

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.

Splunk, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2017 Splunk Inc. All rights reserved.

Agenda

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



Kyle Miller

Senior Lead Engineer

Industrial Cyber Security

Booz | Allen | Hamilton

Introduction

- 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)

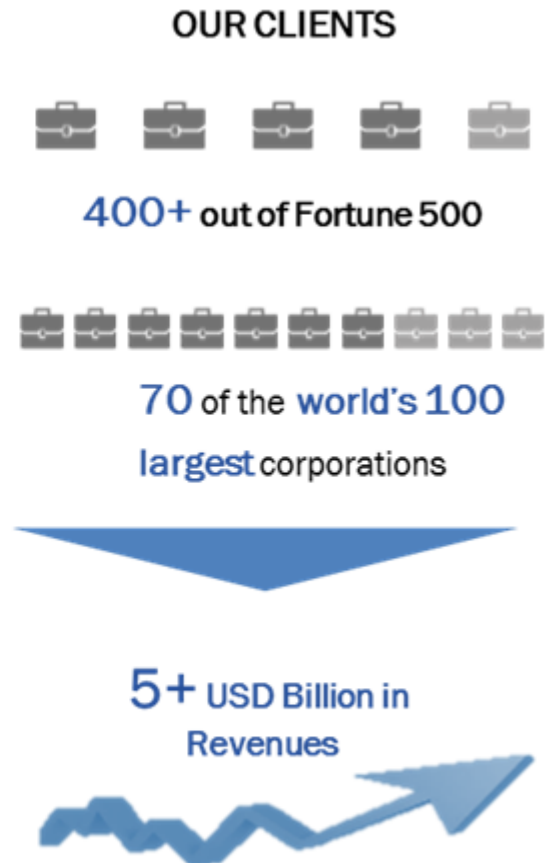
Education

- 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



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

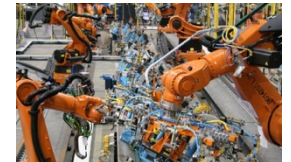
Oil & Gas Exploration, Production, Distribution, and Refining



Electric Power Generation, Transmission, and Distribution



Manufacturing



Water, Wastewater, and Public Utilities



Building Control Systems and Smart Cities





- ## COMPLEXITY

- ## BUSINESS DRIVERS

- 

Visibility is a Key Challenge

The Tip of the Iceberg

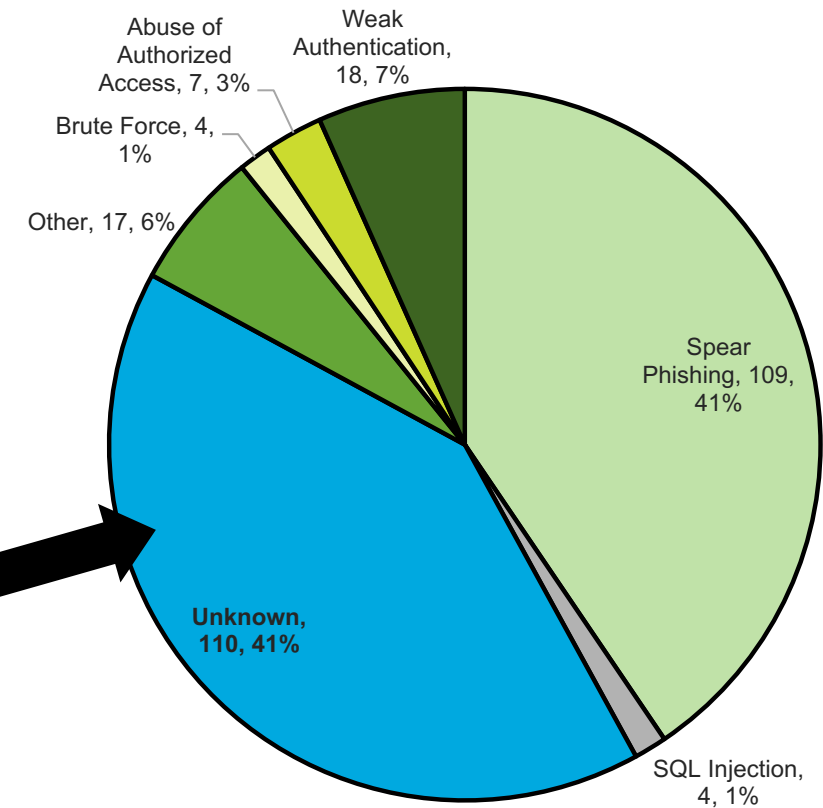
- With these increasing challenges, **traditional cyber protection** mechanisms are not always **feasible**
- Therefore, **obtaining visibility** into these environments to assist with cybersecurity efforts is critical
- Very few OT environments have any form of advanced cyber monitoring in place

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

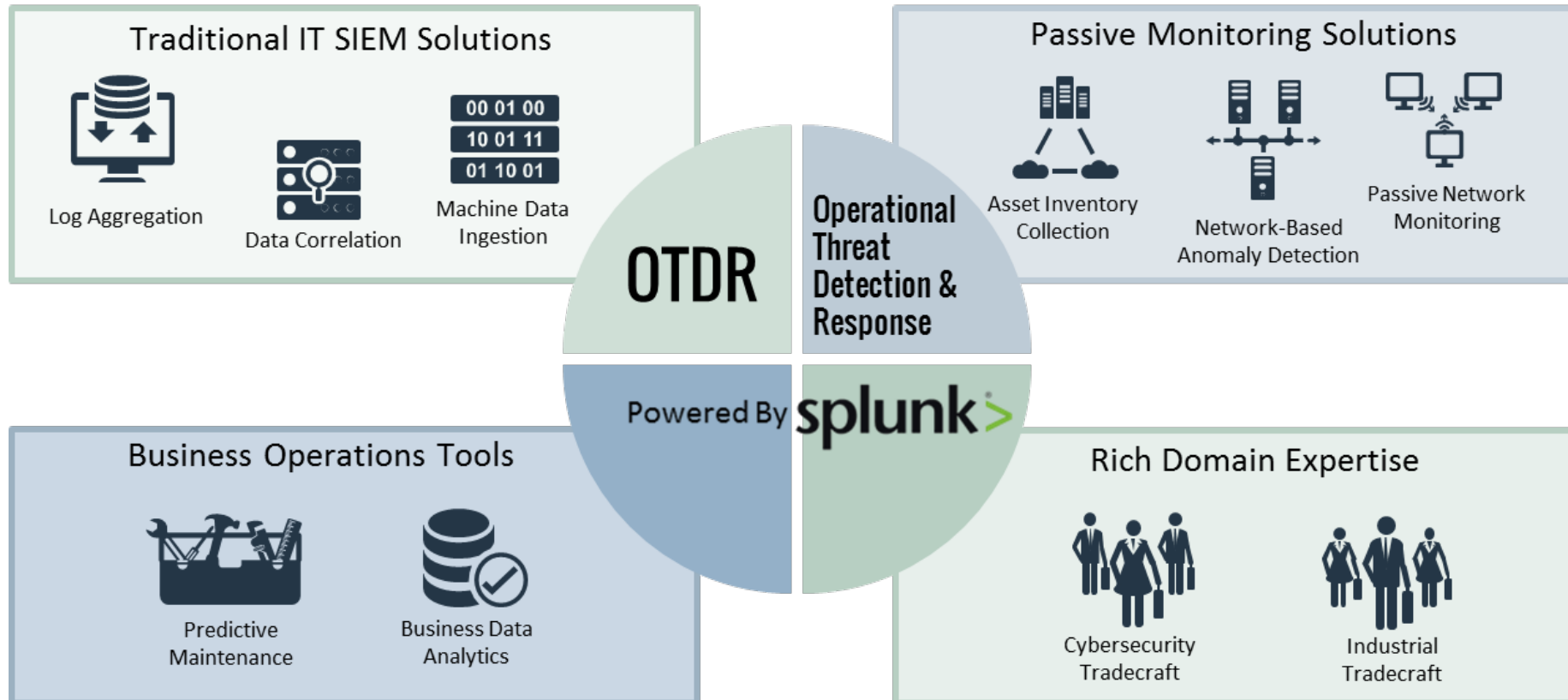
1. Introduction
2. Challenges in OT Environments
3. Our Solution

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

Ask Any Question



Application Delivery

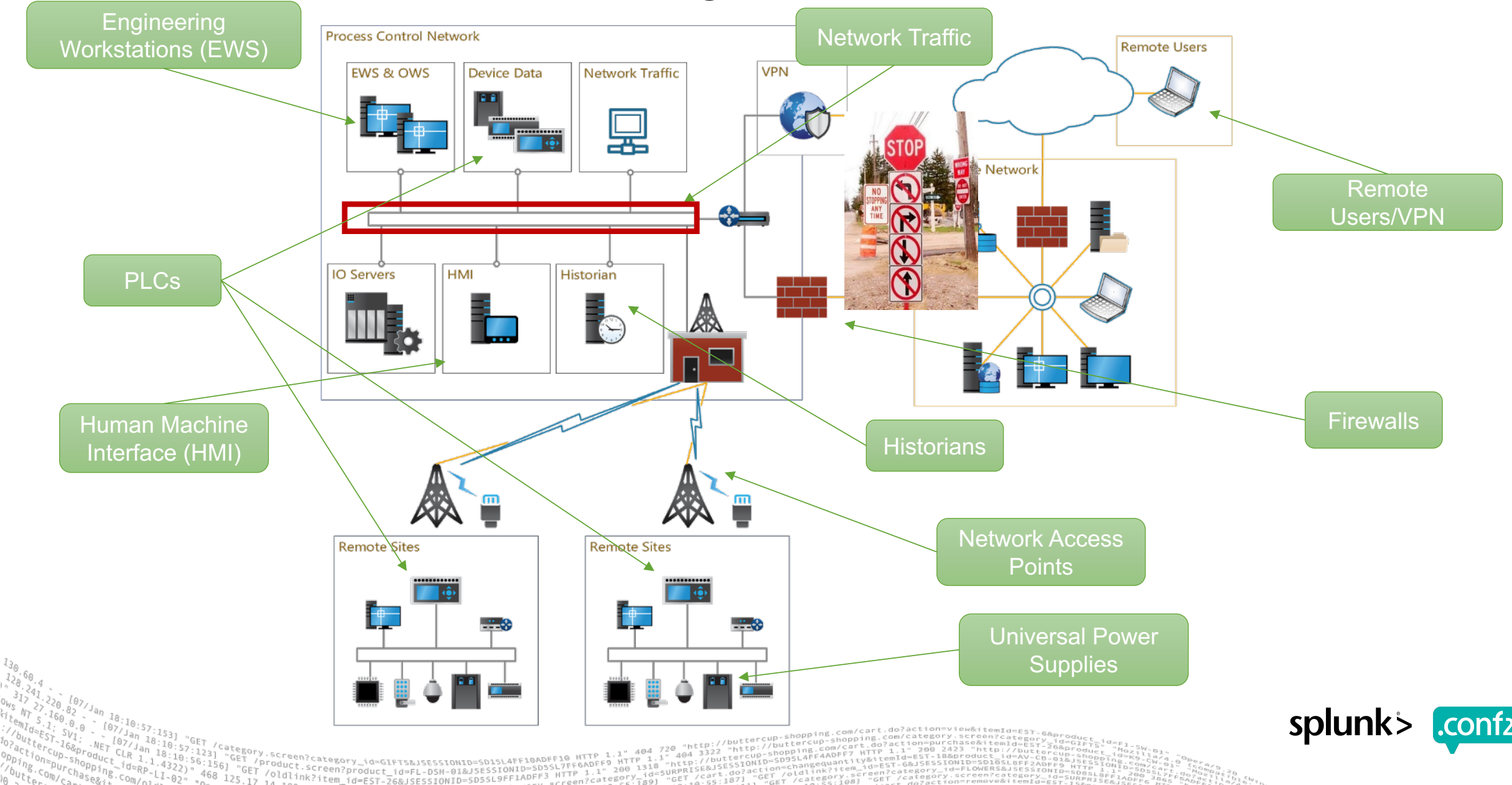
IT Operations

Security, Compliance and Fraud

Business Analytics

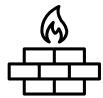
Industrial Data and the Internet of Things

Where can you Extract Data?



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



Equipment

Suspicious Event shut down immediately



Equipment

10.119.1.1 VPN: 10/04/2016 16:55:14 - VPN-2 - [175.45.177.7] acme\srtabrunevans(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 Source IP dwmi_type=UserAccounts

2016-08-18 12:40:16.311 +0000 Tag=""AB-M...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-ME1100-03 FW 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	Firmware Modification	logged in from	10.11.36.20.	0x0016
------------	----------	-----------------------	----------------	--------------	--------

10/04/2016	19:07:32	System: Update successful.	0x004A	Source IP
------------	----------	----------------------------	--------	-----------

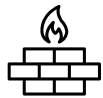
10/04/2016	19:13:40	UPS: The battery power is too low to support the load; if power fails, the UPS will be
------------	----------	--

Suspicious Event shut down immediately

shut down immediately

What Does OT Machine Data Look Like?

DATA SOURCES



Firewall/VPN



Human Machine Interface (HMI)



Programmable Logic Controller (PLC)



Equipment

Suspicious IP
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

Source IP
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 **Source IP** dwmi_type=UserAccounts

Firmware Modification
2016-08-18 12:40:16.311 +0000 Tag=""AB-MEM1100.03 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

Firmware Modification
2016-10-04 18:40:16.311 +0000 Tag=""AB-MEM1100.03 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

Source IP
10/04/2016 19:02:49 **Firmware Modification** logged in from 10.11.36.20. 0x0016

10/04/2016 19:07:32 System: Update successful. 0x004A **Source IP**

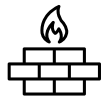
10/04/2016 19:13:40 UPS: The battery power is too low to support the load; if power fails, the UPS will be

Suspicious Event shut down immediately

130.60.4 - - [07/Jun 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=5D5L9FF1ADFF3 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&item_id=EST-6&product_id=FI-SW-03" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)" "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5D5L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&item_id=EST-18&product_id=AV-CB-01&SESSIONID=5D5L9FF1ADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=purchase&item_id=EST-16&product_id=RP-LI-02" 468 125.17 14.000000

What Does OT Machine Data Look Like?

DATA SOURCES



Firewall/VPN



Human Machine Interface (HMI)



Programmable Logic Controller (PLC)



Equipment

Suspicious IP

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

Source IP

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 **Source IP** dwmi_type=UserAccounts

Firmware Modification

2016-08-18 12:40:16.311 +0000 Tag=""AB-MEMLE1100.03 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

Firmware Modification

2016-10-04 18:40:16.311 +0000 Tag=""AB-MEMLE1100.03 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

Source IP

10/04/2016 19:02:49 **Firmware Modification** logged in from 10.11.36.20. 0x0016

10/04/2016 19:07:32 System: Update successful. 0x004A **Source IP**

10/04/2016 19:13:40 UPS: The battery power is too low to support the load; if power fails, the UPS will be **Suspicious Event** shut down immediately

130.60.4 - - [07/Jun 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=5D5SL9FF1ADFF3 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&item_id=EST-6&product_id=FI-SW-03" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.14.189 "GET /category.screen?category_id=FLOWERS&SESSIONID=5D5SL9FF1ADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=purchase&item_id=EST-16&product_id=RP-LI-02" "0x0016



Equipment

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

20161004171221.000000Caption=ACME-2975EB\srta
LocalAccount = IP: 10.11.36.20 TrueName=acme\srta
500SIDType=1 Stat dwmi_type=UserAccounts

Source IP

2016-08-18 12:40:16.311 +0000 Tag="AB-172.16.50.32" value="527" Quality="good" description="Firmware Version", "2016-08-18T05:40:16.311-0700", 12 18 20 august 16 thursday, 2016, 0,, "172.16.50.32", kepware, 1

2016-10-04 18:40:16.311 +0000 Tag=""AB-ME-ME1100-03-FRM" 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	Firmware Modification	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



Time Range

Source IP

Source IP

Firmware Modification

Firmware Modification

Firmware Modification

Source IP

Source IP

Suspicious Event

All four occurring within a 3-hour period





Time Range

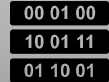
All four occurring within a 3-hour period

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

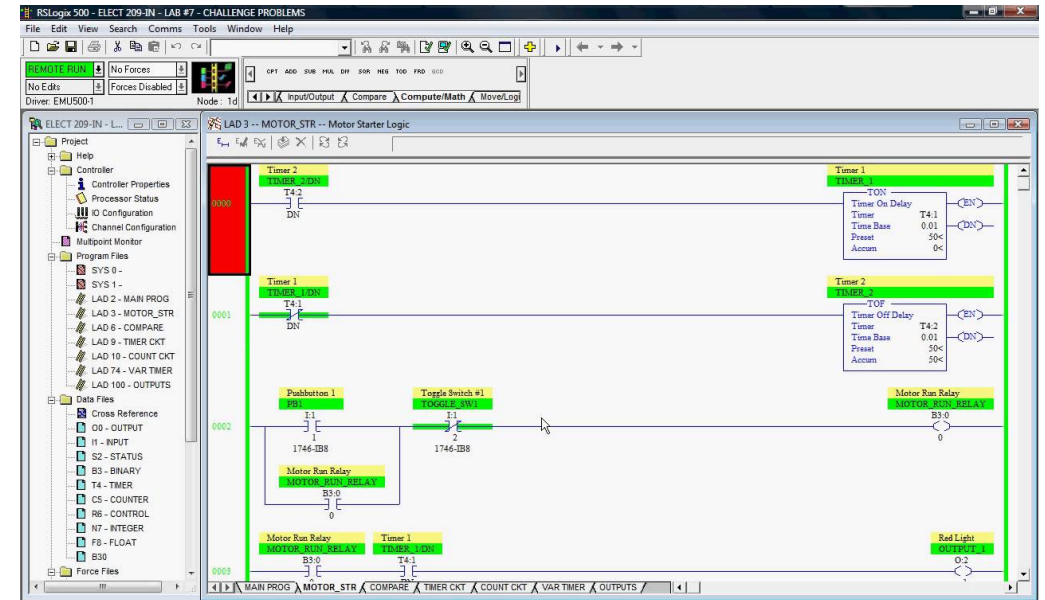
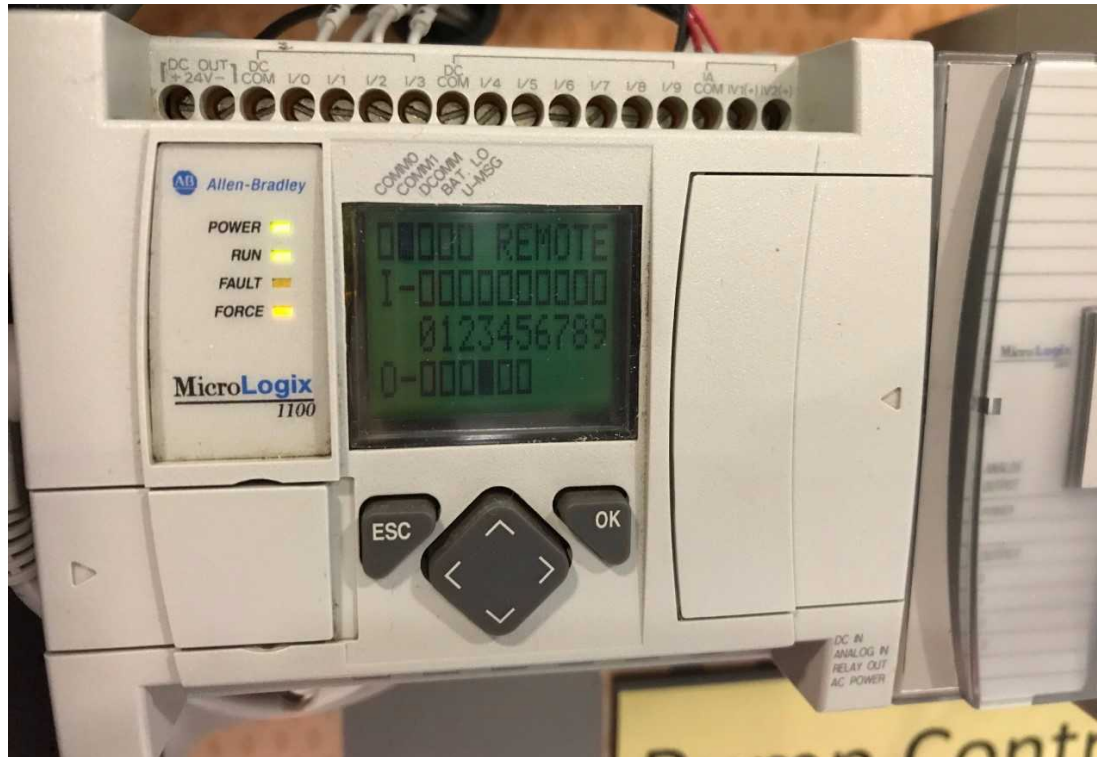
PLC Firmware Changes
 HMI Firmware Changes
 PLC Status Mode Changes
 PLC Response Times/Latency
 PLC Scan Rate Frequency
 PLC/RTU Log Mods Stats

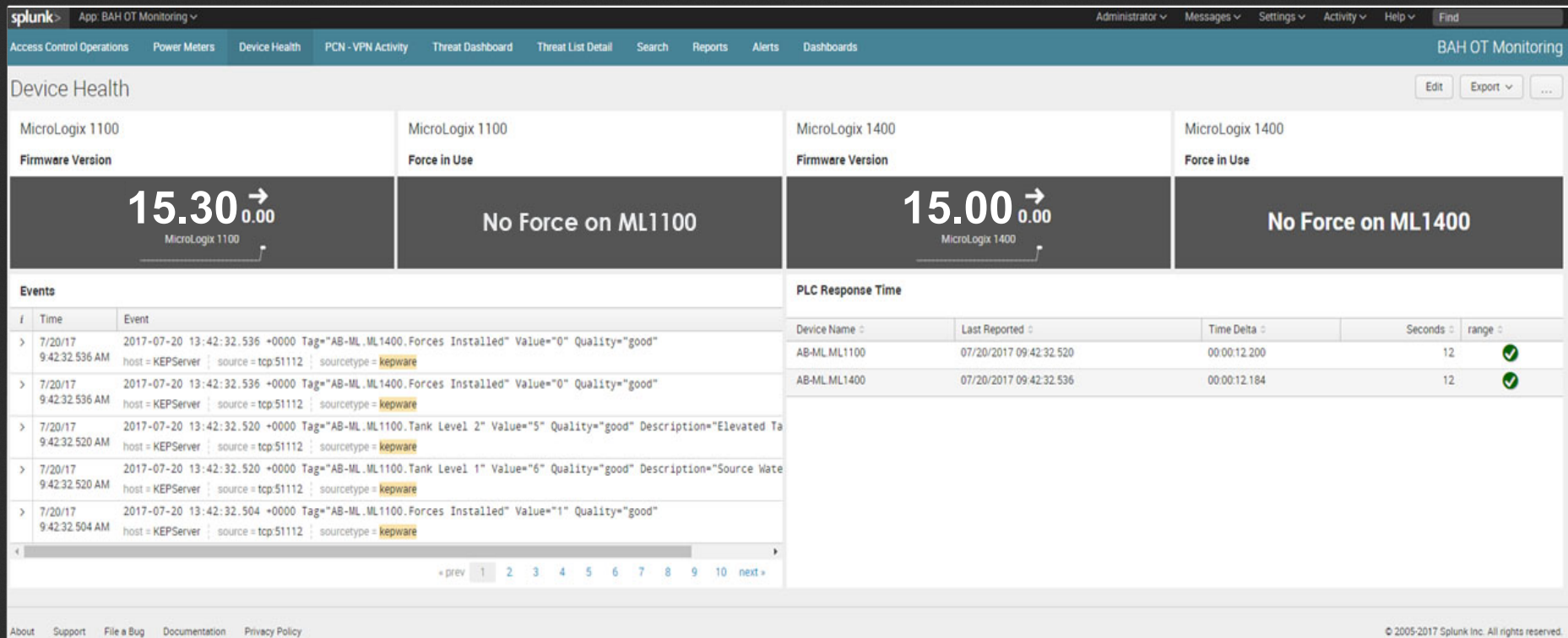
Account Information

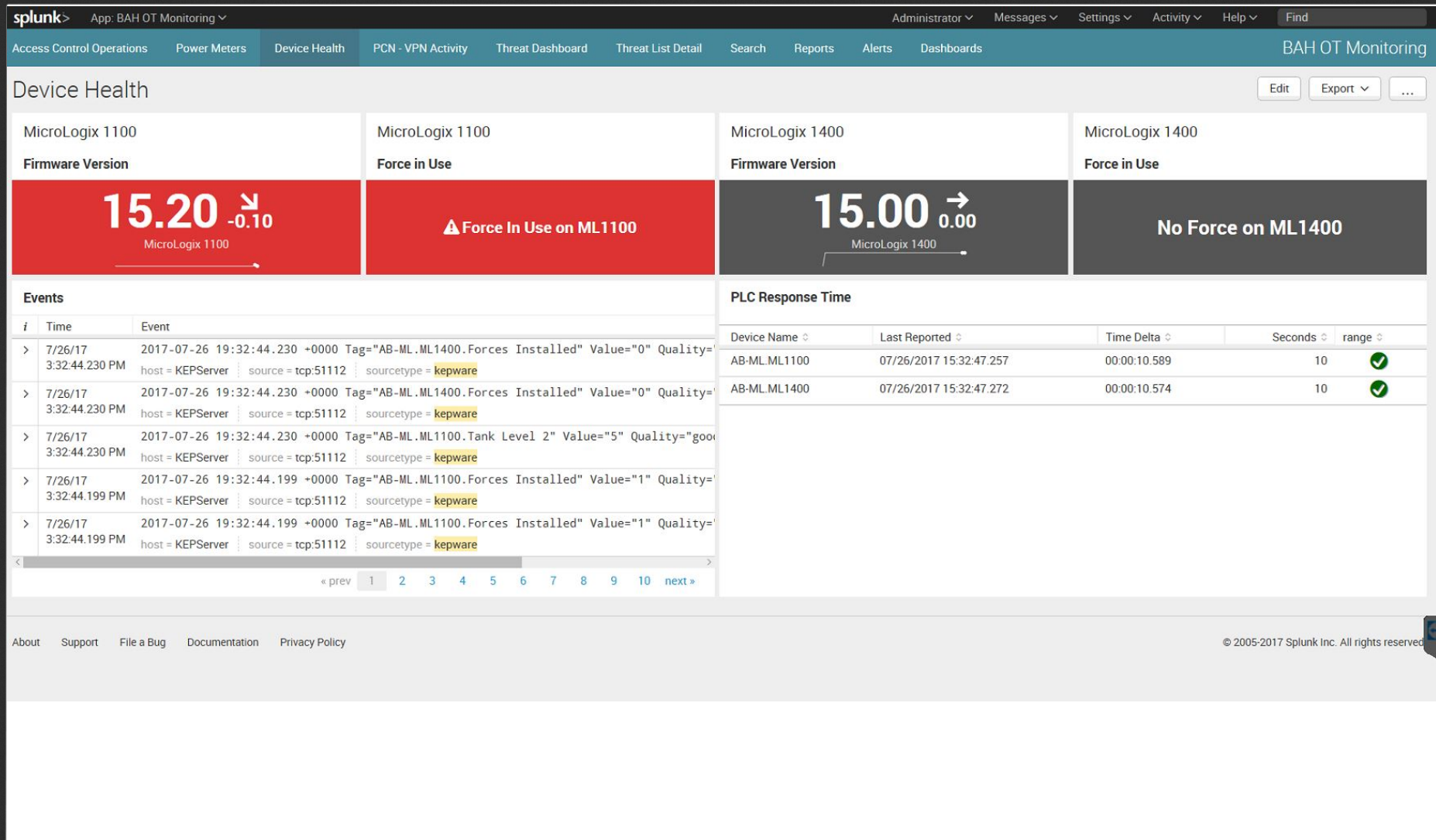
OS Account Creation
 ICS Application Account Creation
 PLC/RTU Account Modification HMI Account Creation
 AD/LDAP Account Creation
 OS Group Assignment
 Workstation Account Lockout
 PLC Account Lockout
 HMI Account Lockout
 Server Account Lockout
 Infrastructure Account Lockout
 HMI Failed Login
 Infrastructure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

► Purpose

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





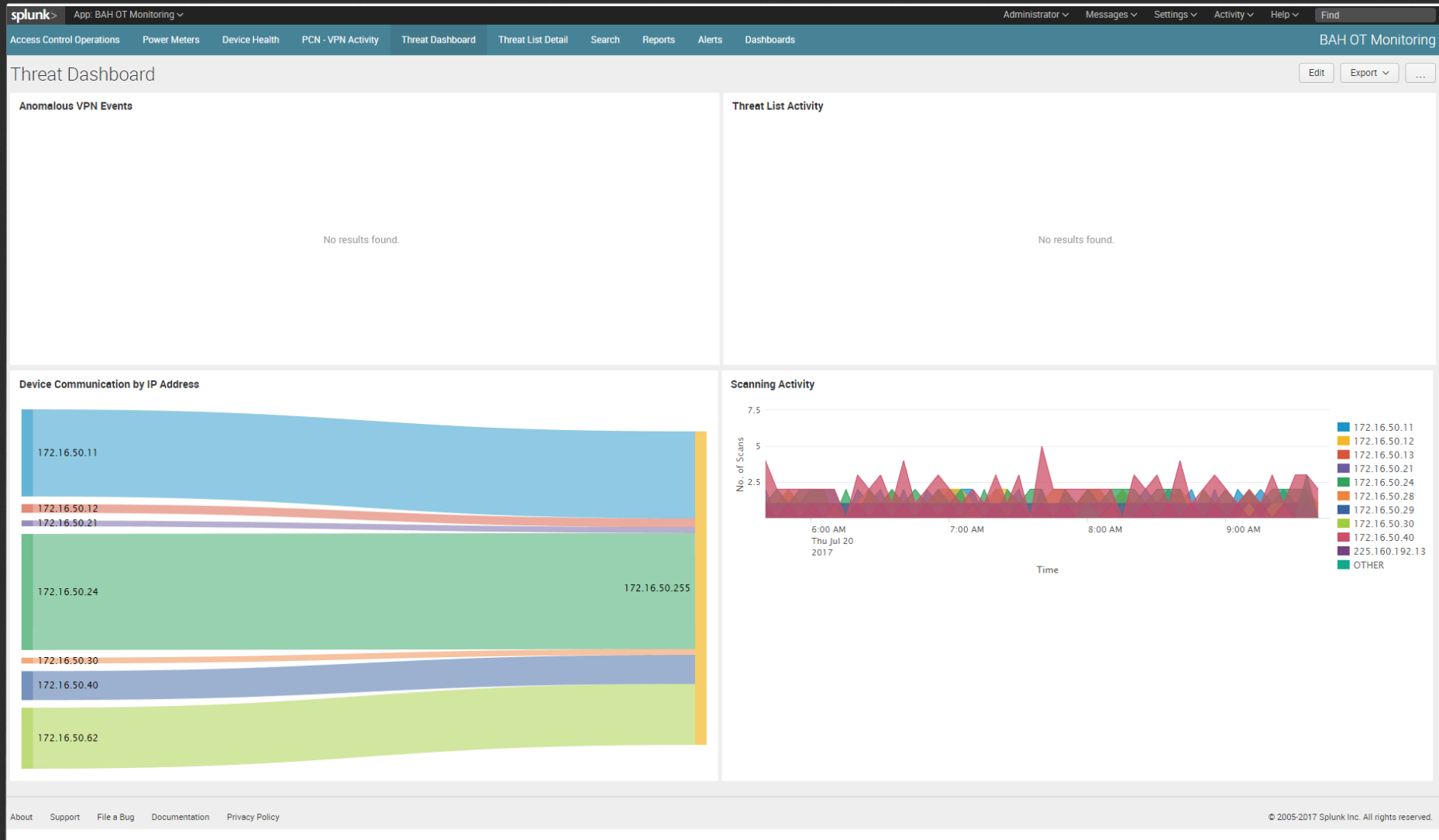


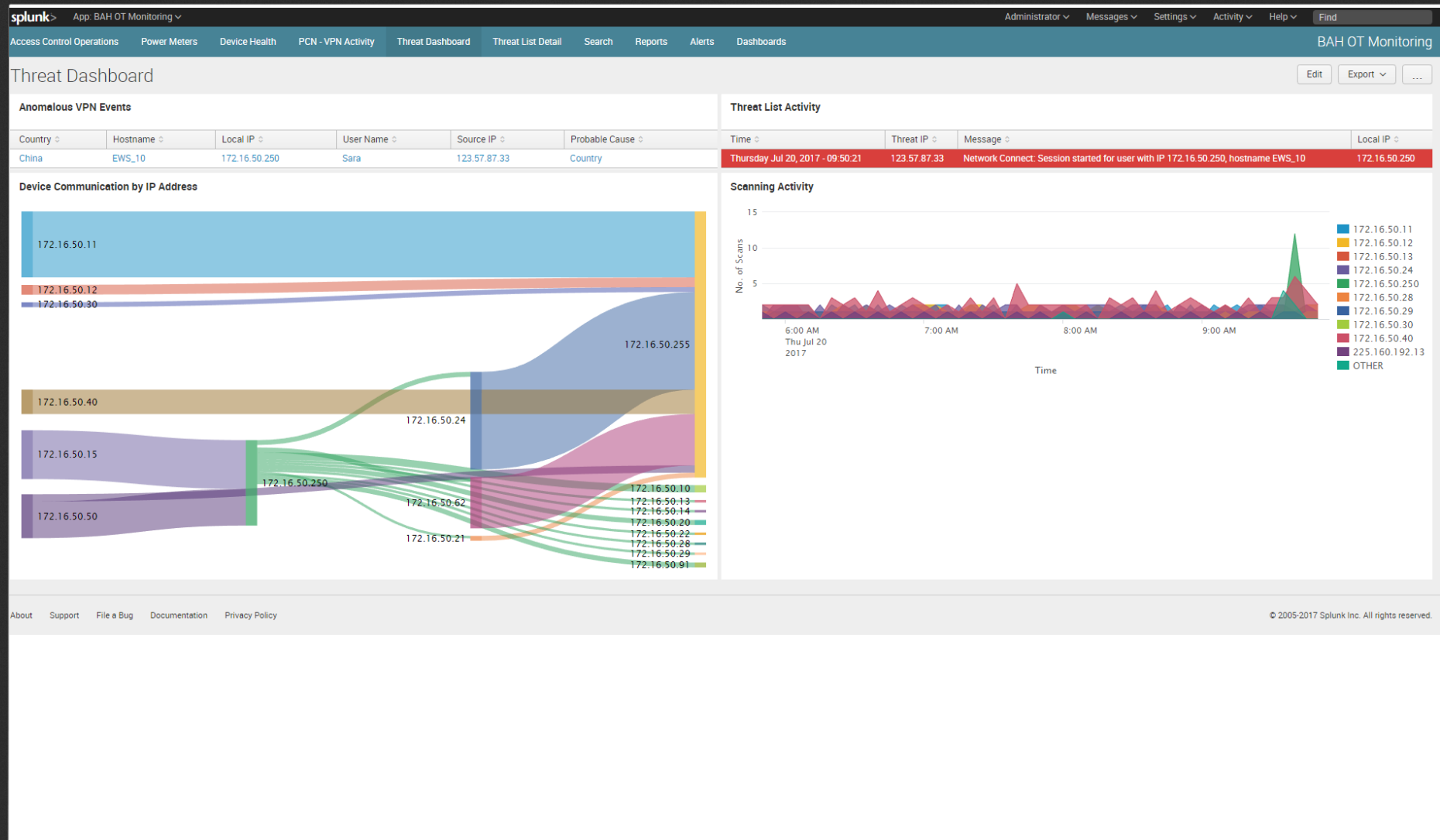
Example Use Case #2 - Anomalous Traffic

► 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

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=5D1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-SW-03"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5D5SL7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/category.screen?category_id=GIFTS"
317 27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&SESSIONID=5D5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=FL-DSH-01"
125.17.14.189 - - [07/Jan 18:10:55:187] "GET /category.screen?category_id=FLOWERS&SESSIONID=5D5SL8FF1ADFF3 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS"
128.241.220.82 - - [07/Jan 18:10:55:187] "GET /category.screen?category_id=FLOWERS&SESSIONID=5D5SL8FF1ADFF3 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS"





► Purpose

- ## ► Outcome

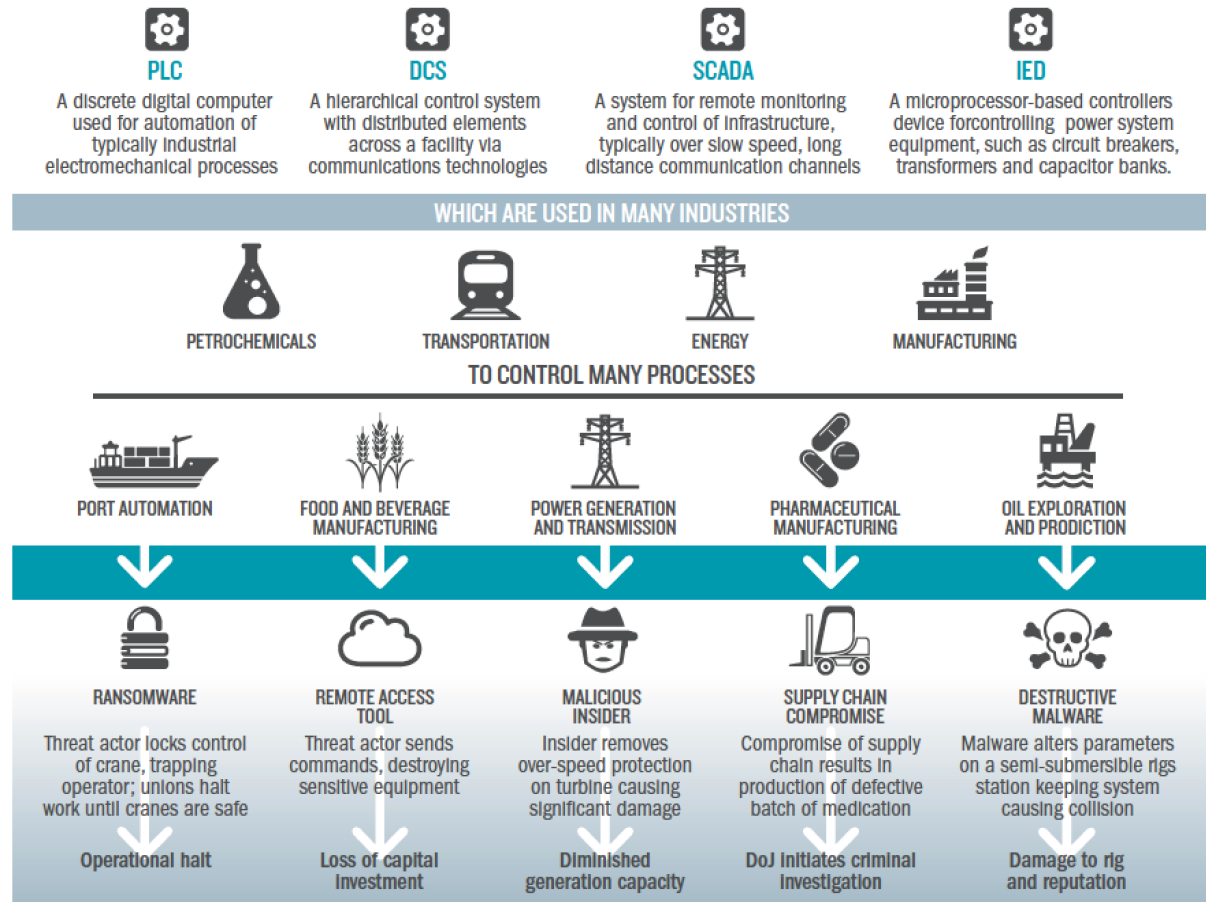
- Correct misconfigurations that may impact plant operations
- Provide administrators information necessary to implement network segmentation

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**



Q&A

Kyle Miller | Industrial Cyber Security Engineer

Thank You

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

splunk> .conf2017