Splunk And Control Systems Enabling A Secure Iot Strategy

Terry McCorkle

Global IoT Architect, Splunk

Menno Vanderlist

Sales Engineer, Splunk

.conf2016

splunk>

Disclaimer

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 the 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> .conf2016

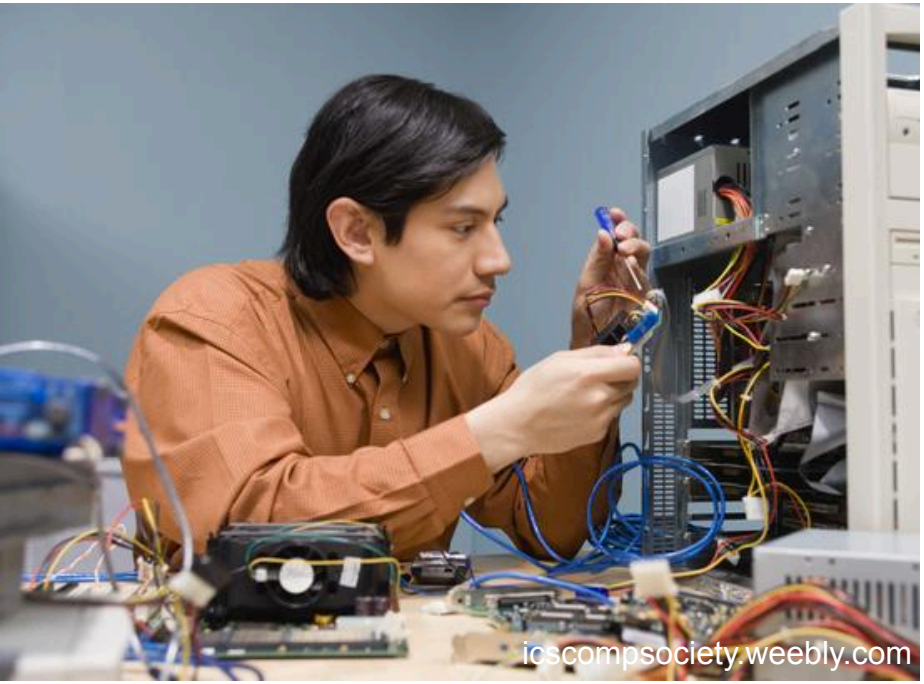
Who are we?

- **Terry McCorkle** – Global IoT Architect, Splunk
- **Menno Vanderlist** – Sales Engineer, Splunk

splunk> .conf2016

the biggest challenge

Systems Created and Managed by **IT teams** vs Systems Created and Managed by **Engineers**



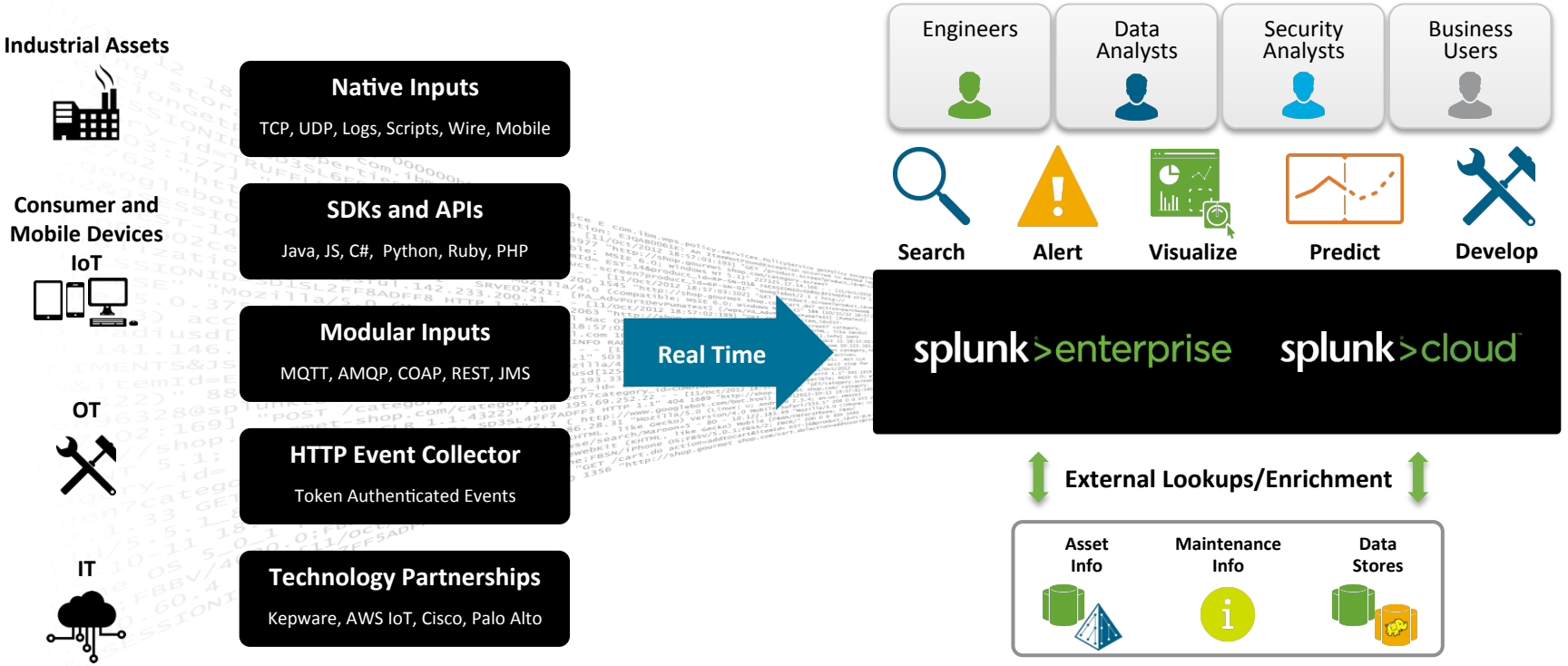
splunk> .conf2016

Agenda

- Getting Control System data into Splunk
- Other important data for Operations and Security
- Creating security communication

splunk> .conf2016

Getting Data In is Easy



Splunk's IoT and Industrial Partner Ecosystem

There is a partner to help bring in your data

Finding the other data sources

Using Splunk across multiple use cases with the same data

IT Operations

- Windows Logs (login issues)
- Network Events (availability)
- Application Logs (HMI issues)
- Windows Updates (patch completion)
- Performance Counters

Security

- Windows Logs (login concerns)
- Network Events (traffic profiles)
- Application Logs (unauthorized apps)
- Windows Updates (missing patches)
- Audit Events
- Access Card Events (entry/exit)
- Unresponsive/Lost Assets (missing data)

splunk> .conf2016

No connectivity?

Air gap between networks?

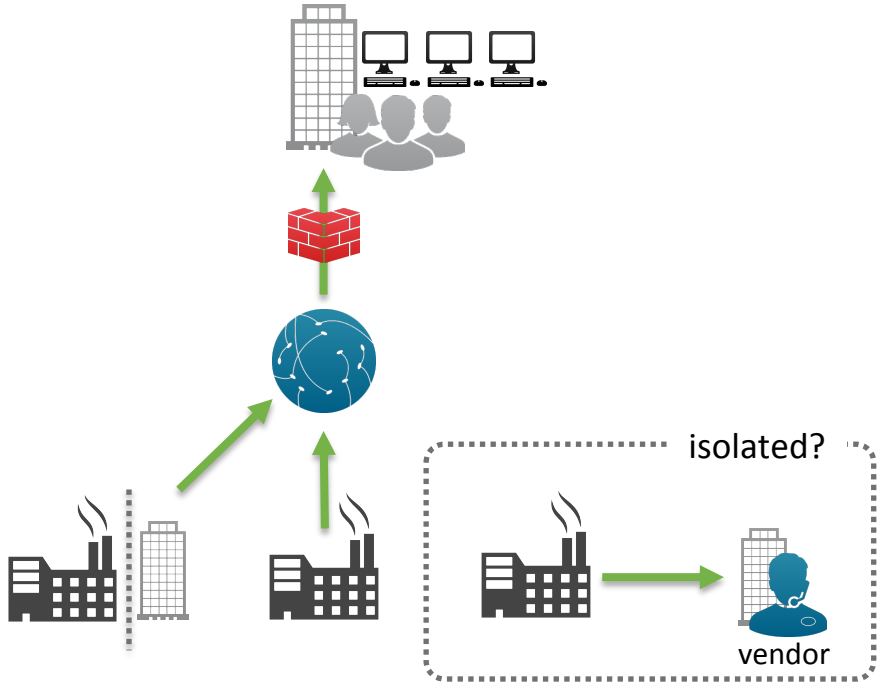
Restrictive firewalls?

splunk> .conf2016

Isolated Process Control Networks

How do we communicate?

- Gaining visibility
- Corporate vs. Control Networks
- Bringing data back to corporate
- Is the network truly isolated?

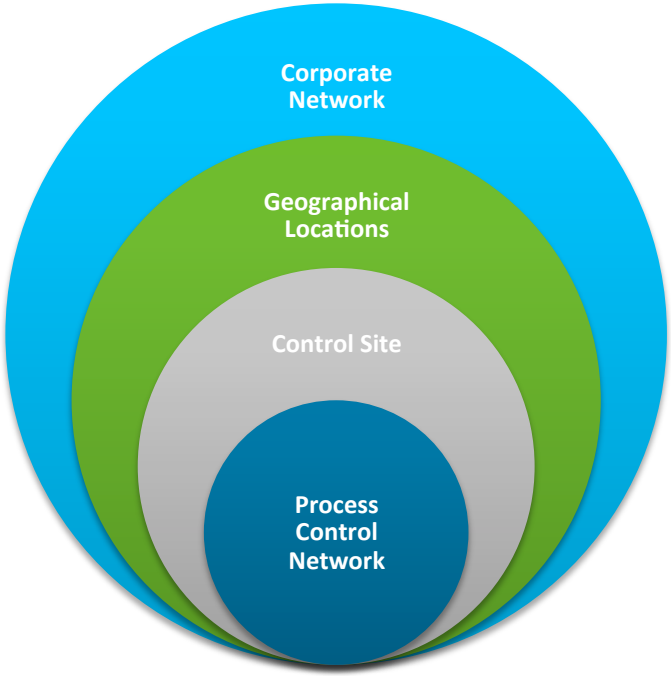


splunk> .conf2016

Centralized vs Isolated Networks

How do we gain visibility?

- Geographically separated sites
- Slow links
- Centralizing Data
- What would you collect from?



splunk> .conf2016

Network Communication

Splunk-to-Splunk (S2S) vs. Syslog vs. other

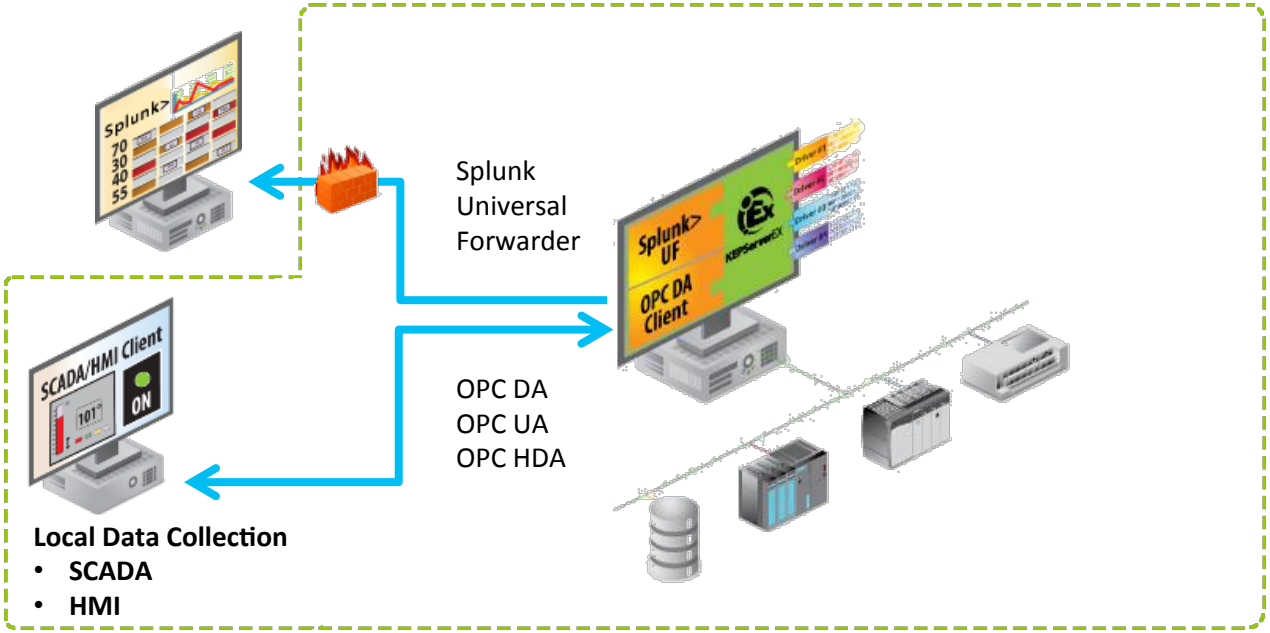
- TCP vs. UDP

splunk> .conf2016

Network Communication

Splunk-to-Splunk (S2S) vs. Syslog vs. other

- TCP vs. UDP
- Encryption
- Acknowledgement
- Compression
- Cloud

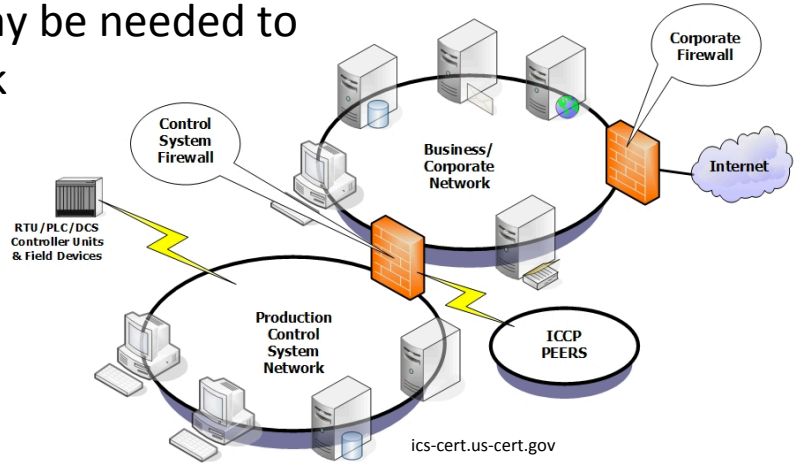


splunk> .conf2016

Industrial Firewall

Difference between traditional and industrial firewall

- Similar to Next gen firewall
- Device and protocol awareness
- Protocol Detection and Inspection
- Custom drivers may be needed to communicate back

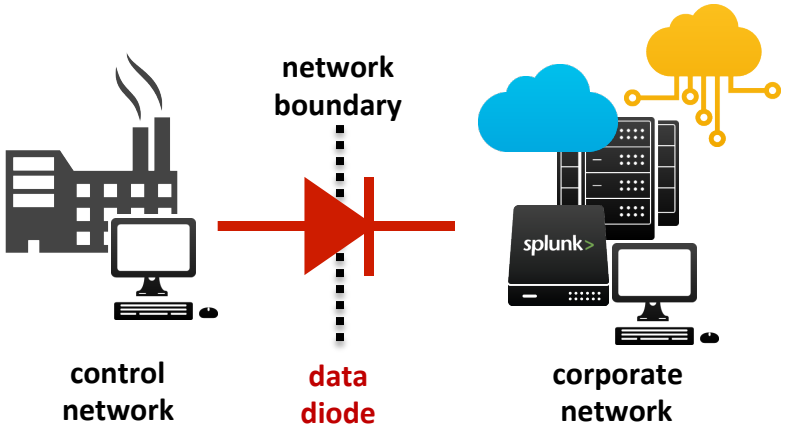


splunk> .conf2016

Communicating through a data diode

Data Diode Benefits: **secure one-way communication**

- One-way fiber optics restrict flow
- Sending using Splunk-to-Splunk
- Syslog
- Custom drivers for communication



splunk> .conf2016

Quick Recap

- Valuable data and insights within control systems
  - OT: availability, data consistency, and data insights
  - IT: System Performance and Availability
  - Security: Auditing of System, User and Application events
- Data Diodes facilitate one-way communication
  - Restrictions enable small paths to communicate out
- Access to Data in Splunk for those who need it
  - Operational and Business Analytics use cases
  - Centralizes all data to compare against multiple data sets and environments
  - Reduces requirements for users to log into control systems

splunk> .conf2016

THANK YOU

splunk>