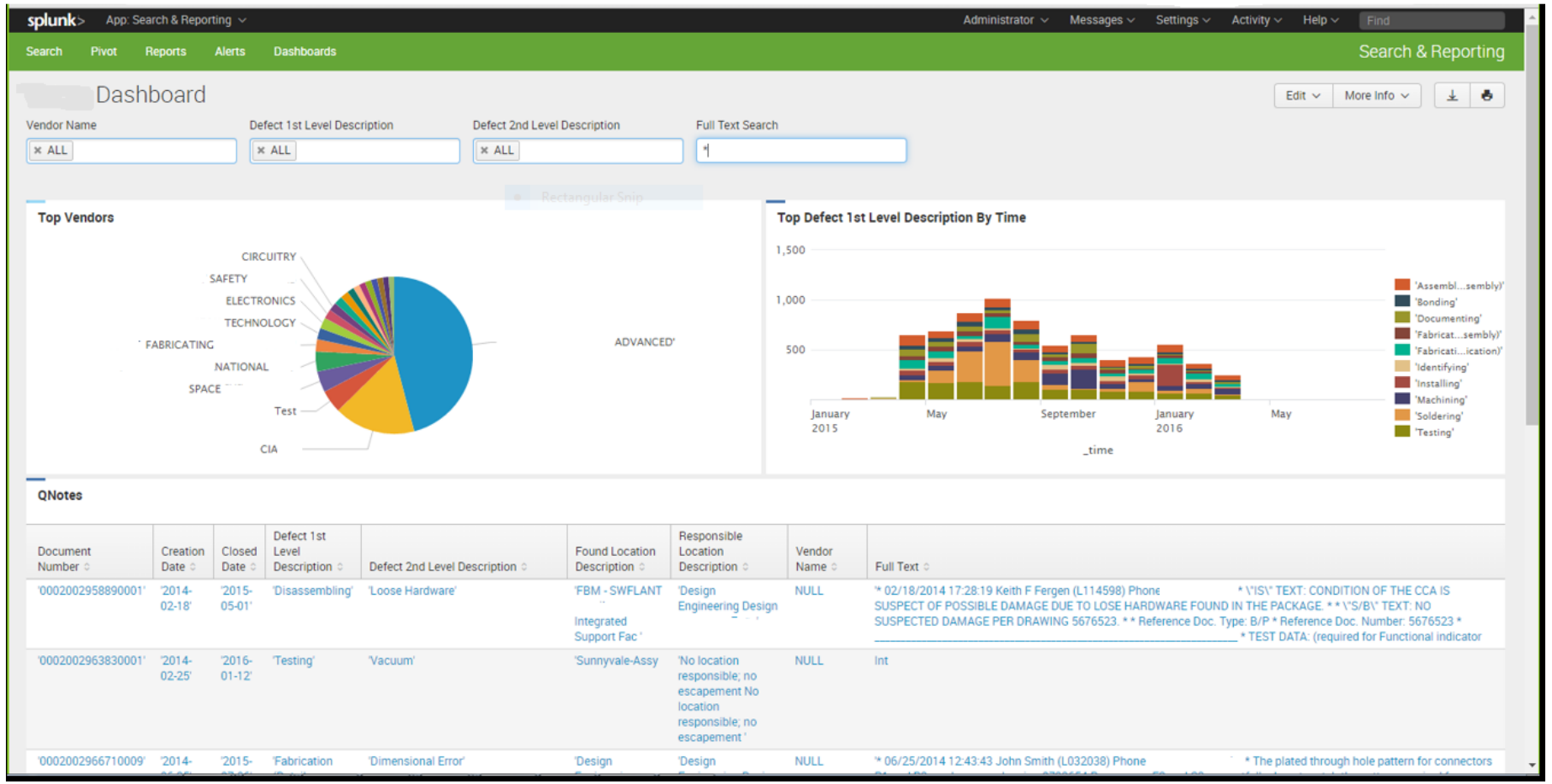
# Tracking Autoclave Temperatures




splunk> .conf2017

© 2017 SPLUNK INC.

# Tracking Quality




splunk> .conf2017

© 2017 SPLUNK INC.

# The Instrumented Enterprise

- Expand knowledgebase to all aspects of the business
- Supply chain to sustainment, from shop floor to the sky
- Collect and use data to be secure, efficient, nimble
- Digital transformation requires transforming your thinking, your organization as well as transforming  your data

© 2017 SPLUNK INC.

- The P-38 Lightning was a fighter of the “Greatest Generation”
- The F-35 Lightning II is the fighter of the “Next Generation”

Splunk is the platform for Lockheed Martin to build a next generation enterprise to respond to digital transformation, emerging cyber threats, and agile operations by striving to be nimble as a fighter jet.

© 2017 SPLUNK INC.

# To get to a new place, start from a new place.

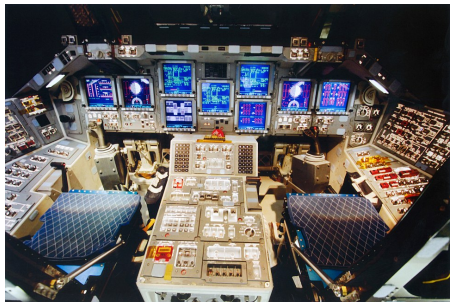
- "If your want to **change the world**, first **change yourself**" – Leo Tolstoy
- We are changing how we look at data, our organization, and ourselves
- Splunk is helping change our enterprise to be as nimble as a fighter jet

F-35 Lightning II

F-22 Raptor

C-130

UH-60 Blackhawk



Orion Spacecraft

© 2017 SPLUNK INC.

# Questions


- Rob Frazier
- robert.p.frazier@lmco.com

splunk> .conf2017