Find & Seek

Real-time Asset Discovery and Identity Attribution Using Splunk

Paul Johnson | Discovered Intelligence

October 2018 | Version 1.0

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> .conf18

About Me

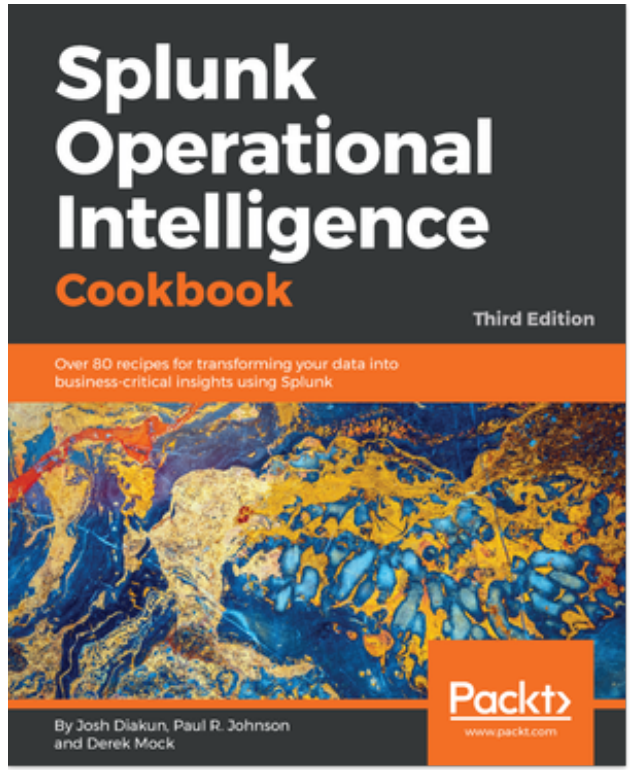
Who is this guy and what does he know?

Discovered Intelligence

www.DiscoveredIntelligence.ca

.conf10

FORTUNE 100 CUSTOMER



Agenda

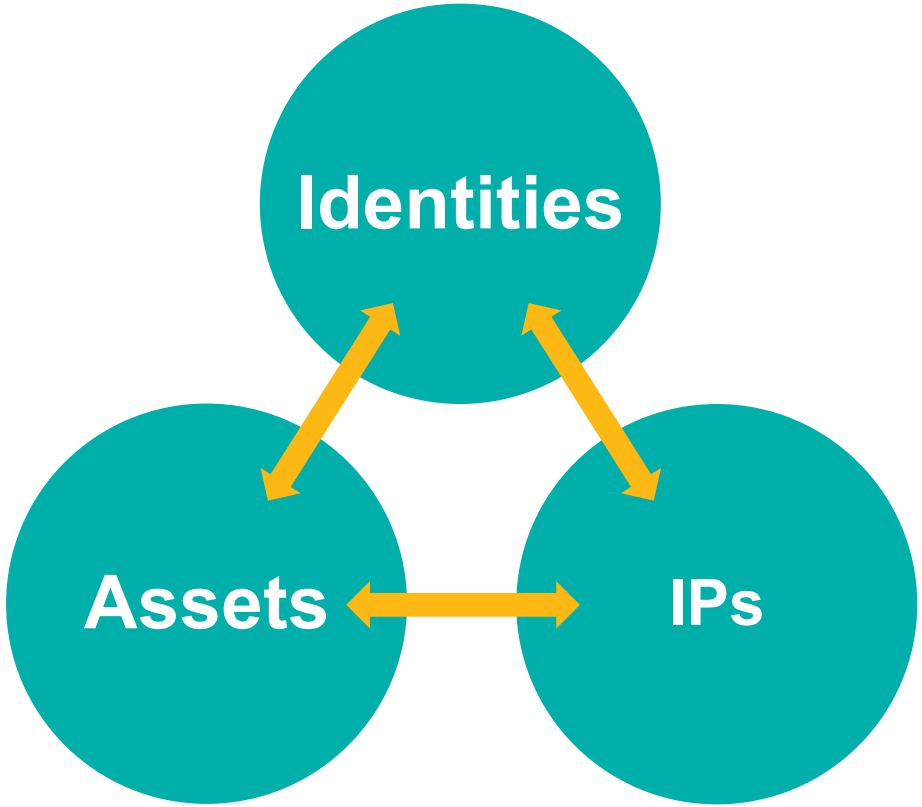
What are we going to talk about?

- Definitions
- The Asset Problem
- Taking a Different Approach
- Getting Started - Building a Simple Real-time Asset Inventory (+ demo)
- Going Further - Enriching the Data (+ demo)
- Going Even Further - Advanced Asset Intelligence (+ demo)
- Integration with Splunk ES (+ demo)
- Key Takeaways
- Q&A

Definitions

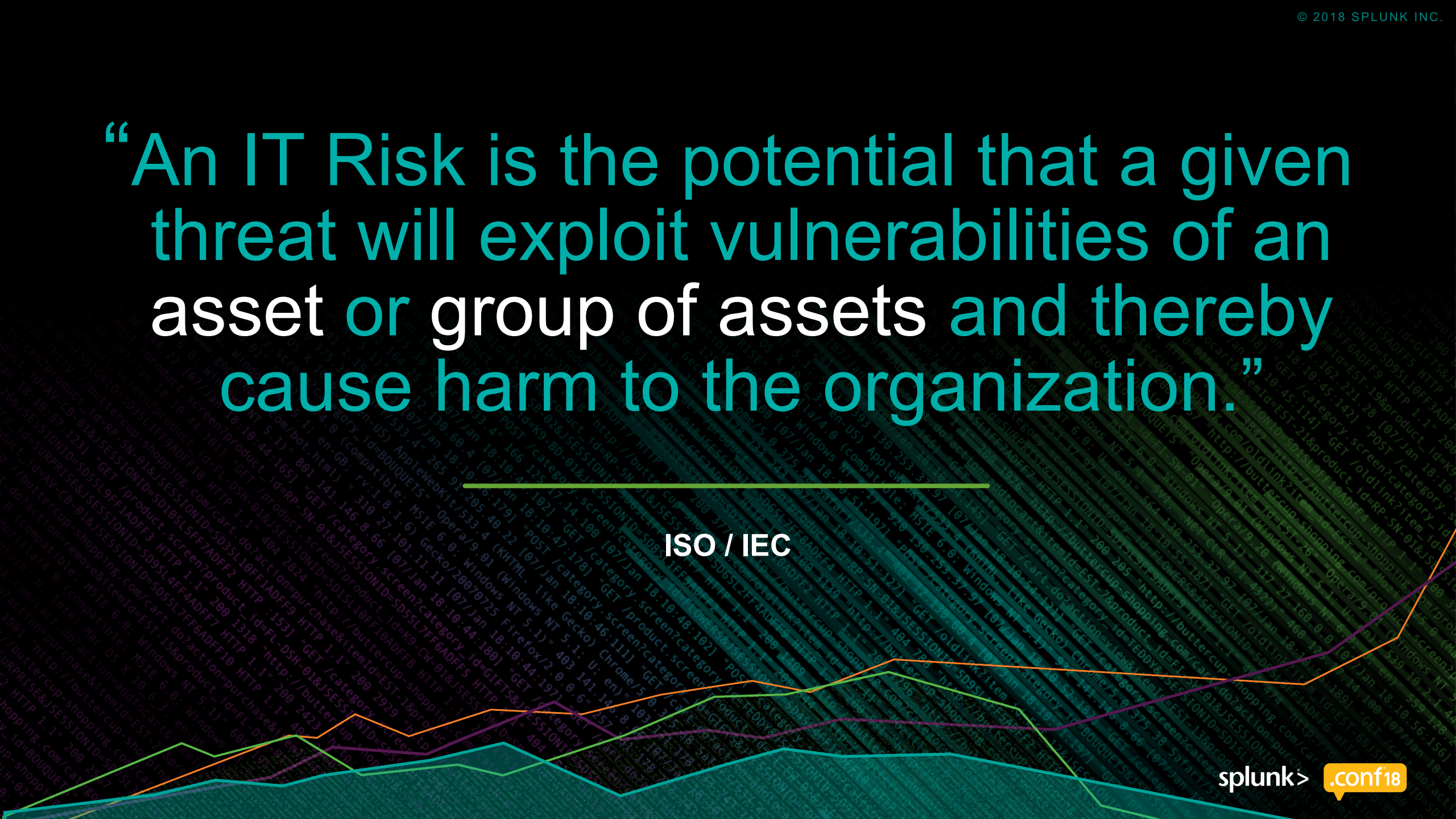
What does he mean?

- Asset
- Asset related data
- Identity
- Attribution
- Real-time
- Unmanaged



"An IT Risk is the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization."

ISO / IEC



The Asset Problem

What's wrong with the way we do it today?

- Operational focus
- Stale
- Incomplete or inaccurate
- Multiple sources of record
- BYOD and IoT

"In big corporate networks, up to 20% of the entire network is unmanaged"

Gartner

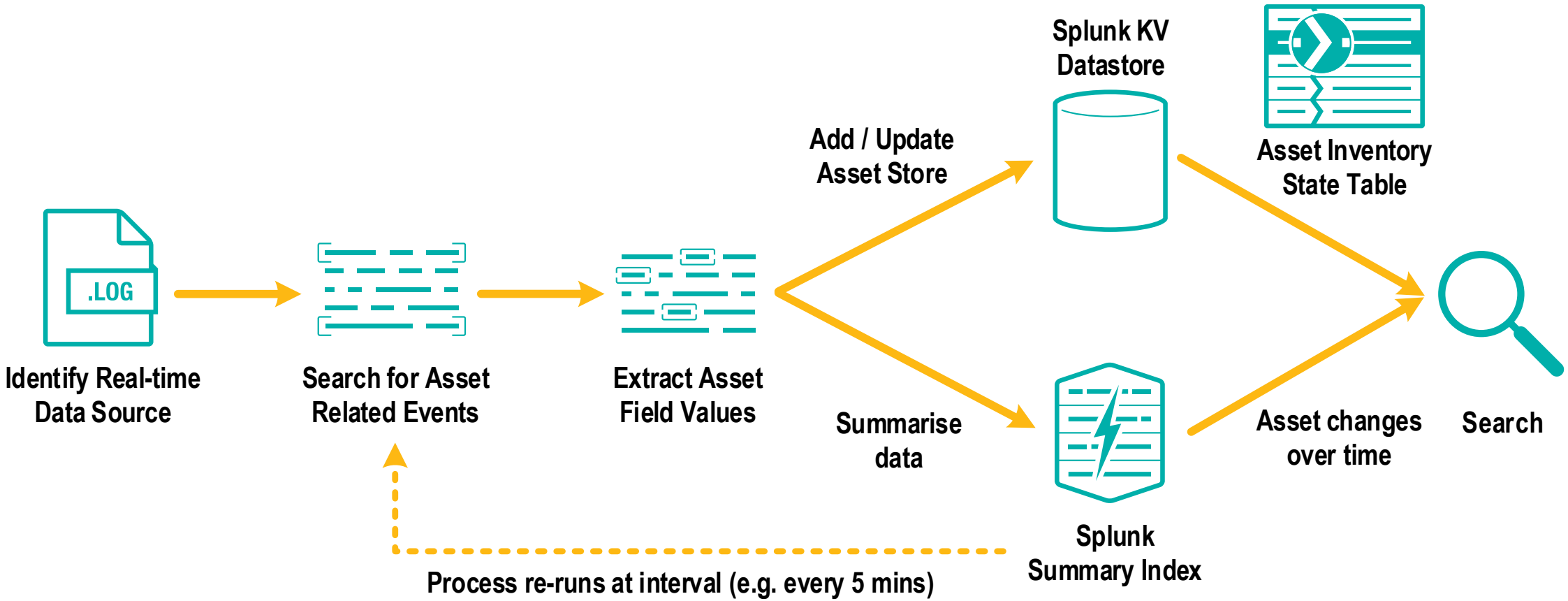
Taking Different Approach

What can we do differently?

- Leverage real-time data
- Correlate and enrich
- Track changes over time
- Apply data driven intelligence
- Increase accuracy and visibility

Building a Simple Real-time Asset Inventory

How do we get started?



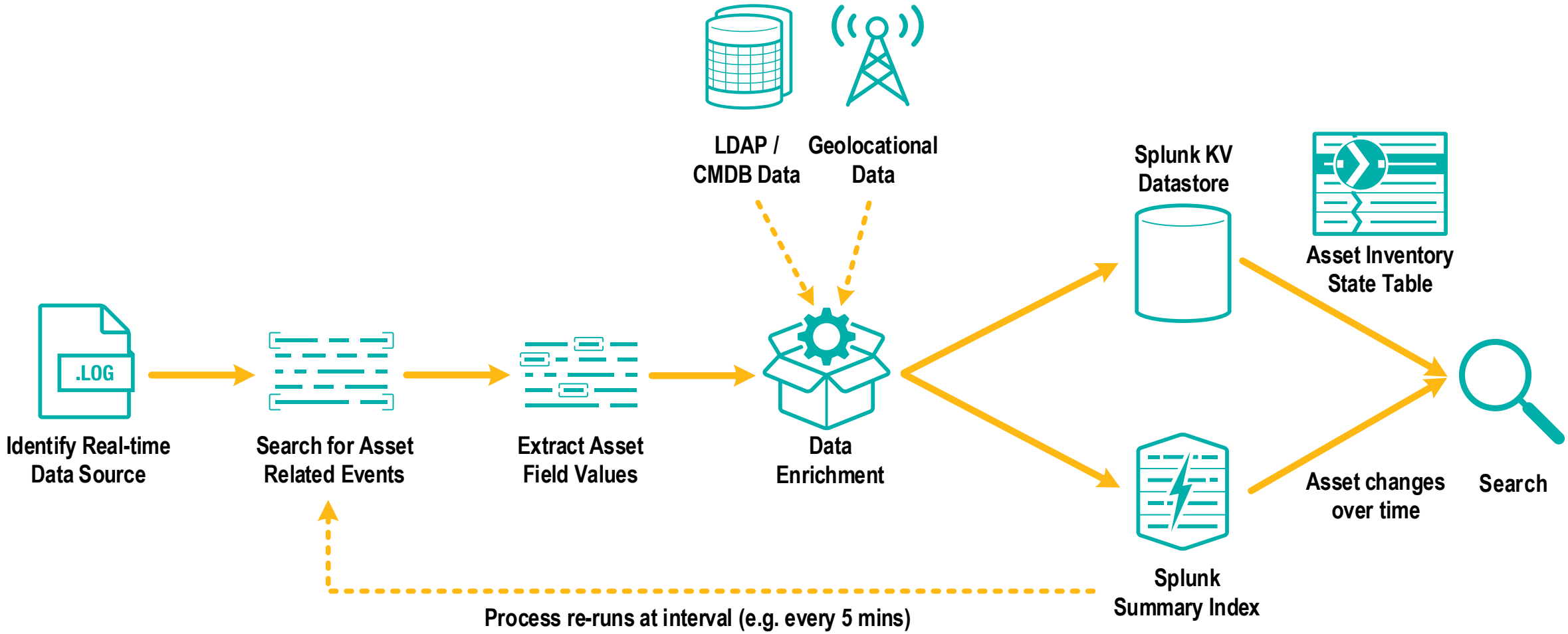
Splunk Demo

Building a Simple Real-time Asset Inventory

splunk> .conf18

Enriching the Data

Go further by adding things we know



Splunk Demo

Enriching the data

splunk> .conf18

Advanced Asset Intelligence

Go even further by applying advanced data driven intelligence

Correlate Multiple Sources

Perform Security Investigations

Raw Event Attribution Over Time

Applied Logic and Anomaly Detection

Compliance Driven Metrics

Splunk Demo

Advanced Asset Intelligence

splunk> .conf18

Integration with Splunk ES

Enrich and enhance Splunk ES and your notable events

Real-time
Asset Integration

Asset Based
Workflow Actions

Asset Intelligence
Driven Swimlanes

Splunk Demo

Integration with Splunk ES

splunk> .conf18

Success Story

Findings from a Fortune 500 company

- 10% Of workstations/servers unmanaged
- Over 5000 IoT devices
- 100s of unencrypted laptops
- Active ‘decommissioned’ servers
- Faster security incident response & investigations
- More accurate attribution in Splunk ES

Key Takeaways

What do I need to know?

1. Take a real-time data driven approach
2. Your event data is a key source of asset intelligence
3. Asset intelligence compliments asset management
4. This is not easy
5. Do it yourself or **AssetIntelligence.app**

Q&A

- Contact Me
  - Paul Johnson
  - Email: paul@discoveredintelligence.ca
- Asset Intelligence
  - Simple Asset Tracker conf18.DiscoveredIntelligence.ca
  - Aura Asset Intelligence™ AssetIntelligence.app
- Other Splunk Conf18 Resources
  - conf18.DiscoveredIntelligence.ca

splunk> .conf18

Thank You

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