Splunk for Industrial Control Systems (ICS) Security

Terry McCorkle
Principal Security Strategist, Splunk

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.

A Little About Me

Terry McCorkle

Principal Security Strategist, Splunk

Minster of Chaos

Background

Security Researcher

Penetration Tester

Incident Responder

Agenda

- IoT/ICS Overview (What is your use case?)
- ICS Security Trends
- ICS/Operational Data Collection Points
- Correlating IT Data with Operational Data
- Use Case Examples

IoT Overview

splunk>

Big Data Comes From Machines…

Volume | Velocity | Variety | Variability

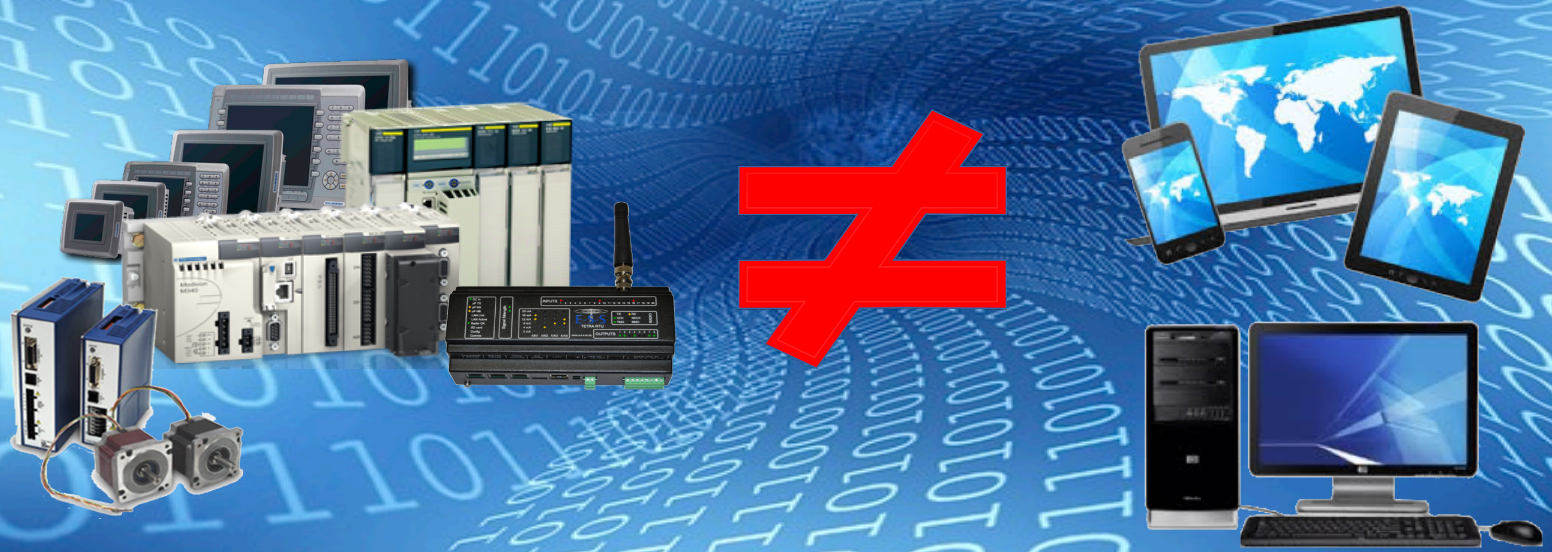
GPS,
RFID,
Hypervisor,
Web Servers,
Email, Messaging,
Clickstreams, Mobile,
Telephony, IVR, Databases,
Sensors, Telematics, Storage,
Servers, Security Devices, Desktops

… Including From OT Environments

Volume | Velocity | Variety | Variability

Sensors, Pumps,
GPS, Valves, Vats,
Conveyors, Pipelines, Drills,
Transformers, RTUs, PLCs, HMIs,
Lighting, HVAC, Traffic Management,
Turbines, Windmills, Generators, Fuel Cells, UPS

Why Is ICS Different Than IT?



Scope of IoT & Industrial Data

Operational Technology (ICS)

- Energy
- Oil & Gas
- Process
- Manufacturing
- Robotics
- Smart Buildings
- Medical Devices
- Telecom

Consumer Technology

- Smart Home
- Wearables
- Media

SCADA	DCS	Other	Emerging Technology

ICS Security Trends

splunk>

ICS Security Threats

CYBER CRIMINALS

MALICIOUS INSIDERS

NATION STATES

Why the Growing Interest in ICS Security?

Everyday Headlines:

South Korean nuclear plant finds malware connected to control systems

By Russell Brandom on December 30, 2014 10:10 am Email @russellbrandom

Damage to German Factory Shows Danger of ICS Hacks

By Robert Lemos | Posted 2014-12-26 Email Print

'Industrial Control Systems' Get Hacked with Notorious BlackEnergy Malware

Russian Hackers Targeting Energy Sector, Says Report

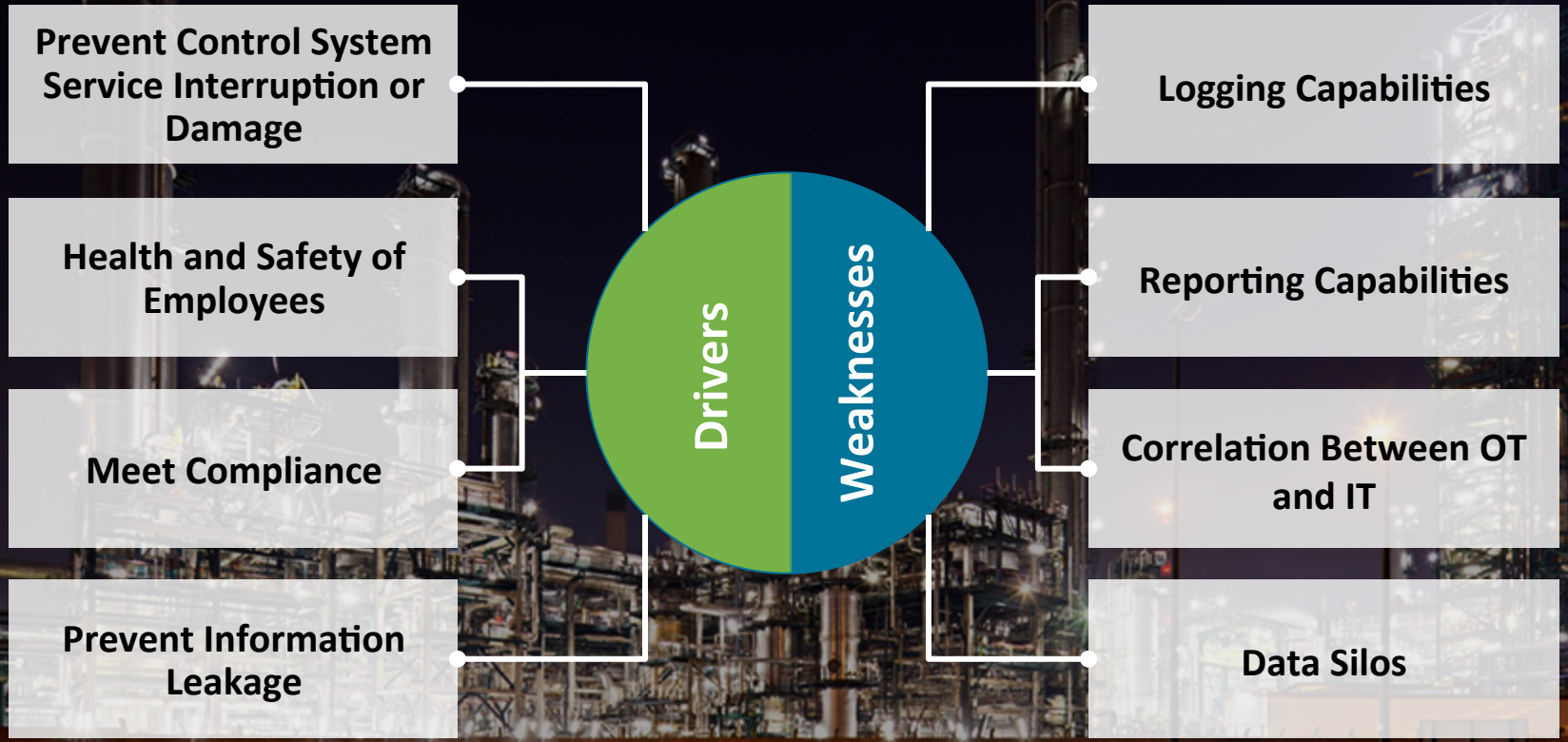
07/01/2014 | Thomas W. Overton, JD

Utility hack led to security overhaul

By Michael Crawford

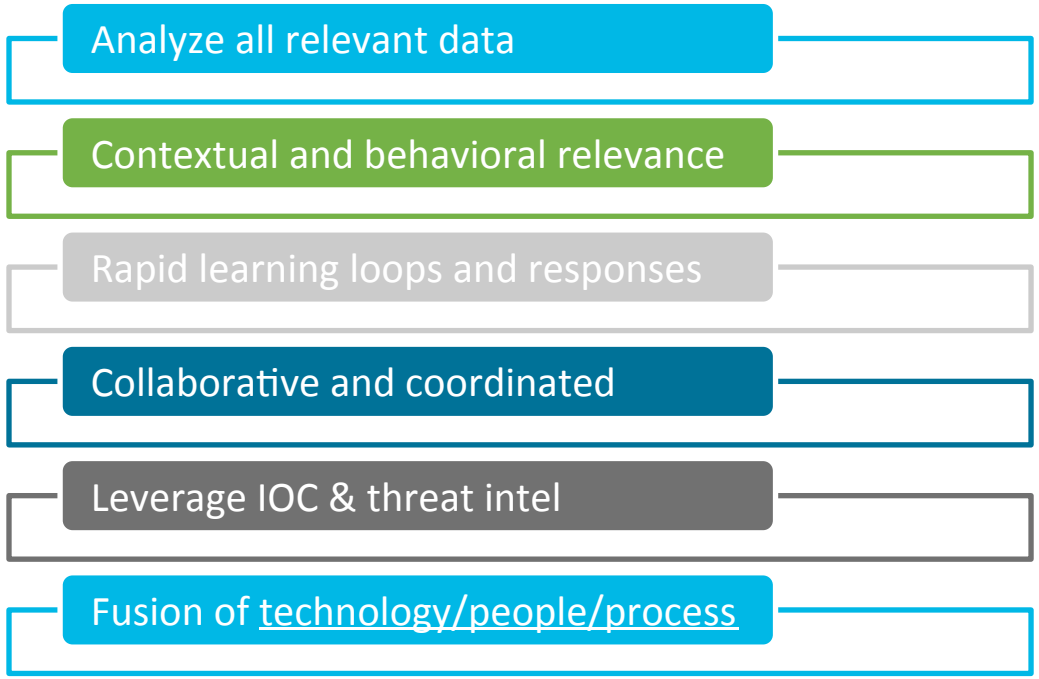
DHS: ATTACKERS HACKED CRITICAL MANUFACTURING FIRM FOR MONTHS

Current State of ICS Security



A New Approach to ICS Security Is Needed

- **Goal oriented**
- **Human directed**
- **Multiple tools, steps and activities**
- **Dynamic**
- **New evasion techniques**
- **Coordinated**



ICS/Operational Data Collection Points

splunk>

All Data is Security Relevant = Big Data


Databases


Email


Web


Desktops

Servers


DHCP/DNS


Network Flows


Hypervisor


Badges

Traditional


Firewall


Authentication


Vulnerability Scans


Intrusion Detection


Data Loss Prevention


Anti-Malware

Custom Apps


Service Desk


Storage


Mobile


Industrial Control


Call Records

Critical ICS Endpoints

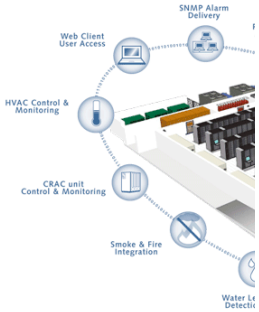
Embedded Devices

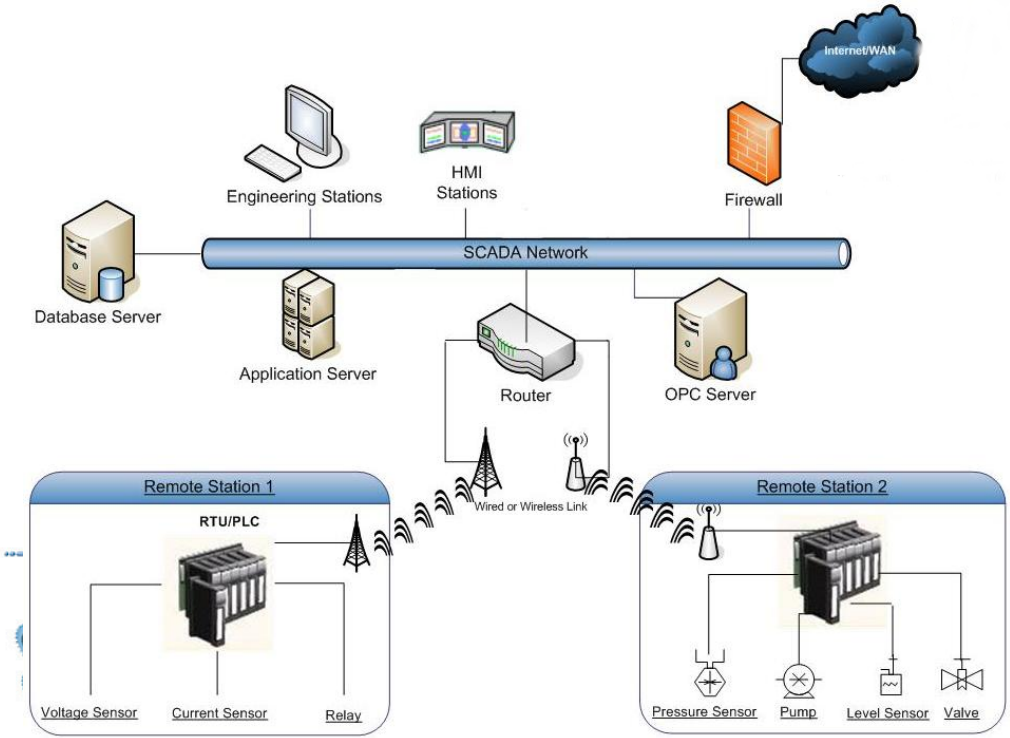
Engineering Workstations

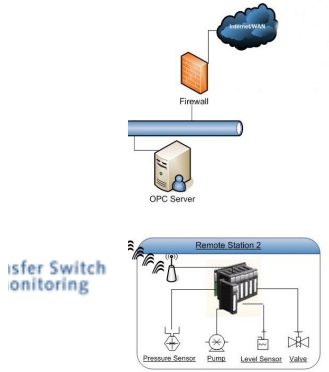
HMI
Historian
Controllers

Control System Communication

Collection Points





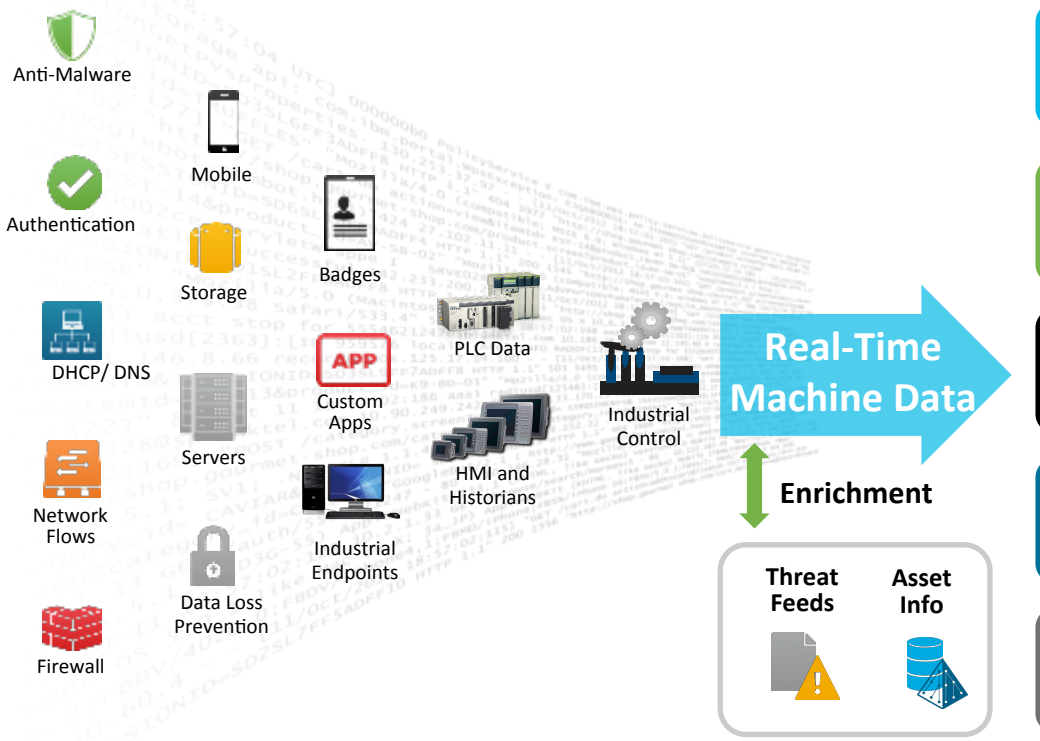


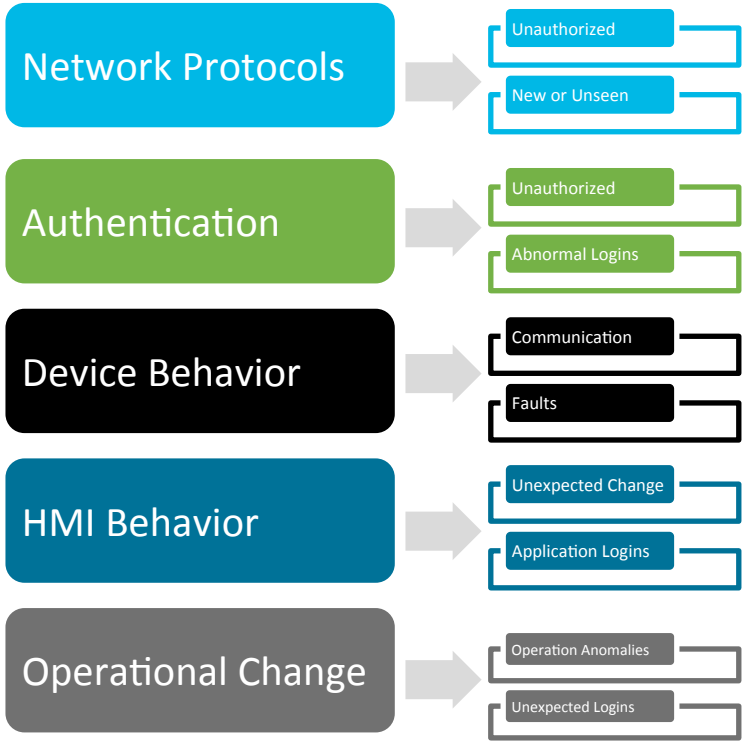
Splunk's ICS Security-Focused Partners

Correlating IT Data With Operational Data

splunk>

Security Data From ICS Devices



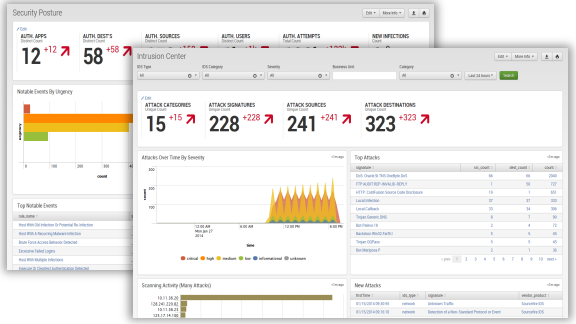


Analytics-Driven Security Use Cases

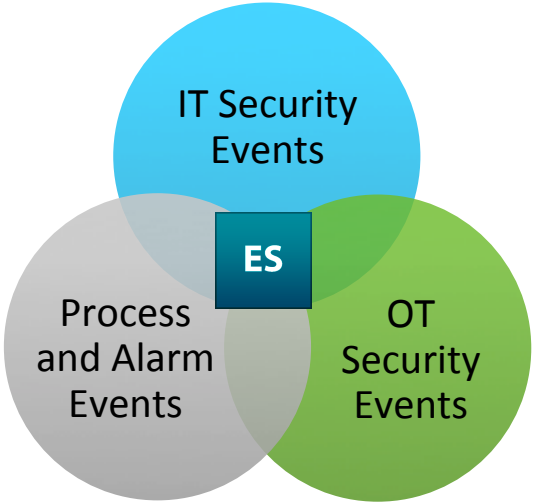
splunk>

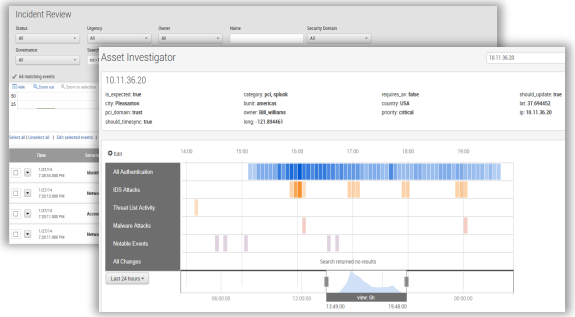
Splunk software complements, replaces and goes beyond traditional SIEMs

The Splunk App for Enterprise Security and ICS

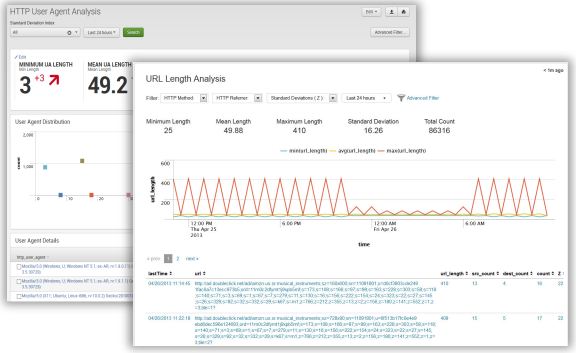


Dashboards and Reports

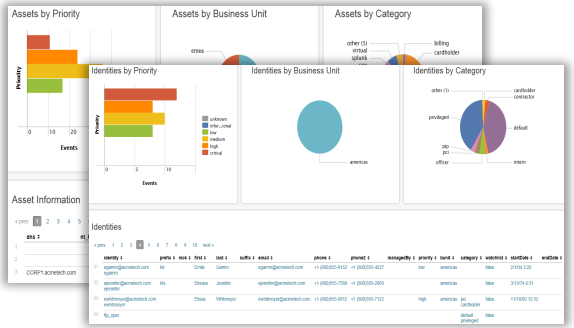




Incident Investigations and Management



Statistical Outliers

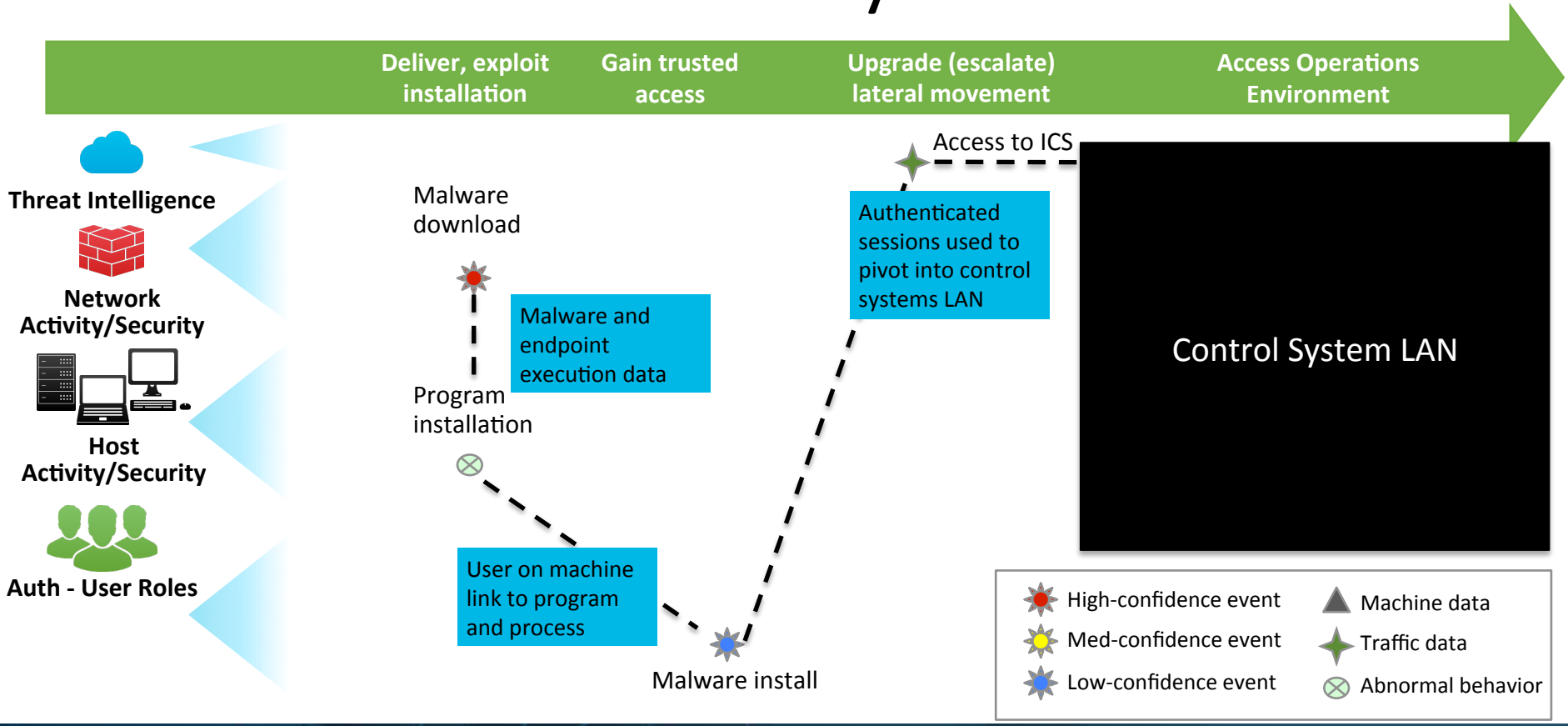


Asset and Identity Aware

Use Case Examples

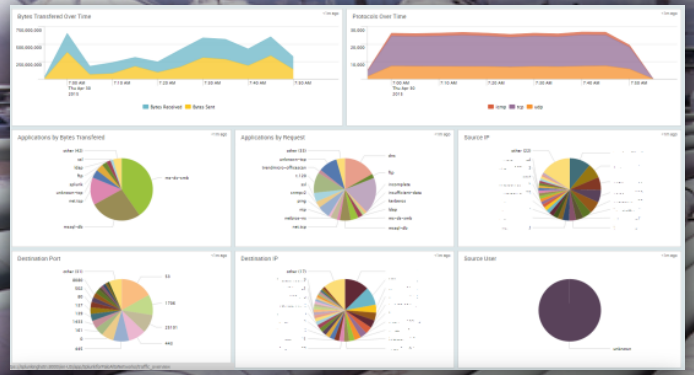
splunk>

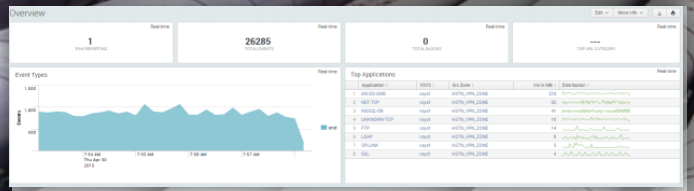
The ICS Security Kill Chain



DEMO

Improving SCADA Operations and Security





Enterprise Products

Analyze 51K miles of pipeline data from servers and OT networks

▼

Improved pipeline safety and availability through higher application uptime

▼

Increase regulatory compliance

▼

95% Improvement in Incident Response Time

Takeaways

Make Your Data Talk to You

- Most organizations have ICS
- ICS Data is valuable
- Protect your ICS data
  - Identify the systems your organization has
  - Splunk it!
  - Correlate it
  - Protect it

What Now?

Related breakout sessions and activities…

- Resources
- Next steps
- Etc.

Questions?

THANK YOU

splunk>