splunk> .conf2017

Operational Threat Detection and Response (OTDR)

Gaining cybersecurity visibility into operational technology blind spots

Kyle Miller | Industrial Cybersecurity Engineer

September 27, 2017 | Washington, DC

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.

Agenda

1. Introduction
2. Challenges in OT Environments
3. Our Solution
4. Use Cases
5. Concluding Comments

Introduction

Kyle Miller

Senior Lead Engineer
Industrial Cyber Security
Booz | Allen | Hamilton

- 10+ years of professional experience, mostly as an ICS/SCADA security consultant across the critical manufacturing, oil & gas, nuclear energy, defense, and water/wastewater critical infrastructure sectors both within the U.S. and abroad
- Specialized in Systems Security Engineering, Design Engineering, Security Test and Evaluations, Risk Assessments, and Detection/Response Design for SCADA and ICS

Certifications

- Certified Information Systems Security Professional (CISSP)
- Global Industrial Cyber Security Professional Certification (GICSP)
- Certified Ethical Hacker (CEH)
- Computer Hacking Forensic Investigator (CHFI)
- ISO 27001 Lead Auditor (BSI Group)
- Project Management Professional (PMP)

Education

- M.S., Cybersecurity
- B.S., Information Technology

Booz | Allen | Hamilton

100 YEARS

Founded in 1914, Booz Allen is considered the world's premium international technology and strategy consulting firm, with engineering and industrial cyber domain expertise across the most challenging industries

100+
OFFICES WORLDWIDE

21,000+
TALENTED PEOPLE

- Aerospace & Defense
- Energy & Environment
- Public Sector
- Health
- Telecommunication
- Financial Services
- Transport

INDUSTRIES SERVED

OUR CLIENTS

400+ out of Fortune 500

70 of the world's 100 largest corporations

5+ USD Billion in Revenues

Agenda

1. Introduction
2. Challenges in OT Environments
3. Our Solution
4. Use Cases
5. Concluding Comments

What is OT?

- Operational Technology, or OT, is a common term that describes hardware and software that *controls physical devices*
- Encompasses *multiple types of control systems* that support physical processes
- Although different, often *used interchangeably* with the terms Industrial Control Systems (ICS) and/or Supervisory Control and Data Acquisition (SCADA) systems

CONTROL SYSTEM PROCESSES

NON-EXHAUSTIVE

Oil & Gas Exploration, Production, Distribution, and Refining

Electric Power Generation, Transmission, and Distribution

Manufacturing

Water, Wastewater, and Public Utilities

Building Control Systems and Smart Cities

OT Cybersecurity Challenges

INCREASING ATTACKS

- Recent high-profile and attacks have **increased demand**
- 1/3rd of operators indicated some form of breach; a **20% increase** in the last 18 months
- Growing **black/dark web** market for ICS or ‘SCADA access-as-a-service’ and other tools
- Ransomware infections on ICS to be **more frequent** and severe

COMPLEXITY

- While devices are **common, implementation is unique**
- Enhanced features on newer ICS devices **increases attack surface** and likelihood of vulnerabilities
- Legacy (like, really legacy) equipment and proprietary protocols require a **light touch**

BUSINESS DRIVERS

- OT relies **more and more** on cyber infrastructure and protocols for daily operations
- Business leaders want **real-time access** into the process data, leading to **increased interconnectivity**
- Finding individuals versed in **industrial engineering and cybersecurity**, is like finding a unicorn

Visibility is a Key Challenge

The Tip of the Iceberg

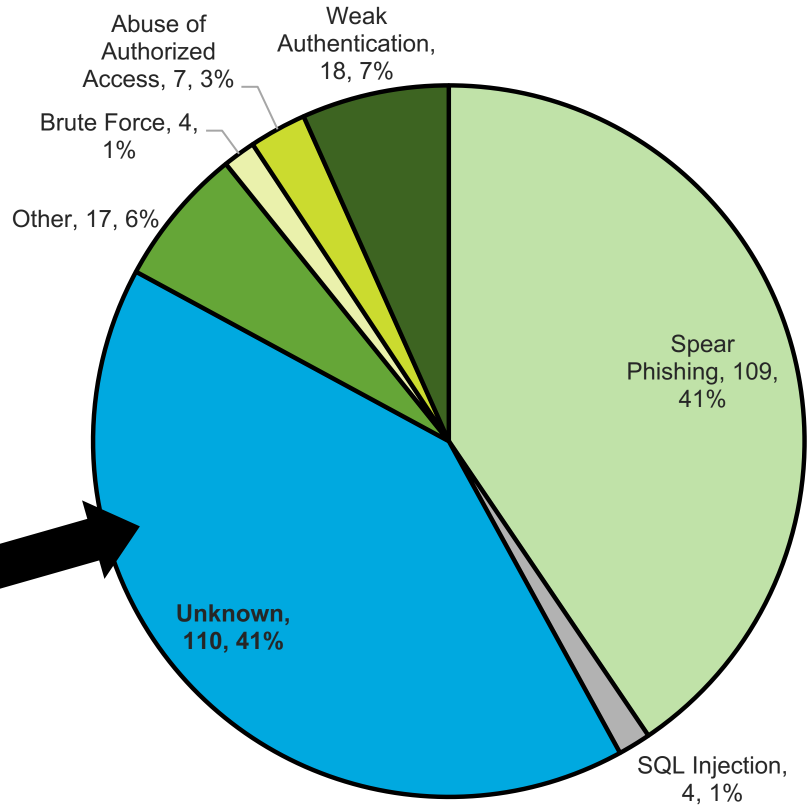
- With these increasing challenges, **traditional cyber protection** mechanisms are not always **feasible**
- Therefore, **obtaining visibility** into these environments to assist with cybersecurity efforts is critical
- Very few OT environments have any form of advanced cyber monitoring in place

Unknown, 110, 41%

*"There were **insufficient forensic artifacts** to definitively identify an initial infection vector. ICS-CERT continues to stress the importance of network security monitoring and host-based intrusion detection technologies, where the underlying systems can support it, to be deployed to better detect, respond to, and analyze incidents."*

Source: *ICS-CERT Monitor Newsletter (FY2015)*

ICS-CERT Incidents by Attack Vector



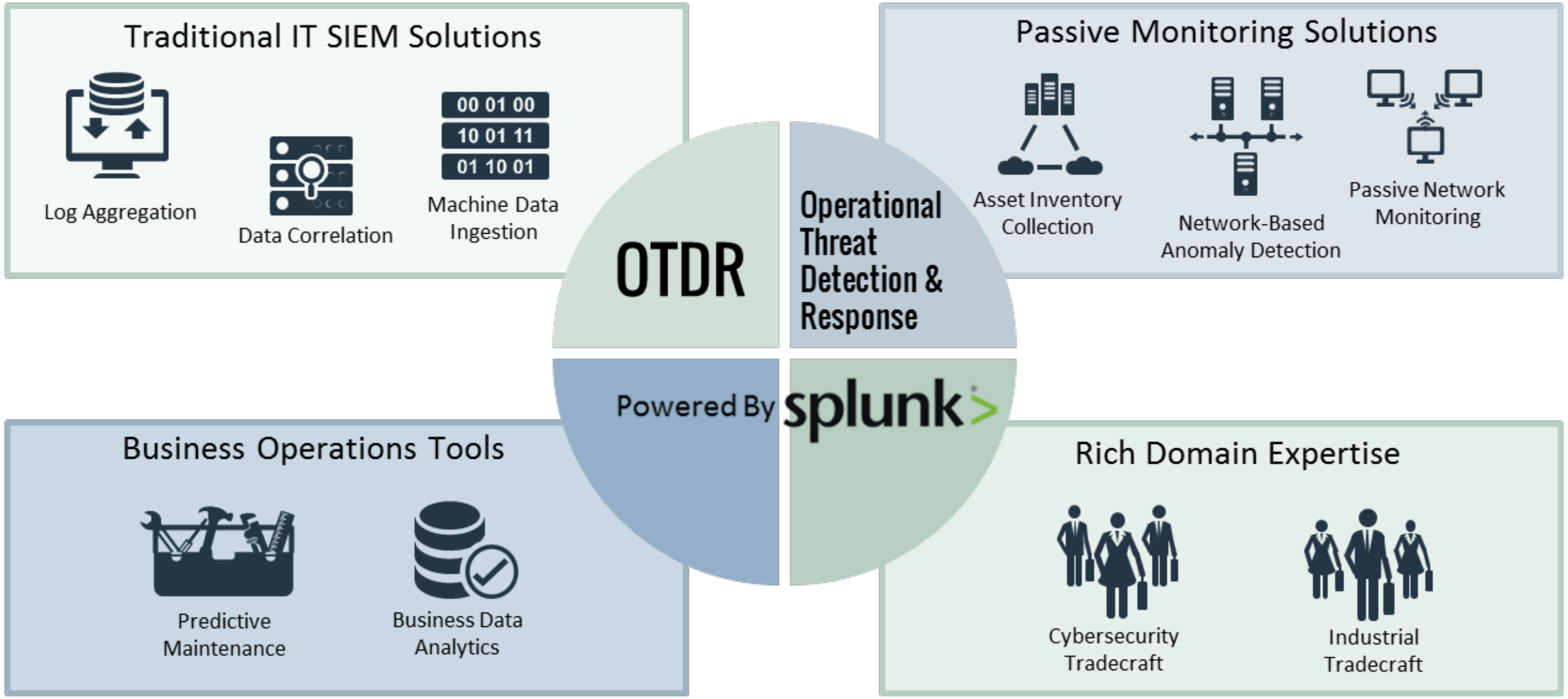
Agenda

1. Introduction
2. Challenges in OT Environments
3. Our Solution
4. Use Cases
5. Concluding Comments

Our Solution

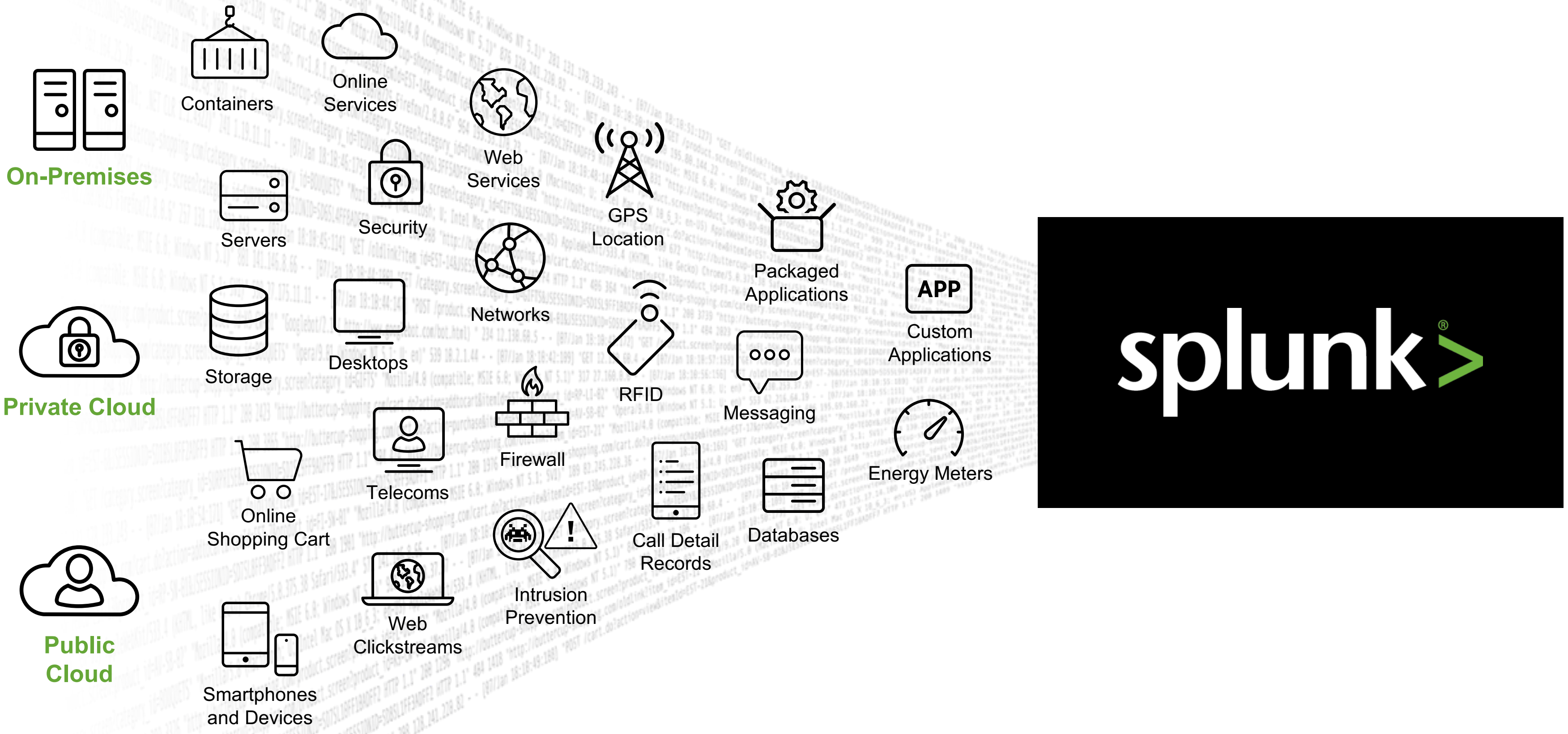
Booz | Allen | Hamilton
Powered By splunk>

Booz Allen's OTDR solution combines capabilities from traditional SIEM providers, OT passive monitoring solutions, and business operations tools—with Booz Allen's rich domain expertise—to provide a single platform for effectively monitoring an OT environment.



Why Splunk?

Index Untapped Data: Any Source, Type, Volume



On-Premises

Private Cloud

Public Cloud

Containers

Online Services

Web Services

GPS Location

Packaged Applications

Servers

Security

Networks

RFID

Messaging

Custom Applications

Storage

Desktops

Firewall

Energy Meters

Online Shopping Cart

Telecoms

Call Detail Records

Databases

Intrusion Prevention

Web Clickstreams

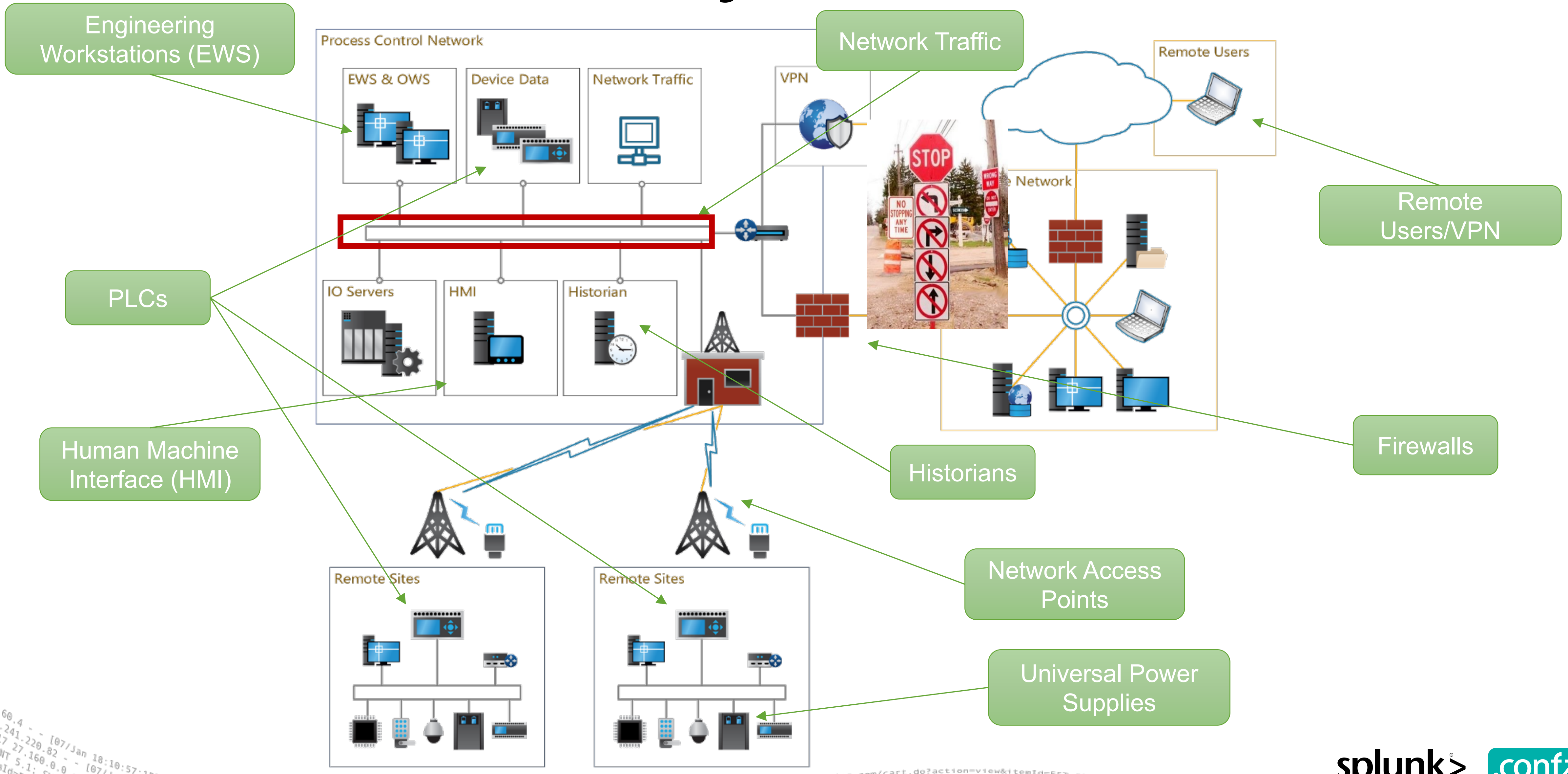
Smartphones and Devices

splunk>

Ask Any Question

- Application Delivery
- IT Operations
- Security, Compliance and Fraud
- Business Analytics
- Industrial Data and the Internet of Things

Where can you Extract Data?



Engineering Workstations (EWS)

Network Traffic

Remote Users/VPN

PLCs

Human Machine Interface (HMI)

Historians

Firewalls

Network Access Points

Universal Power Supplies

What Does OT Machine Data Look Like?

DATA SOURCES

Firewall/VPN

```
10.119.1.1 VPN: 10/04/2016 16:55:14 - VPN-2 - [175.45.177.7] acme\srtabrunaevans(acme AD
Authentication)[Users] - Network Connect: User with IP 10.11.36.20 connected with ESP transport mode
```

Human Machine Interface (HMI)

```
20161004171221.000000Caption=ACME-2975EB\srtabrunaevans  Domain=ACME-2975EB InstallDate=NULL
LocalAccount = IP: 10.11.36.20  TrueName=acme\srtabrunaevans SID =S-1-5-21-1715567821-926492609-725345543
500SIDType=1 Status=Degradedwmi_type=UserAccounts
```

Programmable Logic Controller (PLC)

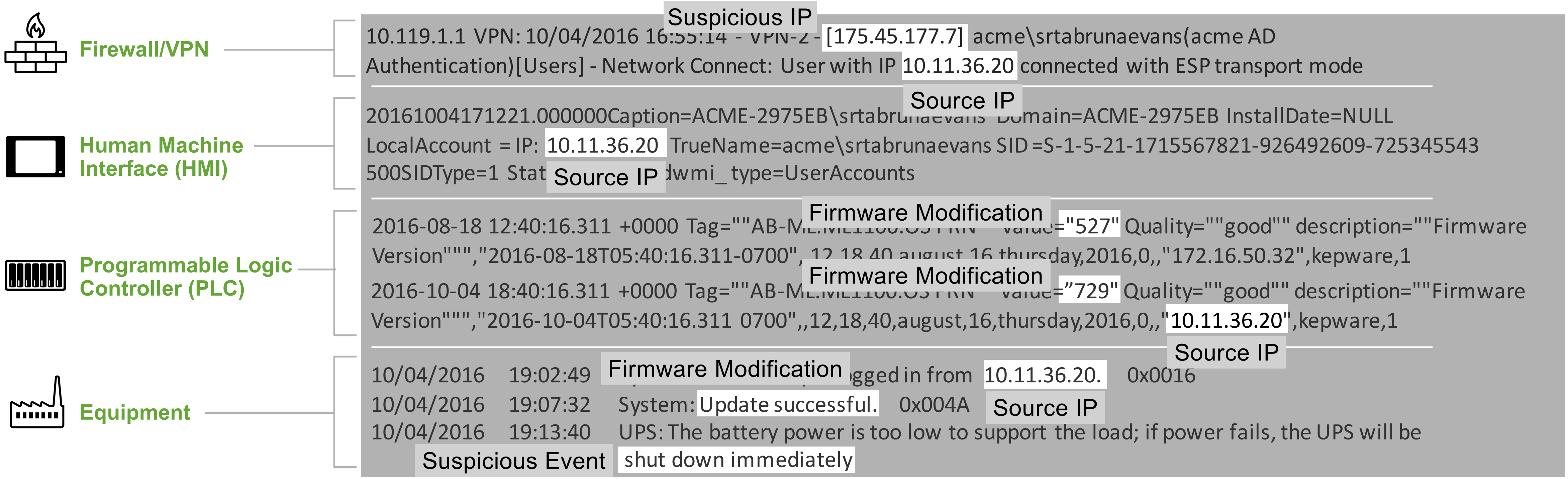
```
2016-08-18 12:40:16.311 +0000 Tag=""AB-ML.ML1100.OS FRN"" Value="527" Quality=""good"" description=""Firmware
Version""","2016-08-18T05:40:16.311-0700",,12,18,40,august,16,thursday,2016,0,,"172.16.50.32",kepware,1
2016-10-04 18:40:16.311 +0000 Tag=""AB-ML.ML1100.OS FRN"" Value=”729" Quality=""good"" description=""Firmware
Version""","2016-10-04T05:40:16.311 0700",,12,18,40,august,16,thursday,2016,0,,"10.11.36.20",kepware,1
```

Equipment

```
10/04/2016    19:02:49    System: FTP user 'apc' logged in from  10.11.36.20.    0x0016
10/04/2016    19:07:32    System: Update successful.    0x004A
10/04/2016    19:13:40    UPS: The battery power is too low to support the load; if power fails, the UPS will be
                           shut down immediately
```

What Does OT Machine Data Look Like?

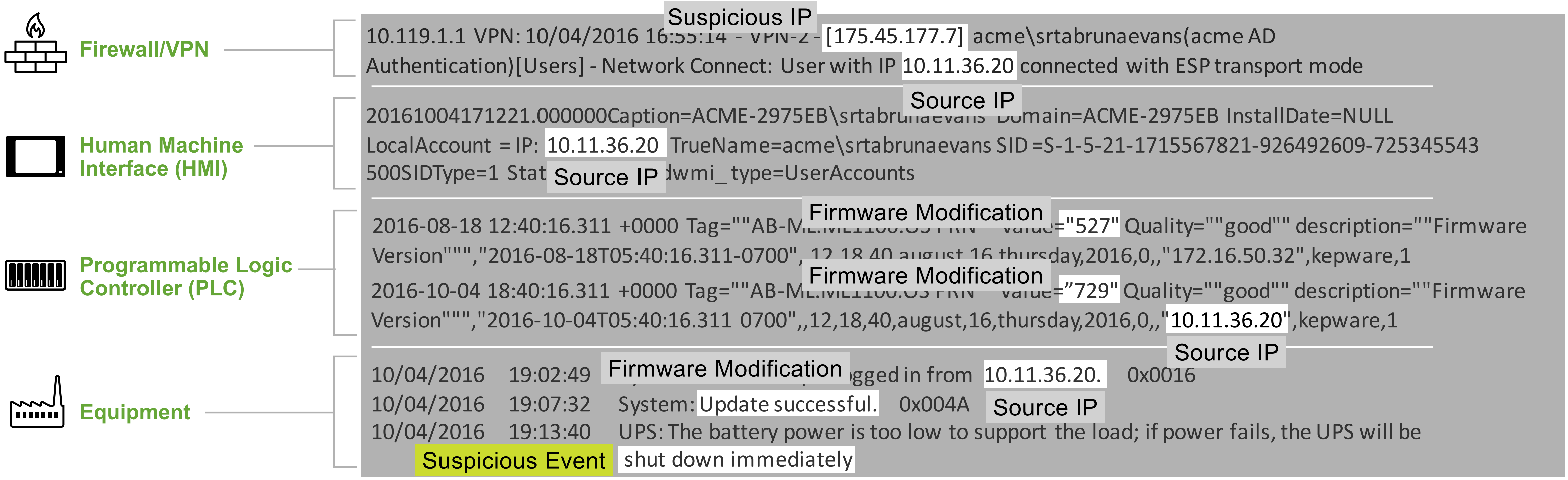
DATA SOURCES



```
10.119.1.1 VPN: 10/04/2016 16:55:14 - VPN-2 - [175.45.177.7] acme\srtabrunaevans(acme AD
Authentication)[Users] - Network Connect: User with IP 10.11.36.20 connected with ESP transport mode

20161004171221.000000Caption=ACME-2975EB\srtabrunaevans Domain=ACME-2975EB InstallDate=NULL
LocalAccount = IP: 10.11.36.20 TrueName=acme\srtabrunaevans SID=S-1-5-21-1715567821-926492609-725345543
500SIDType=1 Stat [illegible] dwmi_type=UserAccounts

2016-08-18 12:40:16.311 +0000 Tag=""AB-ML.ML1100.OS PRN"" value="527" Quality=""good"" description=""Firmware
Version""","2016-08-18T05:40:16.311-0700",,12,18,40,august,16,thursday,2016,0,,"172.16.50.32",kepware,1
2016-10-04 18:40:16.311 +0000 Tag=""AB-ML.ML1100.OS PRN"" value=”729" Quality=""good"" description=""Firmware
Version""","2016-10-04T05:40:16.311 0700",,12,18,40,august,16,thursday,2016,0,,"10.11.36.20",kepware,1

10/04/2016    19:02:49    [illegible] gged in from 10.11.36.20.    0x0016
10/04/2016    19:07:32    System: Update successful.    0x004A
10/04/2016    19:13:40    UPS: The battery power is too low to support the load; if power fails, the UPS will be
                          shut down immediately
```

What Does OT Machine Data Look Like?

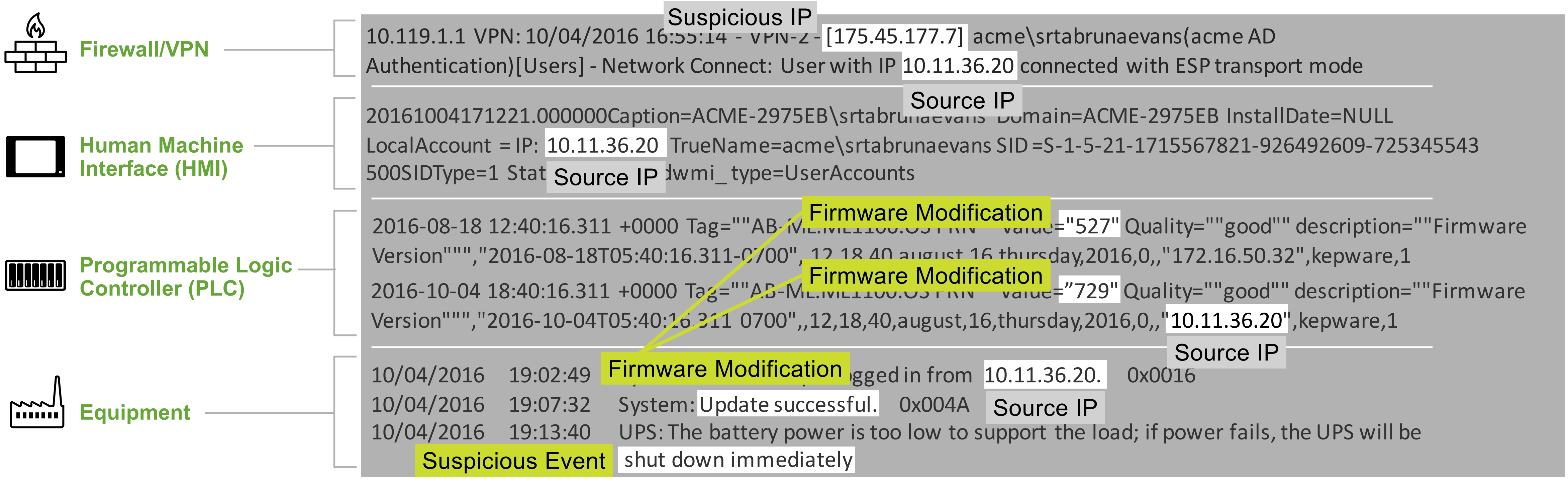
DATA SOURCES



```
10.119.1.1 VPN: 10/04/2016 16:55:14 - VPN-2 - [175.45.177.7] acme\srtabrunaevans(acme AD
Authentication)[Users] - Network Connect: User with IP 10.11.36.20 connected with ESP transport mode

20161004171221.000000Caption=ACME-2975EB\srtabrunaevans Domain=ACME-2975EB InstallDate=NULL
LocalAccount = IP: 10.11.36.20 TrueName=acme\srtabrunaevans SID =S-1-5-21-1715567821-926492609-725345543
500SIDType=1 Stat dwmi_type=UserAccounts

2016-08-18 12:40:16.311 +0000 Tag=""AB-ML.ML1100.OS FRN   Value="527" Quality=""good"" description=""Firmware
Version""","2016-08-18T05:40:16.311-0700",,12,18,40,august,16,thursday,2016,0,,"172.16.50.32",kepware,1
2016-10-04 18:40:16.311 +0000 Tag=""AB-ML.ML1100.OS FRN   Value=”729" Quality=""good"" description=""Firmware
Version""","2016-10-04T05:40:16.311 0700",,12,18,40,august,16,thursday,2016,0,,"10.11.36.20",kepware,1

10/04/2016    19:02:49                gged in from 10.11.36.20.    0x0016
10/04/2016    19:07:32    System: Update successful.    0x004A
10/04/2016    19:13:40    UPS: The battery power is too low to support the load; if power fails, the UPS will be
                          shut down immediately
```

What Does OT Machine Data Look Like?

DATA SOURCES



```
10.119.1.1 VPN: 10/04/2016 16:55:14 - VPN-2 - [175.45.177.7] acme\srtabrunaevans(acme AD
Authentication)[Users] - Network Connect: User with IP 10.11.36.20 connected with ESP transport mode

20161004171221.000000Caption=ACME-2975EB\srtabrunaevans Domain=ACME-2975EB InstallDate=NULL
LocalAccount = IP: 10.11.36.20 TrueName=acme\srtabrunaevans SID =S-1-5-21-1715567821-926492609-725345543
500SIDType=1 Stat [illegible] wmi_ type=UserAccounts

2016-08-18 12:40:16.311 +0000 Tag=""AB-ML.ML1100.OSTRN Value="527" Quality=""good"" description=""Firmware
Version""","2016-08-18T05:40:16.311-0700",,12,18,40,august,16,thursday,2016,0,,"172.16.50.32",kepware,1
2016-10-04 18:40:16.311 +0000 Tag=""AB-ML.ML1100.OSTRN Value=”729" Quality=""good"" description=""Firmware
Version""","2016-10-04T05:40:16.311 0700",,12,18,40,august,16,thursday,2016,0,,"10.11.36.20",kepware,1

10/04/2016    19:02:49    [illegible] logged in from 10.11.36.20.    0x0016
10/04/2016    19:07:32    System: Update successful.    0x004A
10/04/2016    19:13:40    UPS: The battery power is too low to support the load; if power fails, the UPS will be
              shut down immediately
```

splunk> .conf2017

What Does OT Machine Data Look Like?

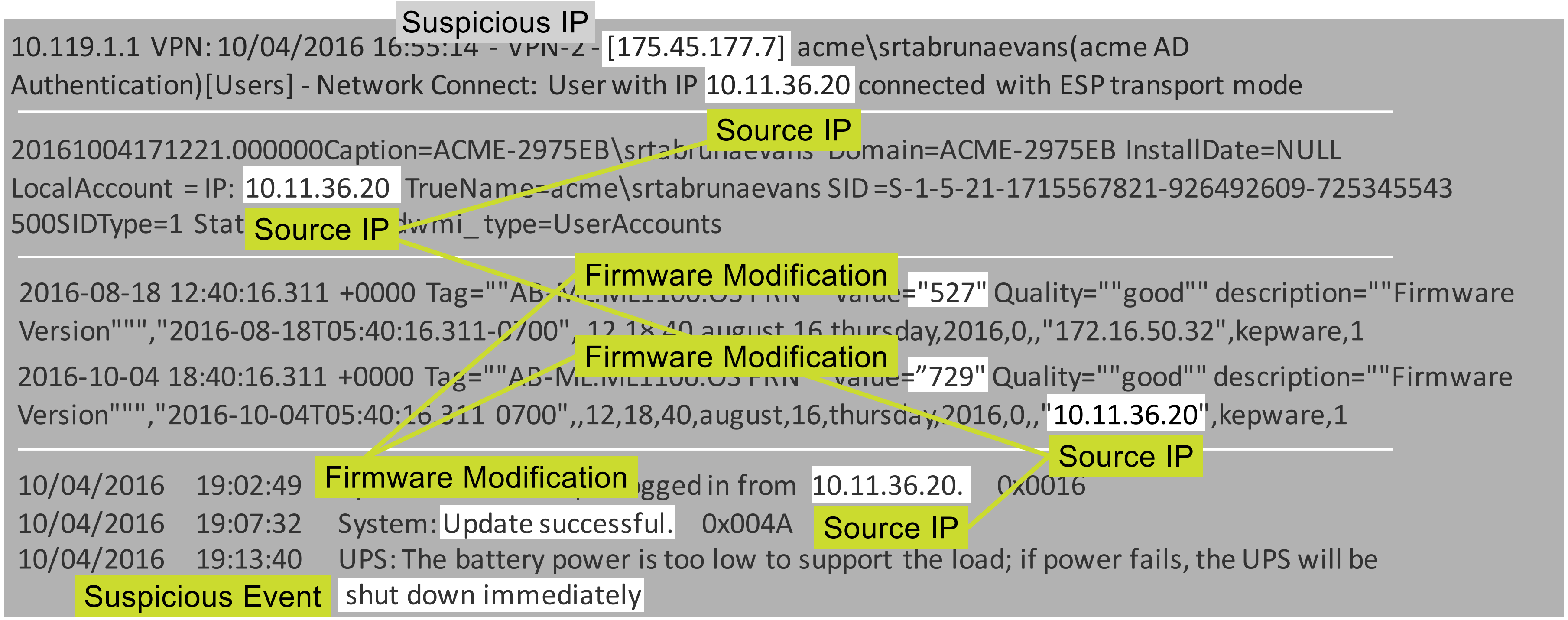
DATA SOURCES

Firewall/VPN

Human Machine Interface (HMI)

Programmable Logic Controller (PLC)

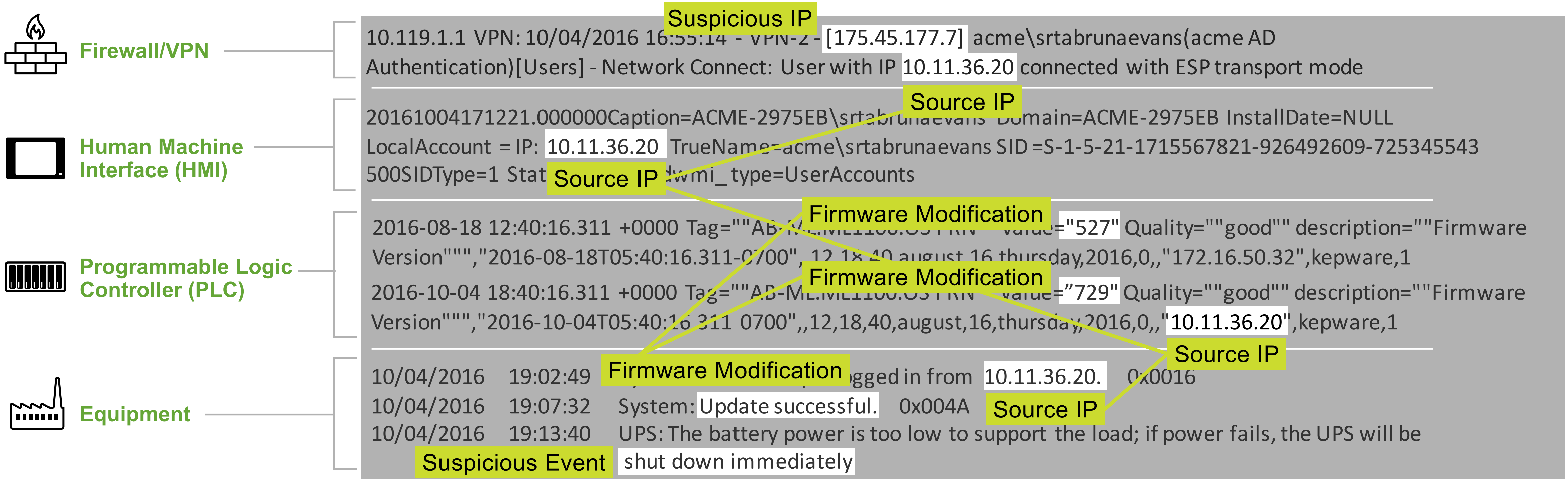
Equipment



```
10.119.1.1 VPN: 10/04/2016 16:55:14 - VPN-2 - [175.45.177.7] acme\srtabrunaevans(acme AD
Authentication)[Users] - Network Connect: User with IP 10.11.36.20 connected with ESP transport mode

20161004171221.000000Caption=ACME-2975EB\srtabrunaevans Domain=ACME-2975EB InstallDate=NULL
LocalAccount = IP: 10.11.36.20  TrueName=acme\srtabrunaevans SID =S-1-5-21-1715567821-926492609-725345543
500SIDType=1 Stat wmi_ type=UserAccounts

2016-08-18 12:40:16.311 +0000 Tag=""AB-ML.ML1100.OS FRN"" value="527" Quality=""good"" description=""Firmware
Version""","2016-08-18T05:40:16.311-0700",,12,18,40,august,16,thursday,2016,0,,"172.16.50.32",kepware,1
2016-10-04 18:40:16.311 +0000 Tag=""AB-ML.ML1100.OS FRN"" value=”729" Quality=""good"" description=""Firmware
Version""","2016-10-04T05:40:16.311 0700",,12,18,40,august,16,thursday,2016,0,,"10.11.36.20",kepware,1

10/04/2016    19:02:49    logged in from  10.11.36.20.    0x0016
10/04/2016    19:07:32    System: Update successful.   0x004A
10/04/2016    19:13:40    UPS: The battery power is too low to support the load; if power fails, the UPS will be
                          shut down immediately
```

What Does OT Machine Data Look Like?

DATA SOURCES



Firewall/VPN

```
10.119.1.1 VPN: 10/04/2016 16:55:14 - VPN-2 - [175.45.177.7] acme\srtabrunaevans(acme AD
Authentication)[Users] - Network Connect: User with IP 10.11.36.20 connected with ESP transport mode
```

Human Machine Interface (HMI)

```
20161004171221.000000Caption=ACME-2975EB\srtabrunaevans Domain=ACME-2975EB InstallDate=NULL
LocalAccount = IP: 10.11.36.20  TrueName=acme\srtabrunaevans SID =S-1-5-21-1715567821-926492609-725345543
500SIDType=1 Stat wmi_ type=UserAccounts
```

Programmable Logic Controller (PLC)

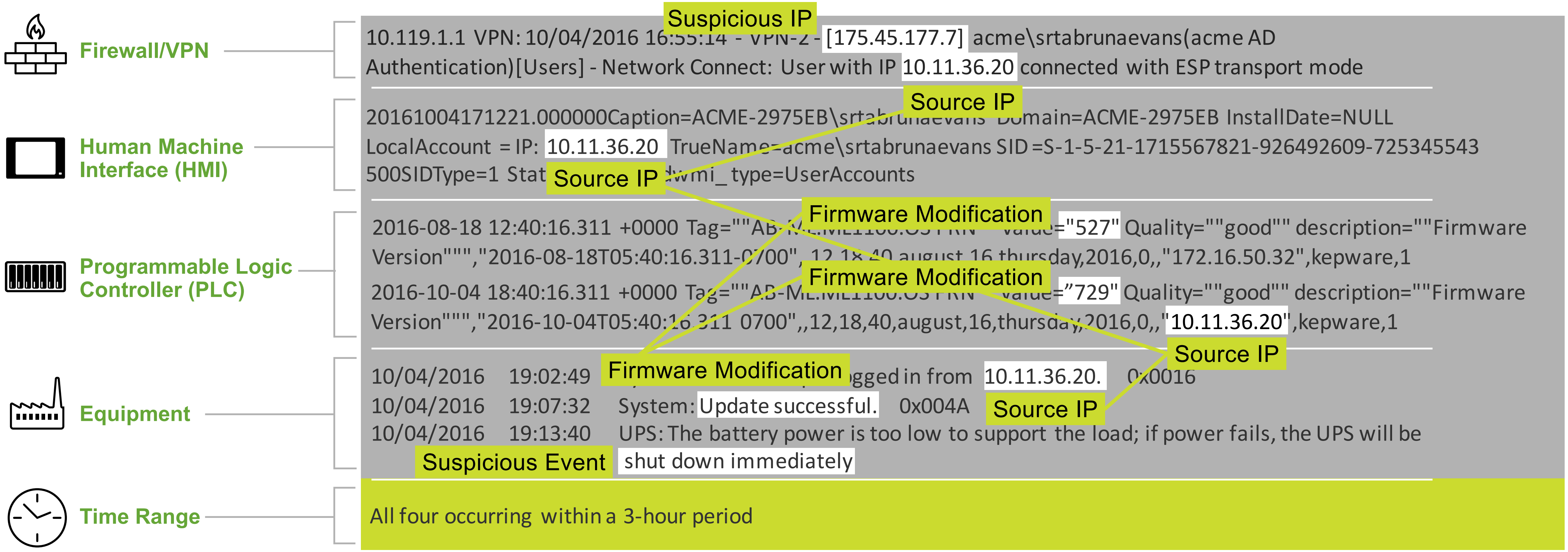
```
2016-08-18 12:40:16.311 +0000 Tag=""AB-ML:ML1100:OS PRN   value="527" Quality=""good"" description=""Firmware
Version""","2016-08-18T05:40:16.311-0700",,12,18,40,august,16,thursday,2016,0,,"172.16.50.32",kepware,1
2016-10-04 18:40:16.311 +0000 Tag=""AB-ML:ML1100:OS PRN   value=”729" Quality=""good"" description=""Firmware
Version""","2016-10-04T05:40:16.311 0700",,12,18,40,august,16,thursday,2016,0,,"10.11.36.20",kepware,1
```

Equipment

```
10/04/2016    19:02:49                           ogged in from 10.11.36.20.    0x0016
10/04/2016    19:07:32    System: Update successful.    0x004A
10/04/2016    19:13:40    UPS: The battery power is too low to support the load; if power fails, the UPS will be
                          shut down immediately
```

What Does OT Machine Data Look Like?

DATA SOURCES



Firewall/VPN

```
10.119.1.1 VPN: 10/04/2016 16:55:14 - VPN-2 - [175.45.177.7] acme\srtabrunaevans(acme AD
Authentication)[Users] - Network Connect: User with IP 10.11.36.20 connected with ESP transport mode
```

Human Machine Interface (HMI)

```
20161004171221.000000Caption=ACME-2975EB\srtabrunaevans Domain=ACME-2975EB InstallDate=NULL
LocalAccount = IP: 10.11.36.20 TrueName=acme\srtabrunaevans SID =S-1-5-21-1715567821-926492609-725345543
500SIDType=1 Stat wmi_type=UserAccounts
```

Programmable Logic Controller (PLC)

```
2016-08-18 12:40:16.311 +0000 Tag=""AB-ML.ML1100.OS FRN"" Value="527" Quality=""good"" description=""Firmware
Version""","2016-08-18T05:40:16.311-0700",,12,18,40,august,16,thursday,2016,0,,"172.16.50.32",kepware,1
2016-10-04 18:40:16.311 +0000 Tag=""AB-ML.ML1100.OS FRN"" Value=”729" Quality=""good"" description=""Firmware
Version""","2016-10-04T05:40:16.311 0700",,12,18,40,august,16,thursday,2016,0,,"10.11.36.20",kepware,1
```

Equipment

```
10/04/2016    19:02:49    ogged in from 10.11.36.20.    0x0016
10/04/2016    19:07:32    System: Update successful.    0x004A
10/04/2016    19:13:40    UPS: The battery power is too low to support the load; if power fails, the UPS will be
                          shut down immediately
```

Time Range

All four occurring within a 3-hour period

What Does OT Machine Data Look Like?

DATA SOURCES

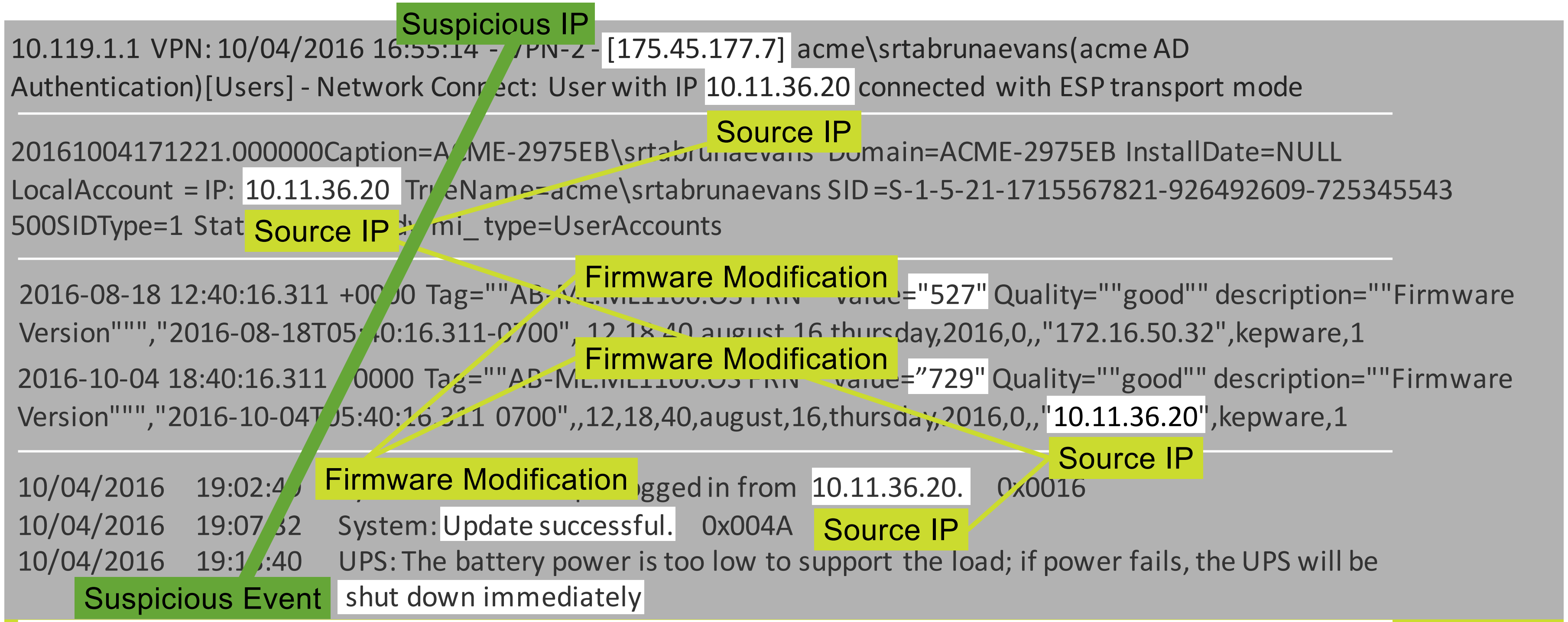
Firewall/VPN

Human Machine Interface (HMI)

Programmable Logic Controller (PLC)

Equipment

Time Range

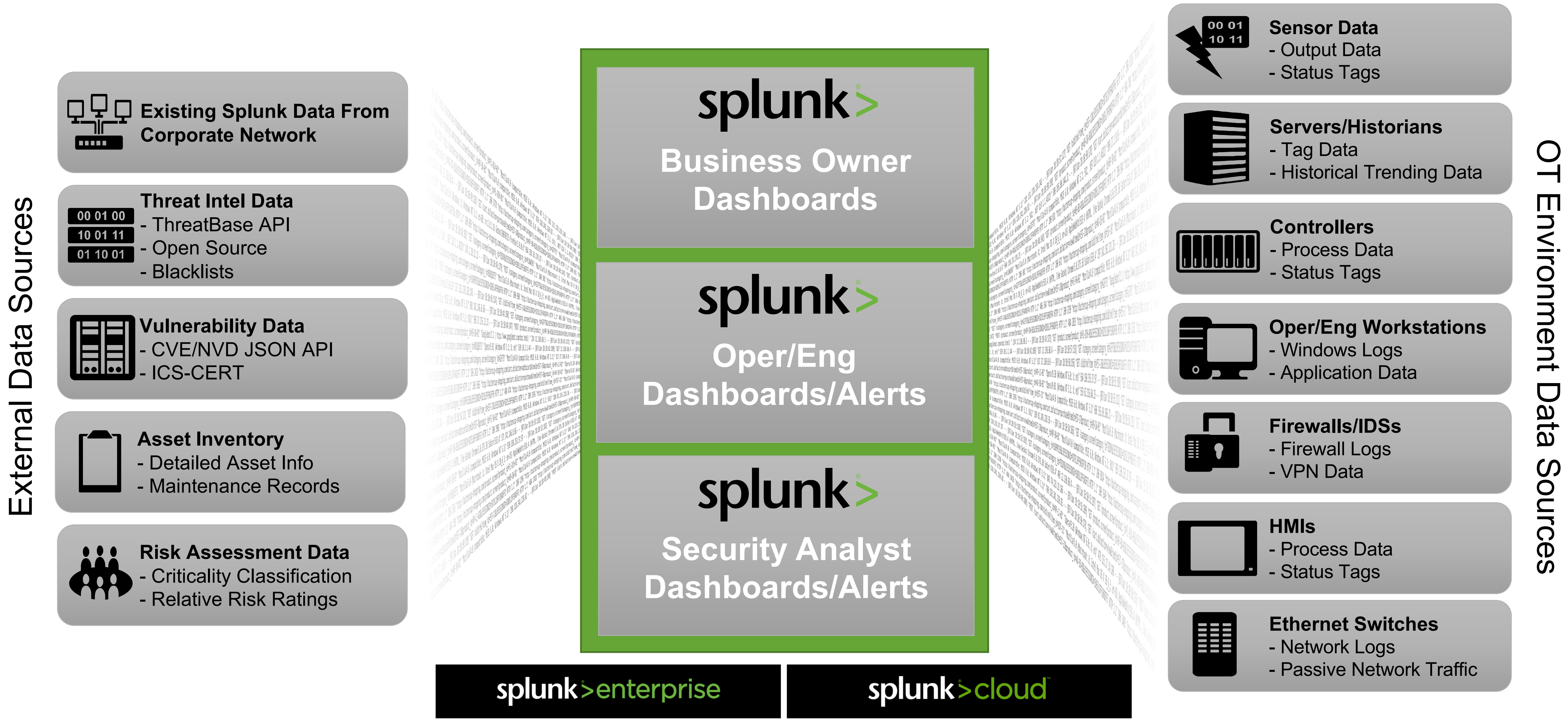


```
10.119.1.1 VPN: 10/04/2016 16:55:14 - VPN-2 - [175.45.177.7] acme\srtabrunaevans(acme AD
Authentication)[Users] - Network Connect: User with IP 10.11.36.20 connected with ESP transport mode

20161004171221.000000Caption=ACME-2975EB\srtabrunaevans Domain=ACME-2975EB InstallDate=NULL
LocalAccount = IP: 10.11.36.20 TrueName=acme\srtabrunaevans SID =S-1-5-21-1715567821-926492609-725345543
500SIDType=1 Stat                  mi_ type=UserAccounts

2016-08-18 12:40:16.311 +0000 Tag=""AB-                  value="527" Quality=""good"" description=""Firmware
Version""","2016-08-18T05:40:16.311-0700",,12,18,40,august,16,thursday,2016,0,,"172.16.50.32",kepware,1
2016-10-04 18:40:16.311 +0000 Tag=""AB-ML.ML1100.OS FRN   value=”729" Quality=""good"" description=""Firmware
Version""","2016-10-04T05:40:16.311 0700",,12,18,40,august,16,thursday,2016,0,,"10.11.36.20",kepware,1

10/04/2016    19:02:4                           ogged in from 10.11.36.20.    0x0016
10/04/2016    19:07:32    System: Update successful.    0x004A
10/04/2016    19:1 :40    UPS: The battery power is too low to support the load; if power fails, the UPS will be
                          shut down immediately
```

All four occurring within a 3-hour period

splunk> .conf2017

Bringing it All Together



External Data Sources

Existing Splunk Data From Corporate Network

Threat Intel Data
- ThreatBase API
- Open Source
- Blacklists

Vulnerability Data
- CVE/NVD JSON API
- ICS-CERT

Asset Inventory
- Detailed Asset Info
- Maintenance Records

Risk Assessment Data
- Criticality Classification
- Relative Risk Ratings

splunk> Business Owner Dashboards

splunk> Oper/Eng Dashboards/Alerts

splunk> Security Analyst Dashboards/Alerts

splunk>enterprise

splunk>cloud

OT Environment Data Sources

Sensor Data
- Output Data
- Status Tags

Servers/Historians
- Tag Data
- Historical Trending Data

Controllers
- Process Data
- Status Tags

Oper/Eng Workstations
- Windows Logs
- Application Data

Firewalls/IDSs
- Firewall Logs
- VPN Data

HMIs
- Process Data
- Status Tags

Ethernet Switches
- Network Logs
- Passive Network Traffic

Agenda

1. Introduction
2. Challenges in OT Environments
3. Our Solution
4. Use Cases
5. Concluding Comments

Targeted Use Cases

External Boundary Activity

Unauthorized Protocol Usage
VPN Failed Login Attempts
VPN Suspicious User Login
VPN Suspicious Login Time
VPN Suspicious Geographical Login
Anomalous Stateful Connections
Attempts for Unauthorized Stateful Connections
Blacklisted IP Access Attempt (e.g. Facebook)
Firewall Rule Changes/Integrity Check
External IP Exposure

Internal Network Activity

Packet Payload Size Increase
Suspicious Network Scanning Activity
Unauthorized Bridged Networks
Rogue Network Device Detection
Use of External Device/Media (e.g. USB, serial)
Physical Changes to PLC/RTU (e.g. IO card)
Anomalous Network Time Protocol Traffic
Substantial Increase in Network Traffic
Suspicious PLC/RTU Comm Port Access
Port Security Violations

Status & Trend Information

OS Patch Status (e.g. up to date)
Application Patch Status
PLC Firmware Patch Status
HMI Firmware Patch Status
Anti-Malware Status
Anti-Virus Status
HIDS Status
Device Uptime Trend Analysis Over Time
Device Inbound Traffic (Host Volume) Trend Analysis Over Time
Device Outbound Traffic (Host Volume) Trend Analysis Over Time
Device Protocol Trend Analysis Over Time
Default Credential Use on Devices
Default Credential Use on ICS App
Default Credential Use on Workstation
Web Interface Activated on Device (e.g. PLC)
Unauthorized Remote Tools on Host (e.g. RDP, VNC)
OS Configuration Change Activated Wireless Drivers
Near Capacity Log Storage
Win 911 Stats

OT Device Monitoring

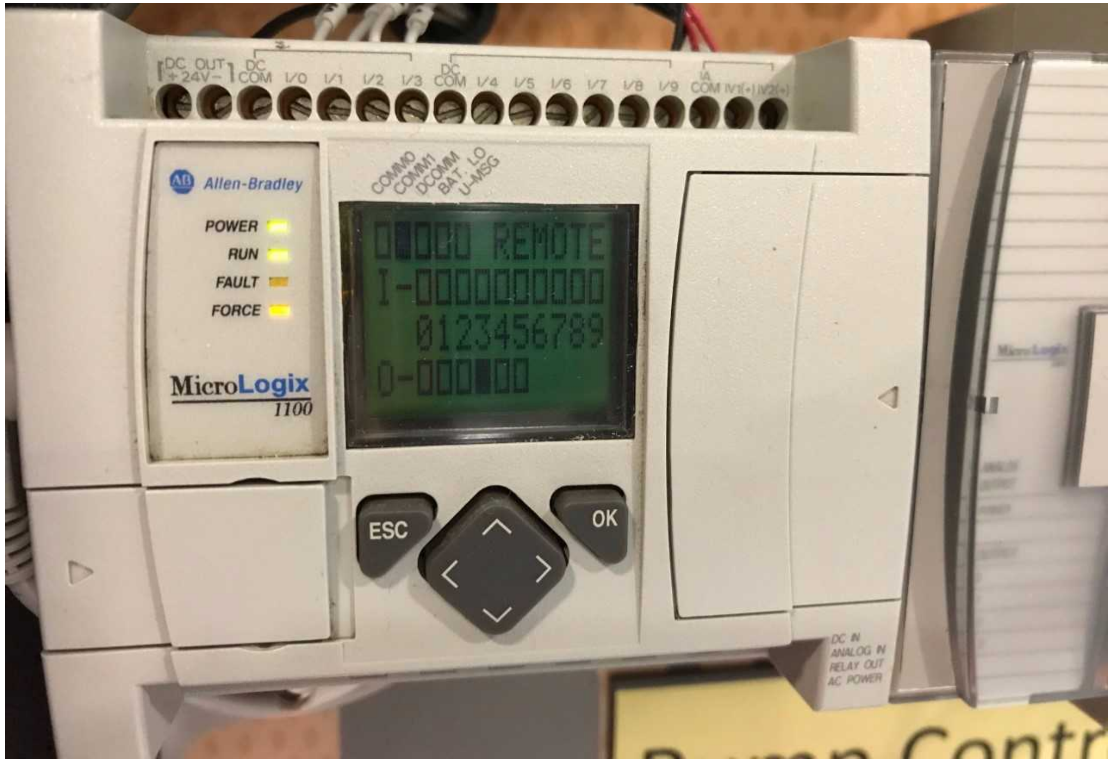
PLC Firmware Changes
HMI Firmware Changes
PLC Status Mode Changes
PLC Response Times/Latency
PLC Scan Rate Frequency
PLC/RTU Log Mods Stats

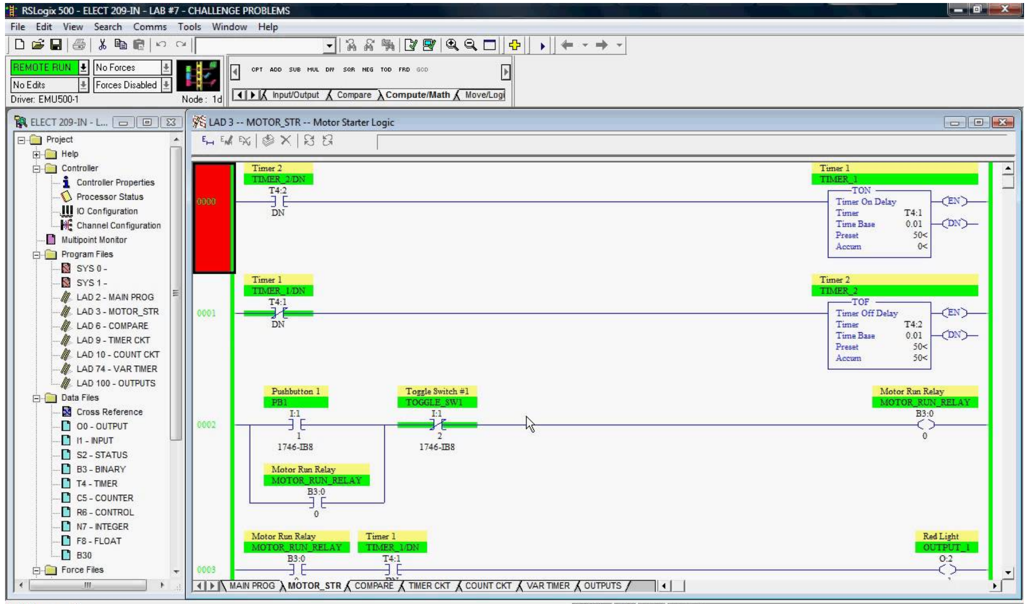
Account Information

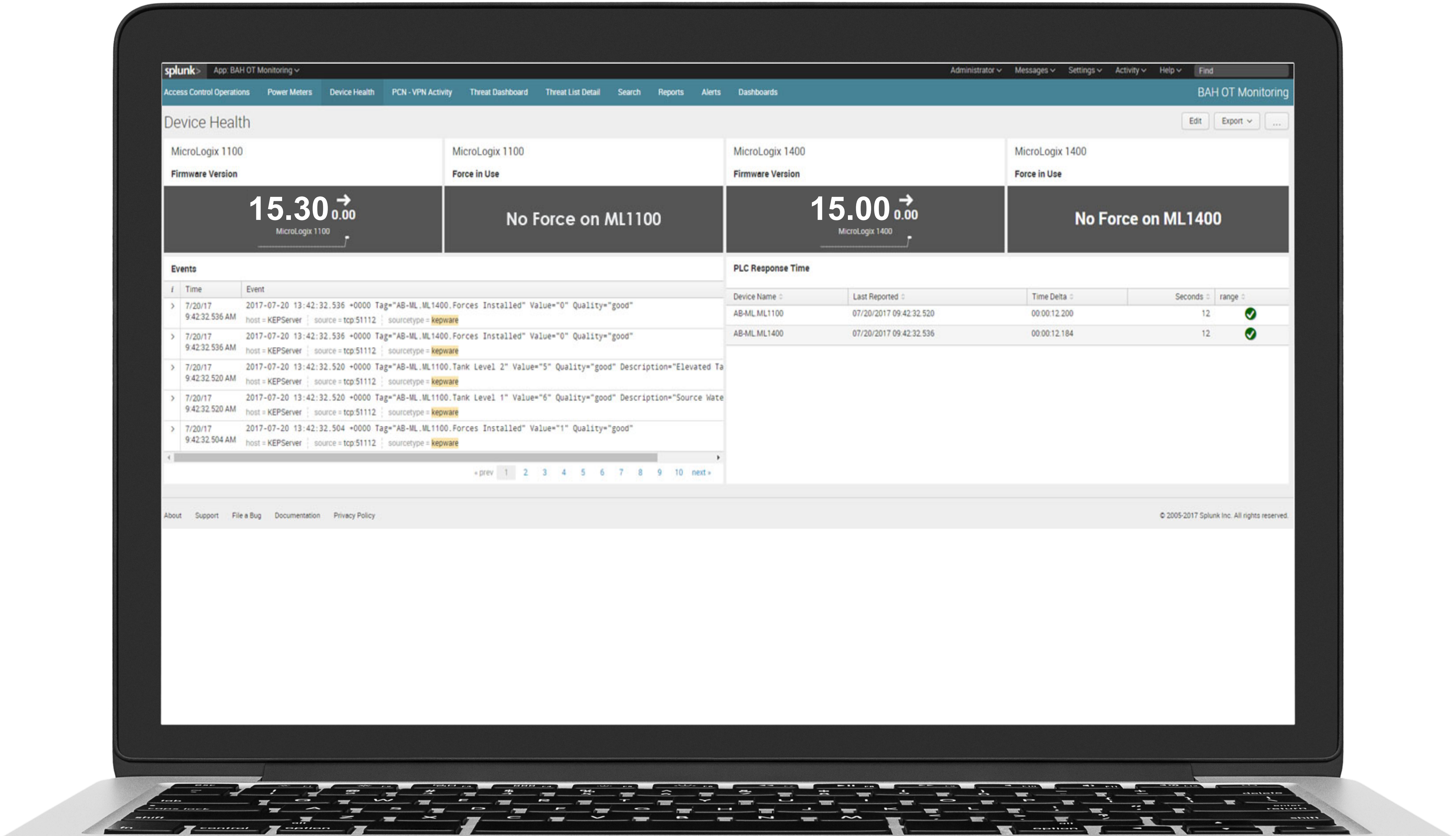
OS Account Creation
ICS Application Account Creation
PLC/RTU Account Modification HMI Account Creation
AD/LDAP Account Creation
OS Group Assignment
Workstation Account Lockout
PLC Account Lockout
HMI Account Lockout
Server Account Lockout
Infrastructure Account Lockout
HMI Failed Login
Infrastructure Failed Login
PLC Failed Login Attempts
Workstation Failed Login Attempts
Server Failed Login Attempts

Example Use Case #1 - Controller Manipulation

- Purpose
  - Identify changes to the logic (programming), firmware, or configuration settings on a controller







Device Health

MicroLogix 1100

Firmware Version

15.30 → 0.00

MicroLogix 1100

MicroLogix 1100

Force in Use

No Force on ML1100

MicroLogix 1400

Firmware Version

15.00 → 0.00

MicroLogix 1400

MicroLogix 1400

Force in Use

No Force on ML1400

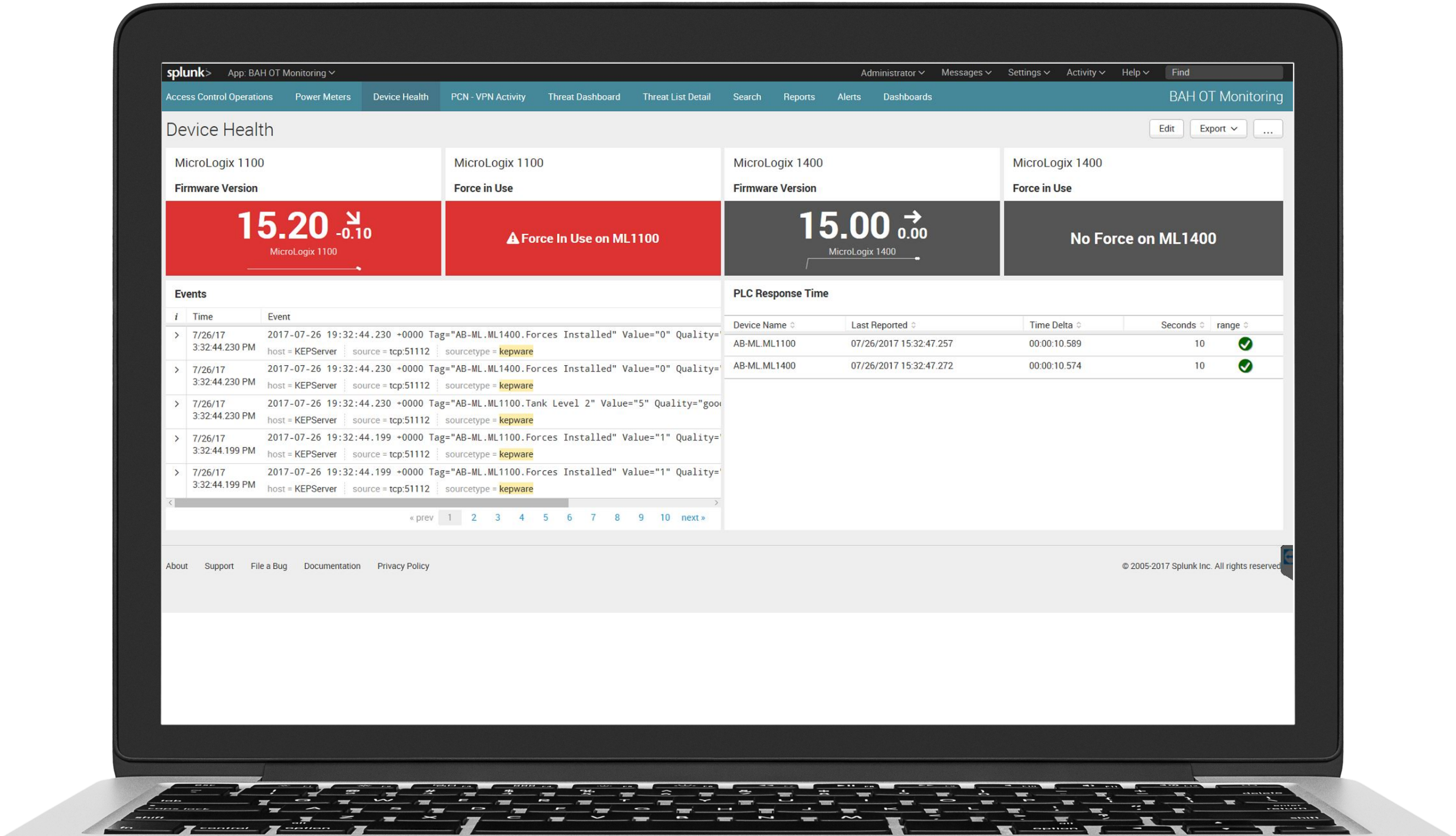
Events

i	Time	Event
>	7/20/17 9:42:32.536 AM	2017-07-20 13:42:32.536 +0000 Tag="AB-ML.ML1400.Forces Installed" Value="0" Quality="good" host = KEPServer ⁝ source = tcp:51112 ⁝ sourcetype = kepware
>	7/20/17 9:42:32.536 AM	2017-07-20 13:42:32.536 +0000 Tag="AB-ML.ML1400.Forces Installed" Value="0" Quality="good" host = KEPServer ⁝ source = tcp:51112 ⁝ sourcetype = kepware
>	7/20/17 9:42:32.520 AM	2017-07-20 13:42:32.520 +0000 Tag="AB-ML.ML1100.Tank Level 2" Value="5" Quality="good" Description="Elevated Ta host = KEPServer ⁝ source = tcp:51112 ⁝ sourcetype = kepware
>	7/20/17 9:42:32.520 AM	2017-07-20 13:42:32.520 +0000 Tag="AB-ML.ML1100.Tank Level 1" Value="6" Quality="good" Description="Source Wate host = KEPServer ⁝ source = tcp:51112 ⁝ sourcetype = kepware
>	7/20/17 9:42:32.504 AM	2017-07-20 13:42:32.504 +0000 Tag="AB-ML.ML1100.Forces Installed" Value="1" Quality="good" host = KEPServer ⁝ source = tcp:51112 ⁝ sourcetype = kepware

« prev 1 2 3 4 5 6 7 8 9 10 next »

PLC Response Time

Device Name	Last Reported	Time Delta	Seconds	range
AB-ML.ML1100	07/20/2017 09:42:32.520	00:00:12.200	12	✓
AB-ML.ML1400	07/20/2017 09:42:32.536	00:00:12.184	12	✓



Device Health

MicroLogix 1100
Firmware Version
15.20 ↘ -0.10
MicroLogix 1100

MicroLogix 1100
Force in Use
⚠ Force In Use on ML1100

MicroLogix 1400
Firmware Version
15.00 → 0.00
MicroLogix 1400

MicroLogix 1400
Force in Use
No Force on ML1400

Events

i	Time	Event
>	7/26/17 3:32:44.230 PM	2017-07-26 19:32:44.230 +0000 Tag="AB-ML.ML1400.Forces Installed" Value="0" Quality=" host = KEPServer source = tcp:51112 sourcetype = kepware
>	7/26/17 3:32:44.230 PM	2017-07-26 19:32:44.230 +0000 Tag="AB-ML.ML1400.Forces Installed" Value="0" Quality=" host = KEPServer source = tcp:51112 sourcetype = kepware
>	7/26/17 3:32:44.230 PM	2017-07-26 19:32:44.230 +0000 Tag="AB-ML.ML1100.Tank Level 2" Value="5" Quality="goo host = KEPServer source = tcp:51112 sourcetype = kepware
>	7/26/17 3:32:44.199 PM	2017-07-26 19:32:44.199 +0000 Tag="AB-ML.ML1100.Forces Installed" Value="1" Quality=" host = KEPServer source = tcp:51112 sourcetype = kepware
>	7/26/17 3:32:44.199 PM	2017-07-26 19:32:44.199 +0000 Tag="AB-ML.ML1100.Forces Installed" Value="1" Quality=" host = KEPServer source = tcp:51112 sourcetype = kepware

« prev 1 2 3 4 5 6 7 8 9 10 next »

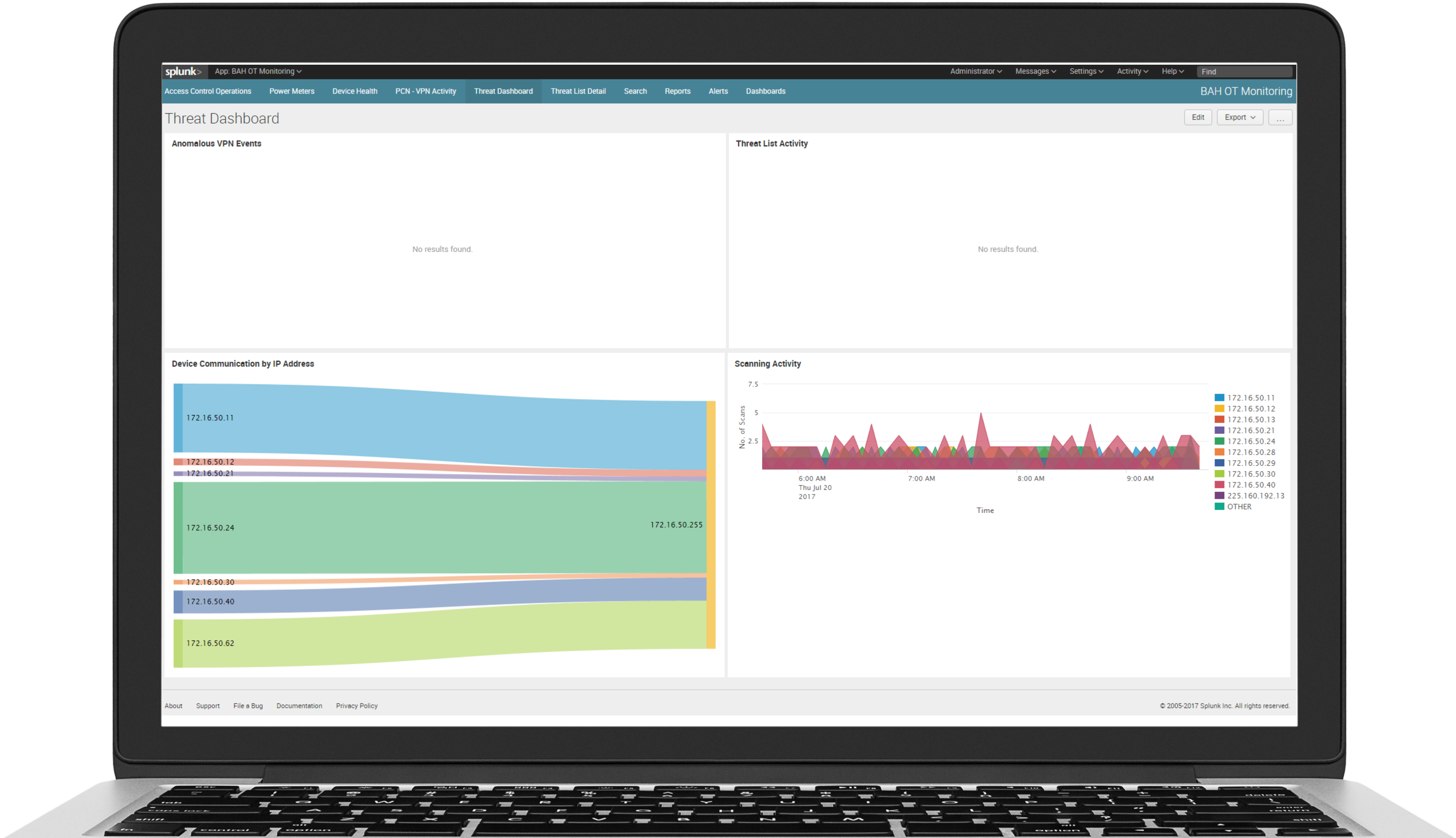
PLC Response Time

Device Name	Last Reported	Time Delta	Seconds	range
AB-ML.ML1100	07/26/2017 15:32:47.257	00:00:10.589	10	✓
AB-ML.ML1400	07/26/2017 15:32:47.272	00:00:10.574	10	✓

© 2005-2017 Splunk Inc. All rights reserved

Example Use Case #2 - Anomalous Traffic

- Purpose
  - Develop a baseline of normal traffic throughout the network
  - Identify network traffic that is out of normal bounds
    - Inbound/outbound # of connections
    - Inbound/outbound # of hosts
    - Inbound/outbound # of ports
  - Tuned around the most critical assets



Threat Dashboard

Anomalous VPN Events

No results found.

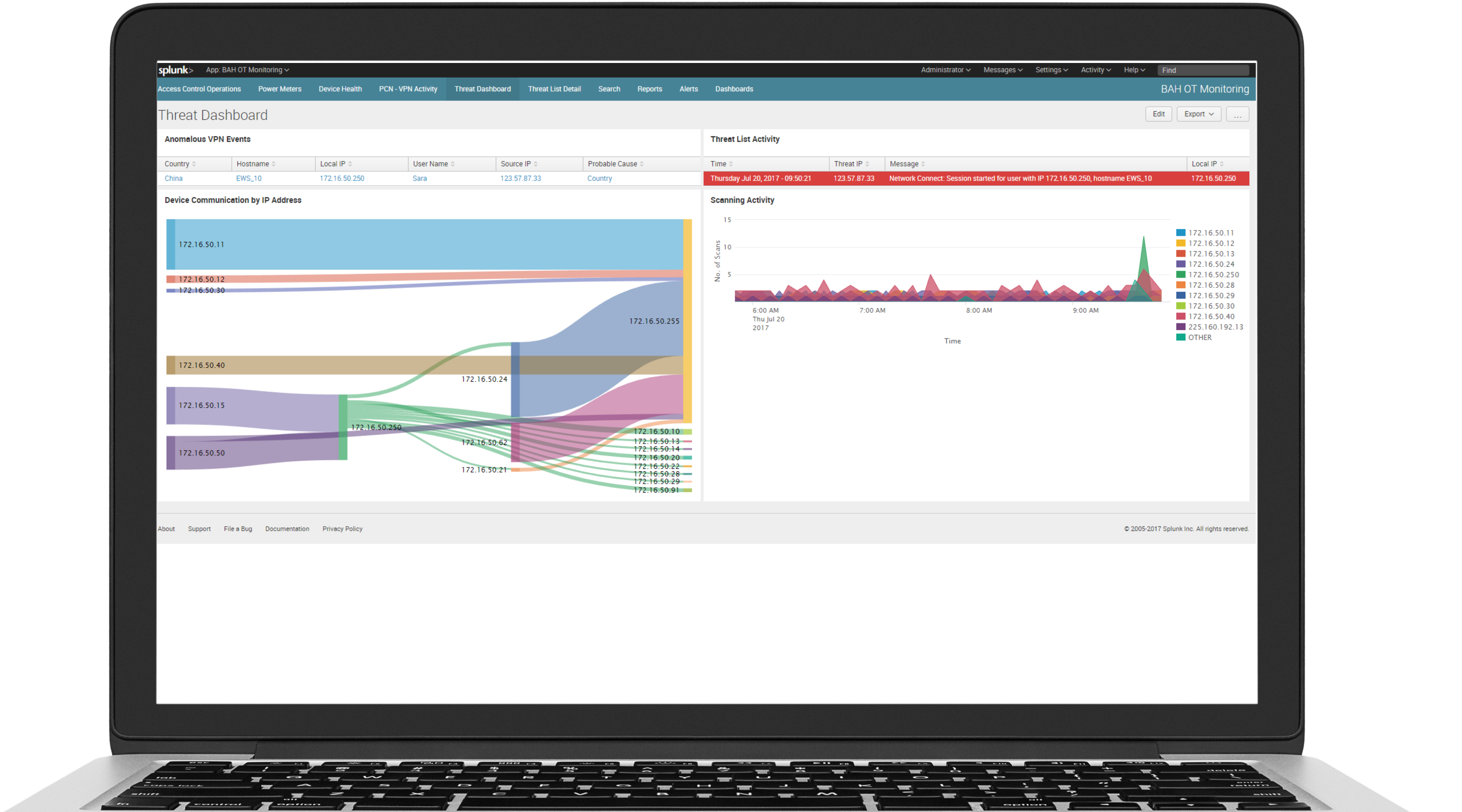
Threat List Activity

No results found.

Device Communication by IP Address

Scanning Activity

© 2005-2017 Splunk Inc. All rights reserved.



Threat Dashboard

Anomalous VPN Events

Country	Hostname	Local IP	User Name	Source IP	Probable Cause
China	EWS_10	172.16.50.250	Sara	123.57.87.33	Country

Threat List Activity

Time	Threat IP	Message	Local IP
Thursday Jul 20, 2017 - 09:50:21	123.57.87.33	Network Connect: Session started for user with IP 172.16.50.250, hostname EWS_10	172.16.50.250

Device Communication by IP Address

Scanning Activity

© 2005-2017 Splunk Inc. All rights reserved.

Example Use Case #3 - Improper Traffic Flow

- Purpose
  - Identify unanticipated or misconfigured traffic flows throughout the network
  - Identify communications that may require specific firewall rules to be put in place

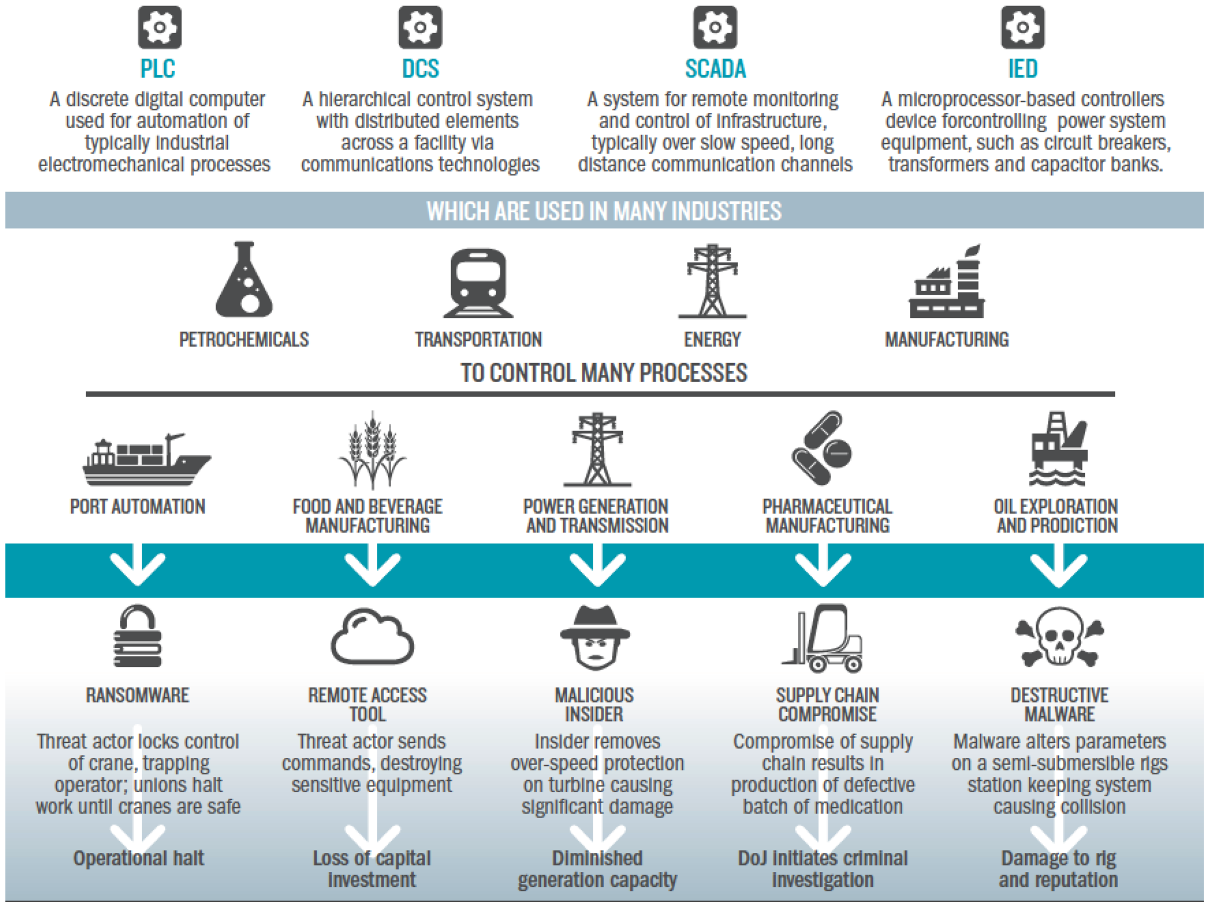
- Outcome
  - Correct misconfigurations that may impact plant operations
  - Provide administrators information necessary to implement network segmentation

Agenda

1. Introduction
2. Challenges in OT Environments
3. Our Solution
4. Use Cases
5. Concluding Comments

The OT Landscape

- Businesses **require a digital footprint** to support optimization, improve safety, and increase automation – but to do this successfully, it must also be secure
- Business is a set of **critical operational processes** – not just connected components
- Traditional IT protection mechanisms are not always feasible in these environments, so **visibility is paramount**



PLC
A discrete digital computer used for automation of typically industrial electromechanical processes

DCS
A hierarchical control system with distributed elements across a facility via communications technologies

SCADA
A system for remote monitoring and control of infrastructure, typically over slow speed, long distance communication channels

IED
A microprocessor-based controllers device forcontrolling power system equipment, such as circuit breakers, transformers and capacitor banks.

WHICH ARE USED IN MANY INDUSTRIES

PETROCHEMICALS

TRANSPORTATION

ENERGY

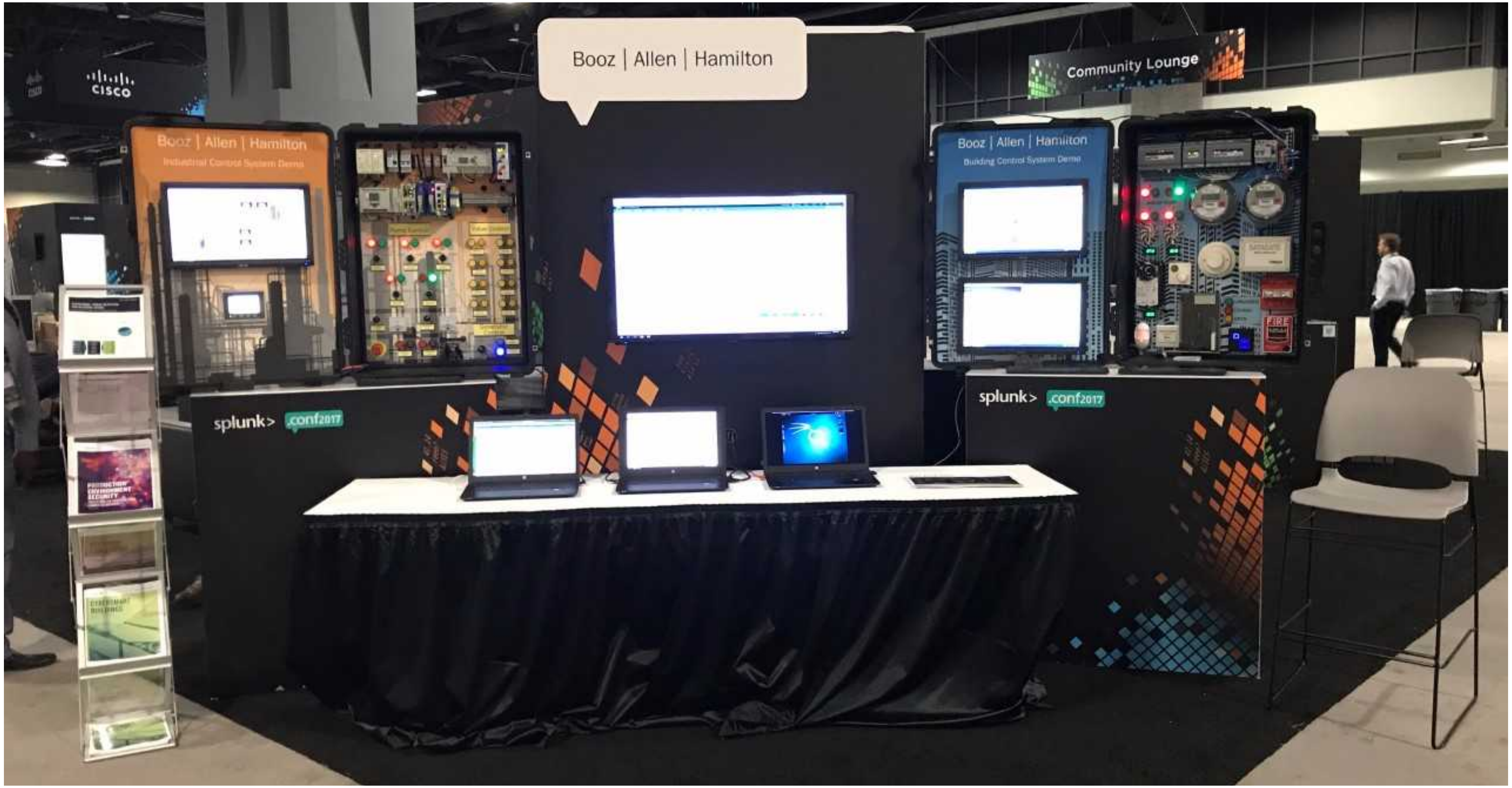
MANUFACTURING

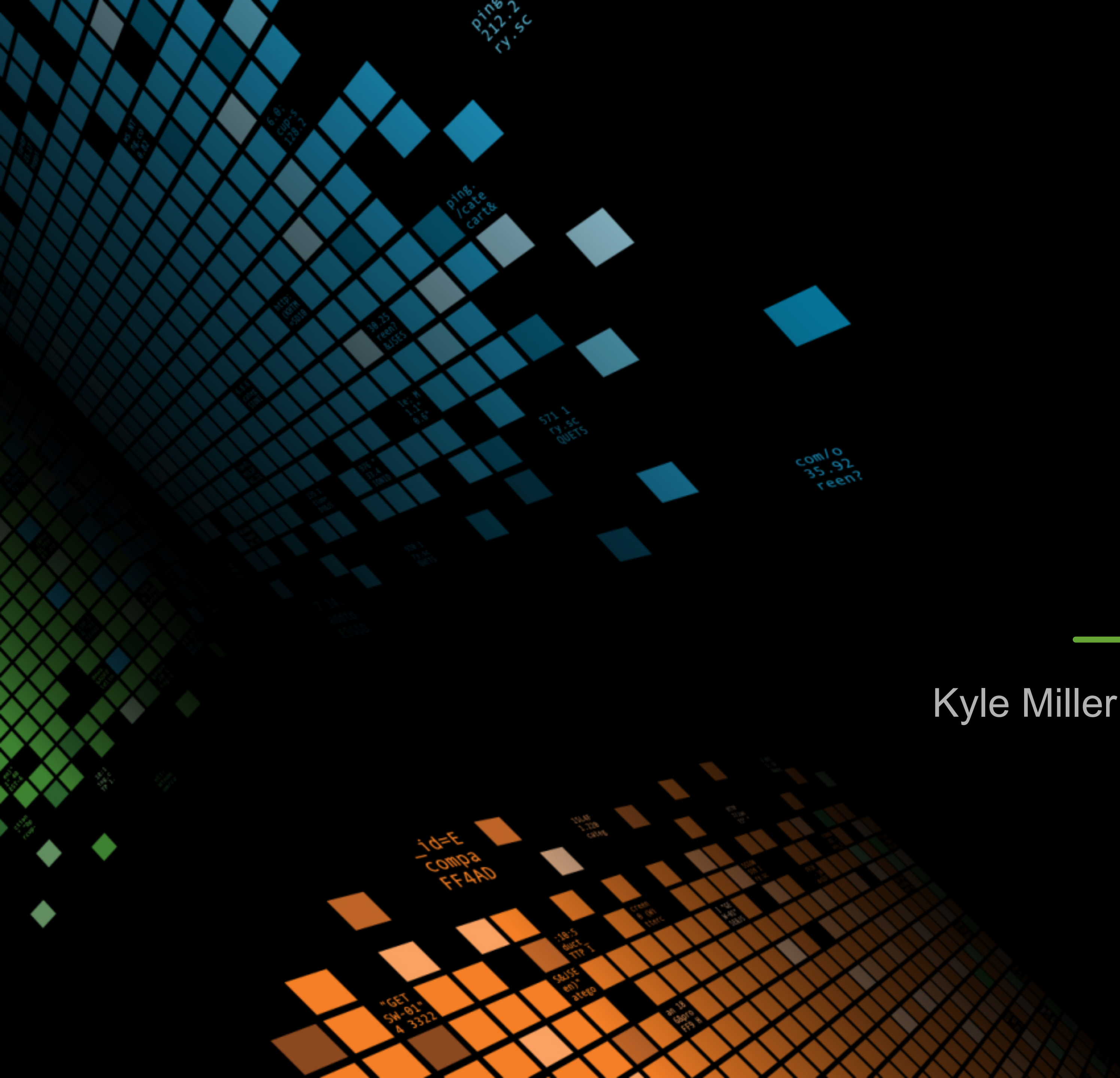
TO CONTROL MANY PROCESSES

PORT AUTOMATION	FOOD AND BEVERAGE MANUFACTURING	POWER GENERATION AND TRANSMISSION	PHARMACEUTICAL MANUFACTURING	OIL EXPLORATION AND PRODICTION
RANSOMWARE	REMOTE ACCESS TOOL	MALICIOUS INSIDER	SUPPLY CHAIN COMPROMISE	DESTRUCTIVE MALWARE
Threat actor locks control of crane, trapping operator; unions halt work until cranes are safe	Threat actor sends commands, destroying sensitive equipment	Insider removes over-speed protection on turbine causing significant damage	Compromise of supply chain results in production of defective batch of medication	Malware alters parameters on a semi-submersible rigs station keeping system causing collision
Operational halt	Loss of capital investment	Diminished generation capacity	DoJ initiates criminal investigation	Damage to rig and reputation

Our Demo Lab

Come check out our booth!





Q&A

Kyle Miller | Industrial Cyber Security Engineer

Thank You

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

splunk> .conf2017