

Big Data in ICS

SCADA Security Conference

Ladislav Straka | Managing Consultant @ Service & Support spol. s r. o.

5. 11. 2019 | Future Forces Forum, Hotel DAP, Prague

Who we are

and what do we do

► Complex Integration Projects

- Utility, Transportation, Healthcare, Gov

► Main Fields

- Cybersecurity solution (Cybersecurity Act 181/2014, ISO 27000)
- ITOps optimization (ITIL®, ISO 20000)

► 15+ years on the market

► System Integration Awards

itSMF Czech Republic
The IT Service Management Forum

ČIMIB



S&S a Splunk

- ▶ Service & Support **Elite Partner** in CZ/SK
 - Experienced Technical Team
 - Integration Projects (SIEM, ITSI, SecOps)
 - Business Analytics (SLA)
- ▶ Splunk conf 2017, Washington DC (25.-28.9.)
 - 7 000+ Participants, 70+ Partners (2 EE)
 - Easy Ride: How to Collect Tolls While Keeping Drivers Happy
 - <https://conf.splunk.com/sessions/2017-sessions.html#search=Service%20%26%20Support&>



Big Data

Sources



- ▶ IT infrastructure
- ▶ Cybersecurity tech
 - IT
 - non IT
- ▶ Applications
- ▶ Users
- ▶ IoT
- ▶ **ICS**

... every digital record

Volume | Speed | Diversity | Variability

Answers across your organization

Dark Data => Clear Answers

IT Operations

How do I predict service-level degradation before it occurs?

Application Performance Analytics

Is my poor app performance due to code-level errors or infrastructure?

Security and Compliance

How can I speed up security investigations and reduce the impact of insider threats?

Business Analytics

Do my marketing campaigns drive more orders through the website or mobile app?

ICS/IoT

How can I monitor and analyze data from tens of thousands of sensors in real time?

ICS World & Security Myths

ICS Characteristics

Comparing to classic IT

IT Operations

- ▶ Supporting Business Processes
 - Outage has local impact
- ▶ Dynamic, up-to-date
 - Technology lifecycle 3 - 5 yrs
- ▶ Operation/Cybersecurity
 - By Design
- ▶ Assets
 - IP Connected
- ▶ IT Personnel

ICS Operations

- ▶ Controlling Business Processes
 - Outage has large impact
- ▶ Conservative
 - Technology lifecycle 10+ yrs
- ▶ Production
 - Redundancy, Performance (300ms/3s)
- ▶ Assets
 - Blind Spots
- ▶ Staff Trained by Industry



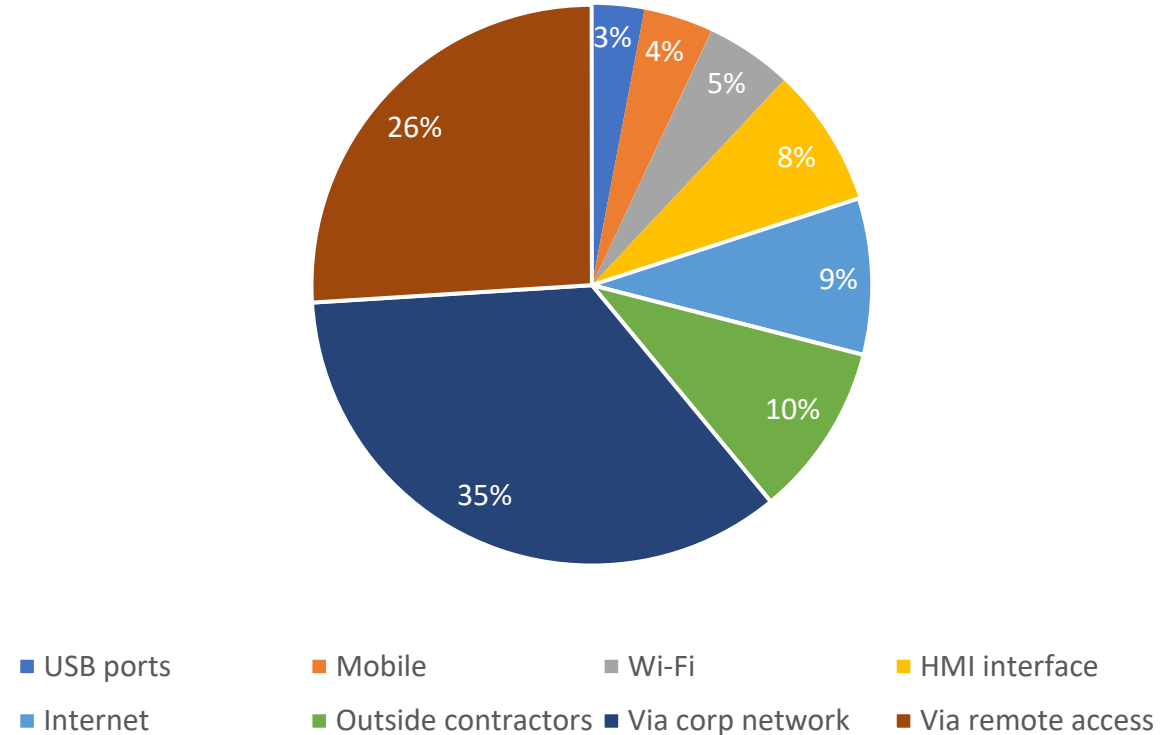
ICS & CyberSecurity

5 Myths

► Myth #1 – We Are „Not Connected“

- Average ICS has 10+ external connections

Malware Sources



130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D5SLAFF10ADFF10 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&JSESSIONID=5D5SL7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=F1-SW-03"
317 27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D5SL8FF3ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=F1-SW-03"
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D5SLAFF10ADFF10 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&JSESSIONID=5D5SL7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=F1-SW-03"
317 27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D5SL8FF3ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=F1-SW-03"
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D5SLAFF10ADFF10 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&JSESSIONID=5D5SL7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=F1-SW-03"
317 27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D5SL8FF3ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=F1-SW-03"

ICS & CyberSecurity

5 Myths

► Myth #2 – We Have NextGen FW

- Almost 80% FW in ICS allowed „any“ services on inbound rules
- Almost 70% machines permitted to manage FW outside of network perimeter

ICS & CyberSecurity

5 Myths

► Myth #3 – Hackers Don't understand ICS/SCADA/PLC

- Cybercrime has become financially very lucrative (just \$80K?)
- Targeted worms and other exploits
- Shodan search engine
- Modules helping in pen testing (Basecamp, Metasploit, ...)

ICS & CyberSecurity

5 Myths

► Myth #4 – We Are Not The Target

- Don't need to be a target to become a victim
 - 80% of ICS security incidents were unintentional

Type	IT	SCADA
Trojan	65%	43%
PUPs	11%	37%
Worm	8%	13%
Virus	16%	6%

ICS & CyberSecurity

5 Myths

- ▶ Myth #5 – Our Safety Systems will prevent any harm
 - Control and safety systems integration using Ethernet/Modbus TCP, OPC
 - SIS communication interface modules run embedded OS and Ethernet stacks



ICS & CyberSecurity

Challenges

- ▶ Asset Management
 - Do I know what I have to protect?
 - Criticality? => Adequate Measures
- ▶ Security Incident Scoring
 - Alerts are good but not enough
- ▶ Root Cause Analysis
 - Essential for Operation/Security Prevention

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=5D15L9FF10ADFF10 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=5D35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=F1-SW-03"
1317 27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&SESSIONID=5D5L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&SESSIONID=5D185L8FF3ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=F1-SW-03"
1317 27.160.0.0 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=5D15L9FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-SW-03"
1317 27.160.0.0 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=F1-SW-03"
1317 27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&SESSIONID=5D5L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&SESSIONID=5D185L8FF3ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=F1-SW-03"
1317 27.160.0.0 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=5D15L9FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-SW-03"
1317 27.160.0.0 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=F1-SW-03"
1317 27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&SESSIONID=5D5L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&SESSIONID=5D185L8FF3ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=F1-SW-03"

ICS & CyberSecurity

Challenges

► IT/OT/Physical Security Gaps

- Holistic Approach to Security Management
- Critical for Effective Forensic

► Personell Education

- 80% of Security Incidents caused by insiders
- Social Profile

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=5D35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268product_id=K9-CW-01"
1317 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=changequantity&itemId=EST-18&product_id=AV-CB-01&SESSIONID=5D18SLBFF3ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-14&product_id=K9-CW-01"
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=5D35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268product_id=K9-CW-01"
1317 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=changequantity&itemId=EST-18&product_id=AV-CB-01&SESSIONID=5D18SLBFF3ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-14&product_id=K9-CW-01"



ICS & Big Data

Potential Role

► High Data Diversity in ICS

- Proprietary devices
- Data Formats
- Protocols

► Data in raw Format

- Operational Stats/Predictions
- Forensic
- Use of ML

► Large Data Volumes

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=5D3SL7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01"
317 27.160.0.0 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=5D1SLAFF10ADFF10 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01"
ows NT 5.1; SV1; - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5D3SL7FF6ADFF0 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01"
itemId=EST-16&product_id=RP-LI-02" 468 125.17 14.189 "GET /category.screen?category_id=GIFTS&SESSIONID=5D1SLAFF10ADFF10 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01"
do?action=purchase&itemId=EST-26&product_id=K9-CW-01" 468 125.17 14.189 "GET /category.screen?category_id=GIFTS&SESSIONID=5D1SLAFF10ADFF10 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01"
http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01" 468 125.17 14.189 "GET /category.screen?category_id=GIFTS&SESSIONID=5D1SLAFF10ADFF10 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01"
http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01" 468 125.17 14.189 "GET /category.screen?category_id=GIFTS&SESSIONID=5D1SLAFF10ADFF10 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01"

ICS & Big Data

ICS/Security Operations Monitoring

► Classic SIEMs

- Problems with proprietary ICS devices
- Architectural Limitations
- Performance Issues

► Big Data Based SIEMs

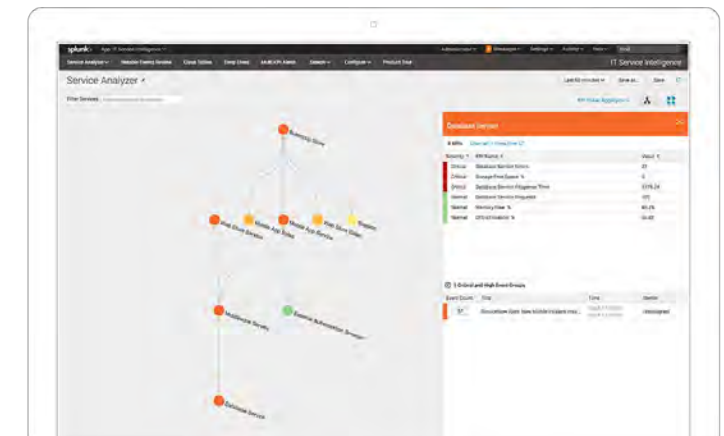
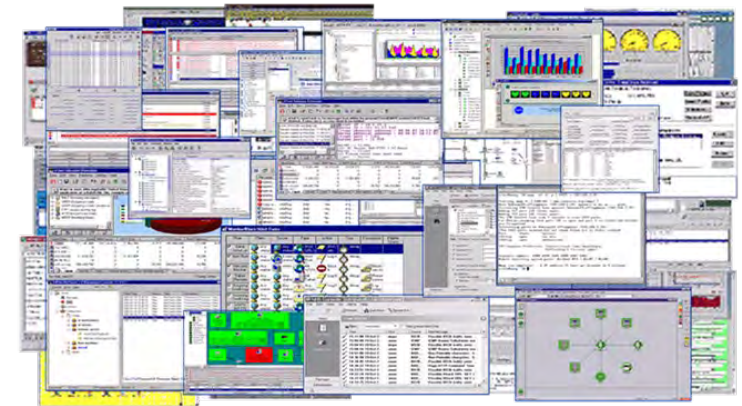
- Predestined for ICS environment
- High Customization
- Flexible Architecture



ICS & Big Data

ICS/IT Operations Monitoring

- ▶ Vendor proprietary systems
 - Domains oriented
 - Indication only (no root cause)
 - No prediction functions
- ▶ Third party solutions
 - Same „features“
- ▶ Big Data based Service Monitoring
 - Visible Assets
 - Fast Impact Analysis
 - Root Cause Analysis
 - What about Good KPI?



SecOps Synergy

```

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GLFISJWJSESSIONID=SD5LSL4FF10ADFF10 HTTP 1.1" 404 720 "http://buttermcup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=PI-SW-01"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?category_id=GLFISJWJSESSIONID=SD5LSL4FF10ADFF10 HTTP 1.1" 404 332 "http://buttermcup-shopping.com/category.screen?category_id=PI-SW-01"
" 317 27.160.0.0 - - [07/Jan 18:10:56:156] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=SD5LSL4FF10ADFF10 HTTP 1.1" 200 1318 "http://buttermcup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=PI-SW-01"
ows NT 5.1; SV1; - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=SURPRIS&SESSIONID=SD5LSL4FF10ADFF10 HTTP 1.1" 200 1318 "http://buttermcup-shopping.com/category.screen?category_id=PI-SW-01"
:/buttermcup-product_id=RP-LI-02" 468 125 17 10 "GET /category.screen?category_id=FLOWERS&SESSIONID=SD5LSL4FF10ADFF10 HTTP 1.1" 200 1318 "http://buttermcup-shopping.com/cart.do?action=purchase&itemId=EST-6&product_id=PI-SW-01"
toaction=purchase_id=RP-LI-02" 468 125 17 10 "GET /category.screen?category_id=FLOWERS&SESSIONID=SD5LSL4FF10ADFF10 HTTP 1.1" 200 1318 "http://buttermcup-shopping.com/category.screen?category_id=PI-SW-01"
opping.com/case&id=RP-LI-02" 468 125 17 10 "GET /category.screen?category_id=FLOWERS&SESSIONID=SD5LSL4FF10ADFF10 HTTP 1.1" 200 1318 "http://buttermcup-shopping.com/category.screen?category_id=PI-SW-01"

```

Key Takeaways

1. ICS Infrastructure is no longer isolated
2. Efficient Sec & Ops Control over ICS Assets is crucial
3. Time to Change Approach

**SecOps Concept
Becomes Imperative**

Thank you

Ladislav Straka, straka@sands.cz