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

Service & Support

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

Service & Support

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

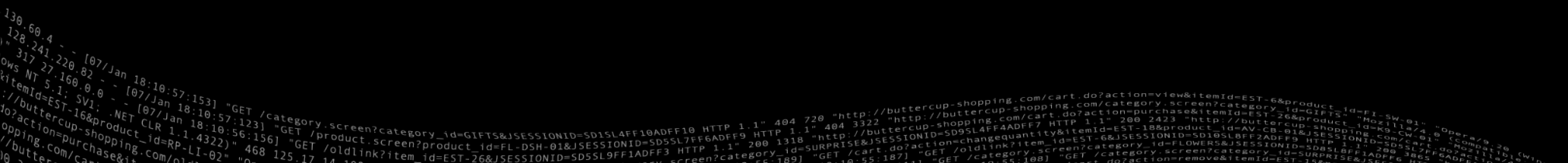
How can I speed up security investigations and reduce the impact of insider threats?

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?



Service & Support

ICS World & Security Myths

Service & Support

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

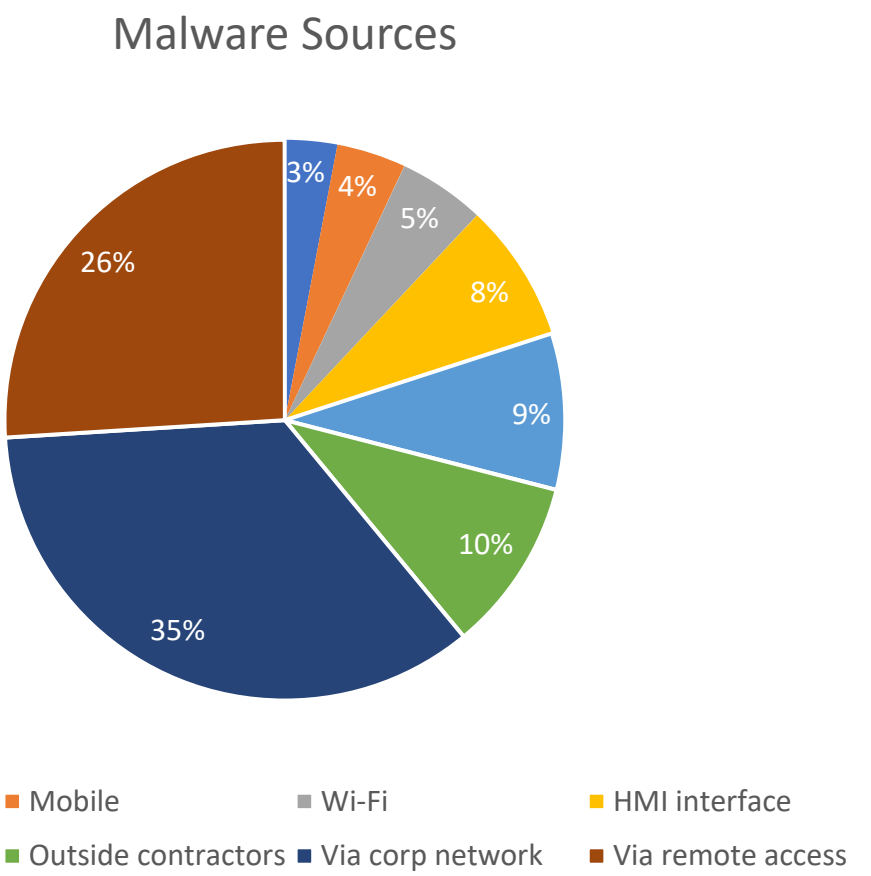
- Controlling Business Processes
  - Outage has large impact
- Conservative
  - Technology lifecycle 10+ yrs
- Production
  - Redundancy, Performance (300ms/3s)
- Assets
  - Blind Spots
- Stafff Trained by Industry

Service &Support

ICS & CyberSecurity

5 Myths

- Myth #1 – We Are „Not Connected“
  - Average ICS has 10+ external connections



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

Service & Support

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, …)

Service &Support

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%

Service & Support

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

Service & Support

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

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

Service & Support

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

Service & Support

ICS & Big Data

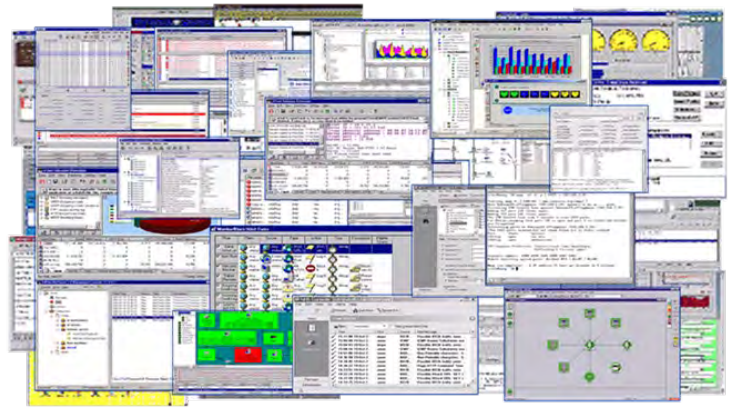
ICS/Security Operations Monitoring

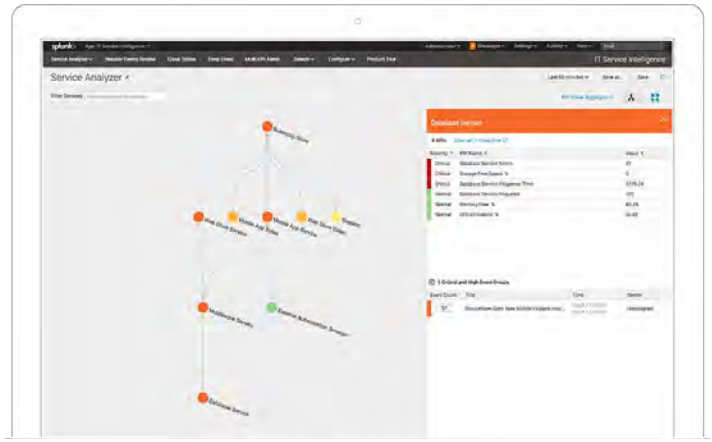
- Classic SIEMs
  - Problems with proprietary ICS devices
  - Architectural Limitations
  - Performance Issues
- Big Data Based SIEMs
  - Predestined for ICS environment
  - High Customization
  - Flexible Architecture

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?



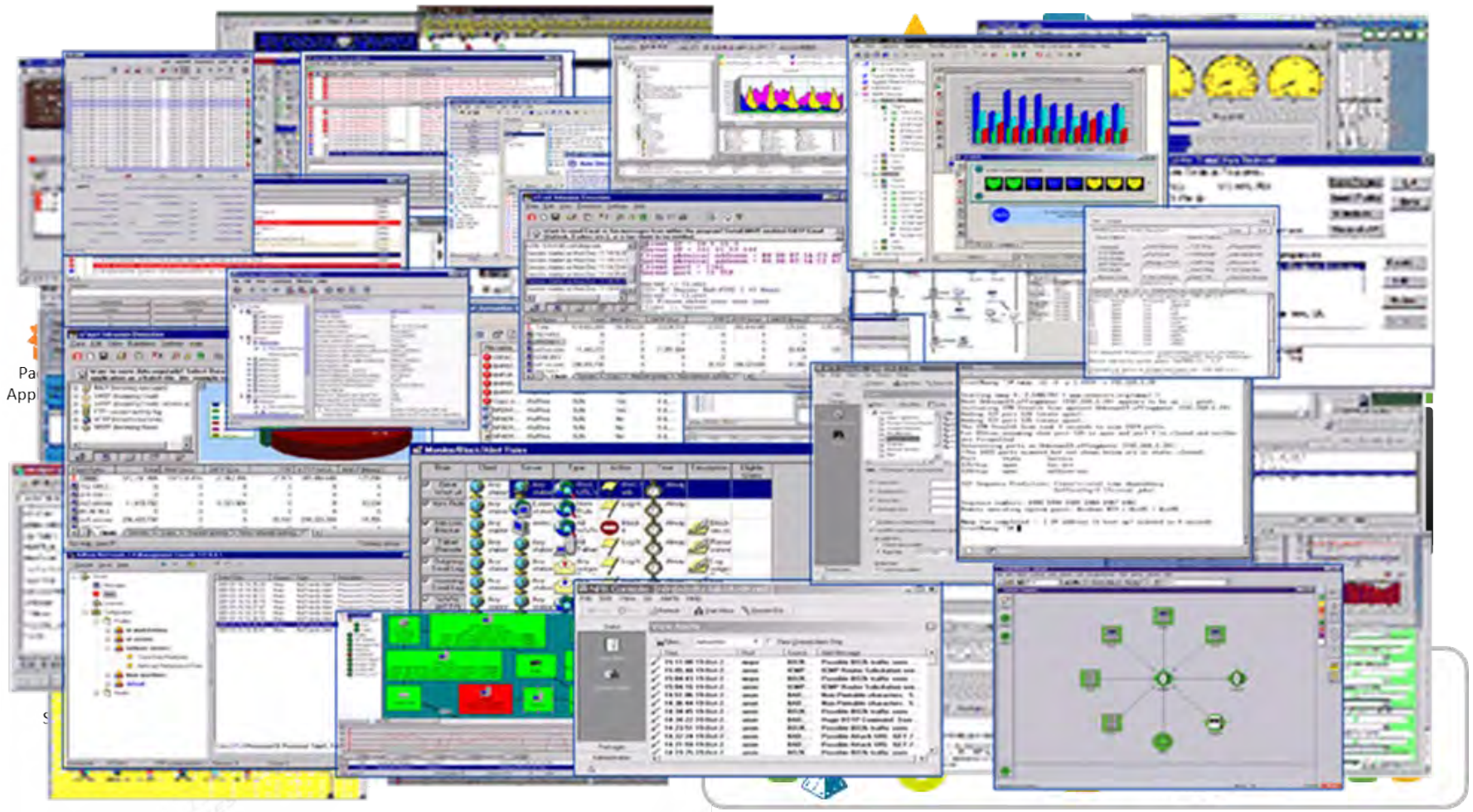


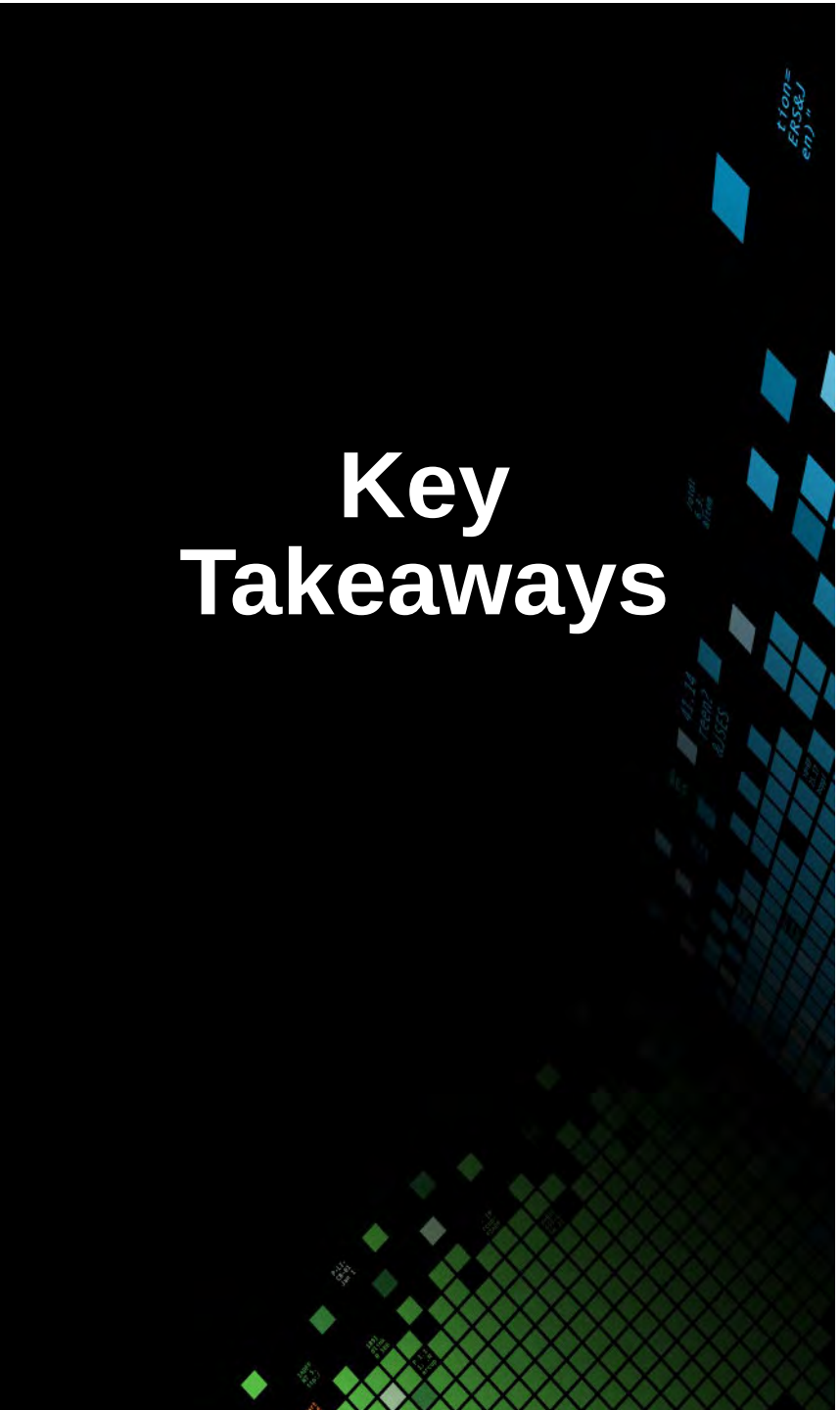
SecOps Synergy

Service & Support

SecOps

Security & Operation Center for ICS





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

Service & Support

Thank you

Ladislav Straka, straka@sands.cz