splunk> .conf2017

# Surprise and Consequences

## Breaking through Analysis Paralysis

Joel M. Fulton, PhD | Chief Information Security Officer @ Splunk
Grant Wernick | Chief Executive Officer @ Insight Engines

September 26, 2017

TURNING DATA INTO ANSWERS

# Agenda

| | |
|---|---|
| **Patterns of Analysis Failure** | Joel M. Fulton, Splunk CISO |
| **Demo Cyber Security Investigator** | Grant Wernick, Insight Engines CEO |
| **Applying CSI, Achieving Excellence** | Joel M. Fulton, Splunk CISO |
| **Next gen Intelligence Augmentation** | Grant Wernick, Insight Engines CEO |
| **Q&A** | |

# Joel Fulton

SPLUNK CISO

splunk> .conf2017

# Security Intelligence Operations


splunk> .conf2017

# Where do we rock?

- Playbooks, workflows, automated ticketing
- Ingestion
- Pattern matching
- Incident investigation
- Rudimentary digital forensics
- Cross-platform analysis and investigation

# What are we embarrassed about?

- Data completeness
- Thinking like an analyst
- Accurately prioritized and weighted alerting and triage
- Percentages and judgment calls
- The boy who cried wolf: too much or not enough warning?
- Being surprised.

# What's the purpose of intelligence?

- Buy time in order to make the appropriate decisions and take the necessary counter measures to face the threat

- Assume invulnerability, deny danger
- Underestimate hazard
- Over-estimate resiliency

**The analyst's rule: don't speak to clearly or precisely about the future. When pressed to do so, lower the probabilities.**

Ambiguous warnings protect the individuals but are useless to protect the entity

# Grant Wernick

INSIGHT ENGINES CEO

# Darien Kindlund

INSIGHT ENGINES VP TECHNOLOGY

splunk> .conf2017

# Insight Engines Cyber Security Investigator (CSI)

splunk> .conf2017

# Splunk SPL

If you want to know what vulnerable systems had failed updates

## Construct SPL like this…

```
| tstats allow_old_summaries=t append=t prestats=t summariesonly=t count values(Updates.severity) as Updates.severity from
datamodel=Updates where Updates.status="failure" earliest=06/20/2016:00:00:00 latest=06/27/2016:00:00:00 by Updates.dest,
Updates.signature
  | tstats allow_old_summaries=t append=t prestats=t summariesonly=t count from datamodel=Vulnerabilities where
earliest=06/20/2016:00:00:00 latest=06/27/2016:00:00:00 by Vulnerabilities.dest
  | fillnull value="" Updates.signature
  | eval dest=coalesce('Updates.dest', 'Vulnerabilities.dest'), join_node=if(isnotnull('Updates.dest'), "Updates", "Vulnerabilities")
  | stats count values(Updates.severity) as Updates.severity by dest, join_node, Updates.signature
  | eval count_Updates=if(join_node=="Updates", 'count', null()), count_Vulnerabilities=if(join_node=="Vulnerabilities", 'count', null())
  | stats list(count_Updates) as count_Updates list(Updates.signature) as Updates.signature list(count_Vulnerabilities) as count_Vulnerabilities
values(Updates.severity) as Updates.severity by dest
  | where isnotnull('count_Updates') AND isnotnull('count_Vulnerabilities')
  | stats sum(count) as count
```

# Plain English Search

If you want to know what vulnerable systems had failed updates

**Ask something like this…**

"Show me vulnerable systems with failed updates"

splunk> .conf2017

# The World With CSI

## Before—SPL

- Limited value from Splunk
- Weakened security posture
- Limited people can get insight
- Too much time spent on SPL
- Hard to find/train/retain SPL experts

## After—CSI

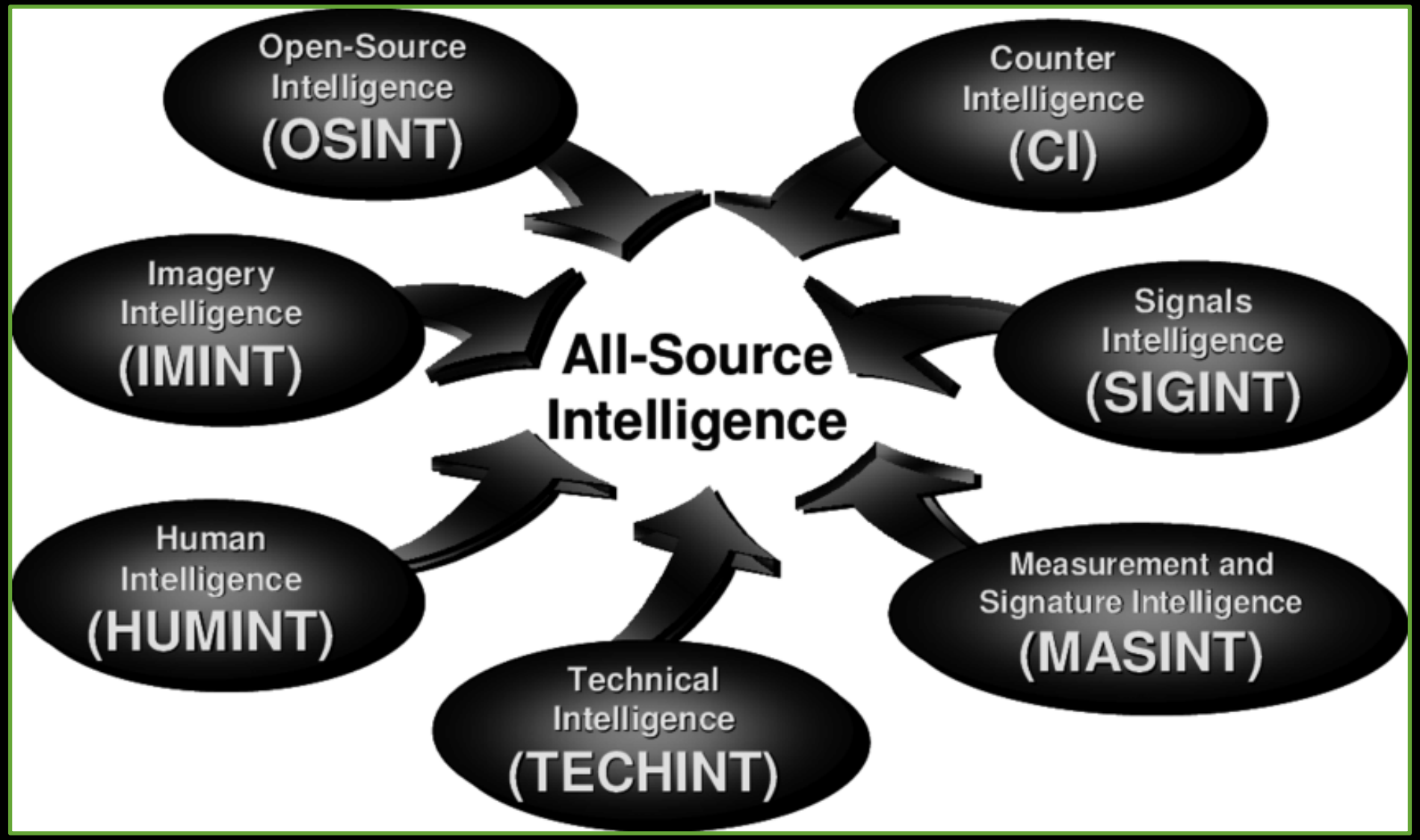
- Full value of Splunk
- Stronger security posture
- Data democratization
- More time investigating/detecting
- Less reliance on SPL expertise

# CSI Demo

Real time insight engine that understands plan English always learning

splunk> .conf2017

# Splunk + CSI + HUMINT + SIGINT = >SIO

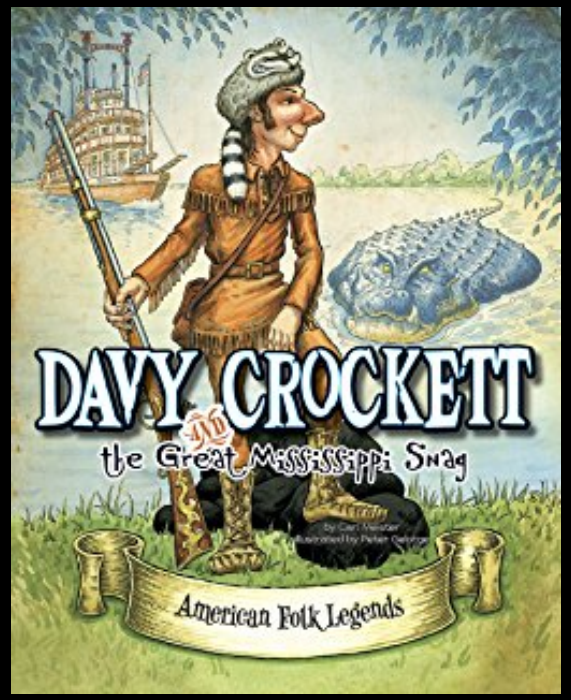


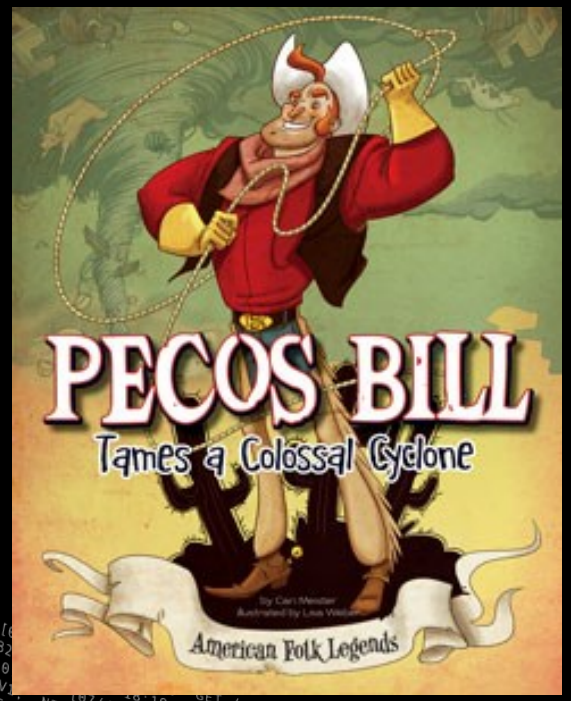

splunk> .conf2017

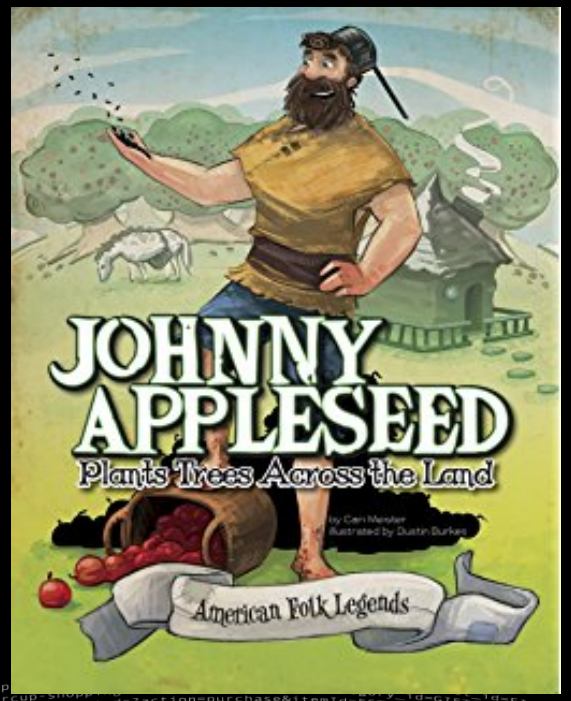
# Building a better Security Intelligence Operations

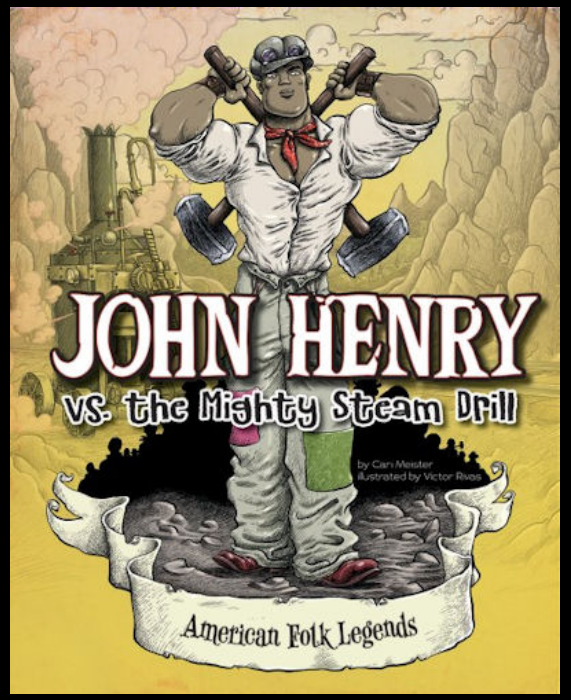
- There are no such things as cyber-only-risks
- All threats begin with people
- Cyber-analysts understand systems, data, and flow
- Human analysts understand people, motive, and the consequences of intent
- Every company has a physical security “SOC”
- If their HUMINT skills could be applied to SIGINT data, a radical transformation is possible

# Splunk + CSI + HUMINT + SIGINT = >SIO




splunk> .conf2017

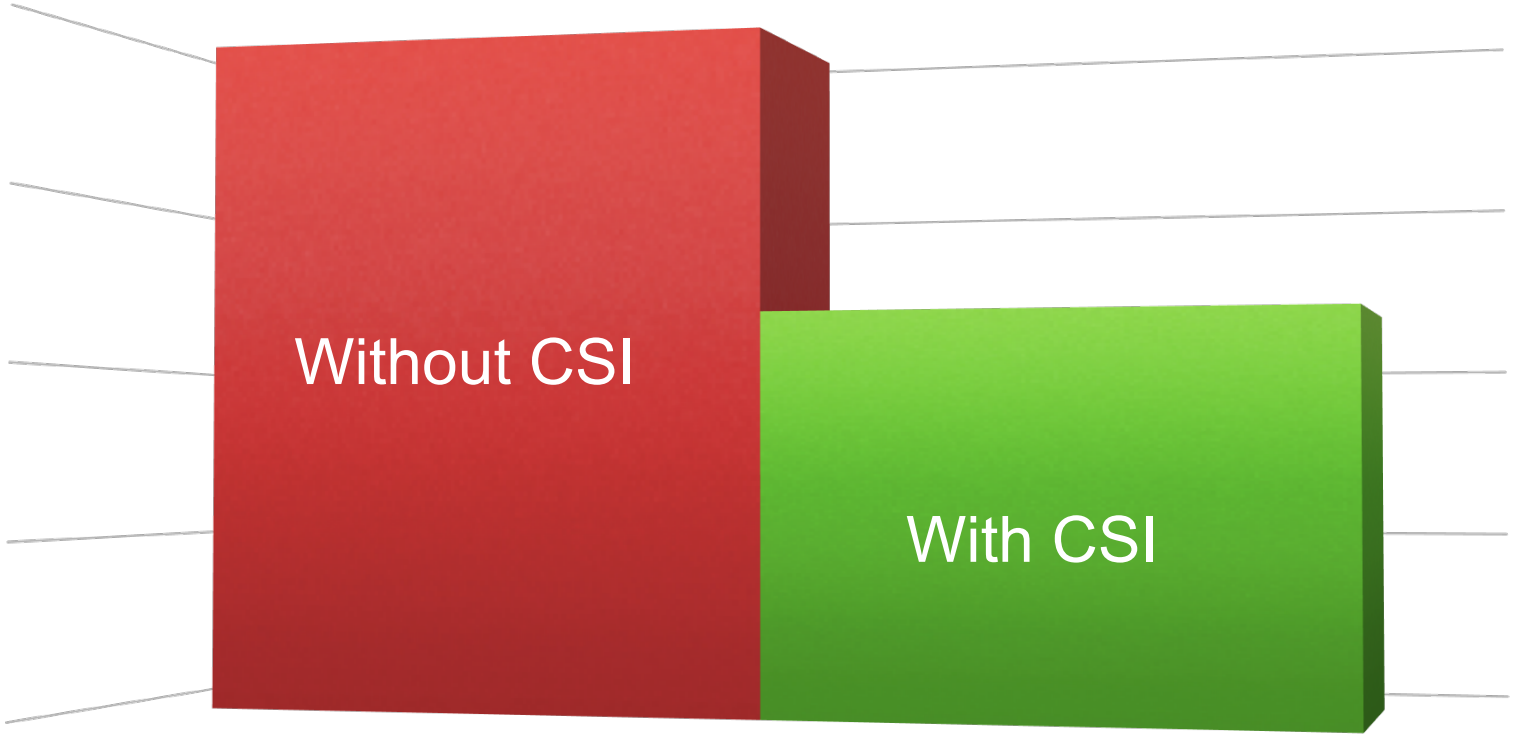
# Splunk + CSI + HUMINT + SIGINT = >SIO

splunk> .conf2017

# ROI By Enabling Physical Security Team

**$1MM** in savings per year in hiring and training costs

- 40% SOC Analyst Increased Productivity
- 60% Physical Security Analyst Productivity
- 80% Training Reduction




Annual Costs

*Based on enabling physical security team with CSI and hiring more physical security folks to become cyber analysts

# The Next Generation Analyst Workbench

Hands on Demo

splunk> .conf2017

# The Future

# Q&A

# Don't forget to rate this session in the .conf2017 mobile app

splunk> .conf2017