أرامكو السعودية
saudi aramco

How Operation Technology (OT) Monitoring fits well with Machine Learning Toolkit (MLTK)

Saleh Ghamdi, IT Security Manager, Saudi Aramco

Anas Faruqui, IT Security Analyst, Saudi Aramco

October 2018

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> .conf18

Introductions

So, who are we, and what we do?

Saleh Al-Ghamdi

- Worked in IT for over 20 years
- Worked in IT Security for last 15 years
- Seasoned Manager for IT Security
- Lead Manager “go to person” for Splunk and SIEM.
- Contributed to Internal Security Logging Standards

Anas Faruqui

- Worked with Splunk for over 10 years
- ICS/IOT Cyber Security Specialist
- Experience with “Data Diodes” and worked to improve concept of zones/conduits for Architecture Design in various vendors
- Experience in America, Middle East and Asia
- During my “free” time busy with running an non-for-profit in Chicago

where energy is opportunity

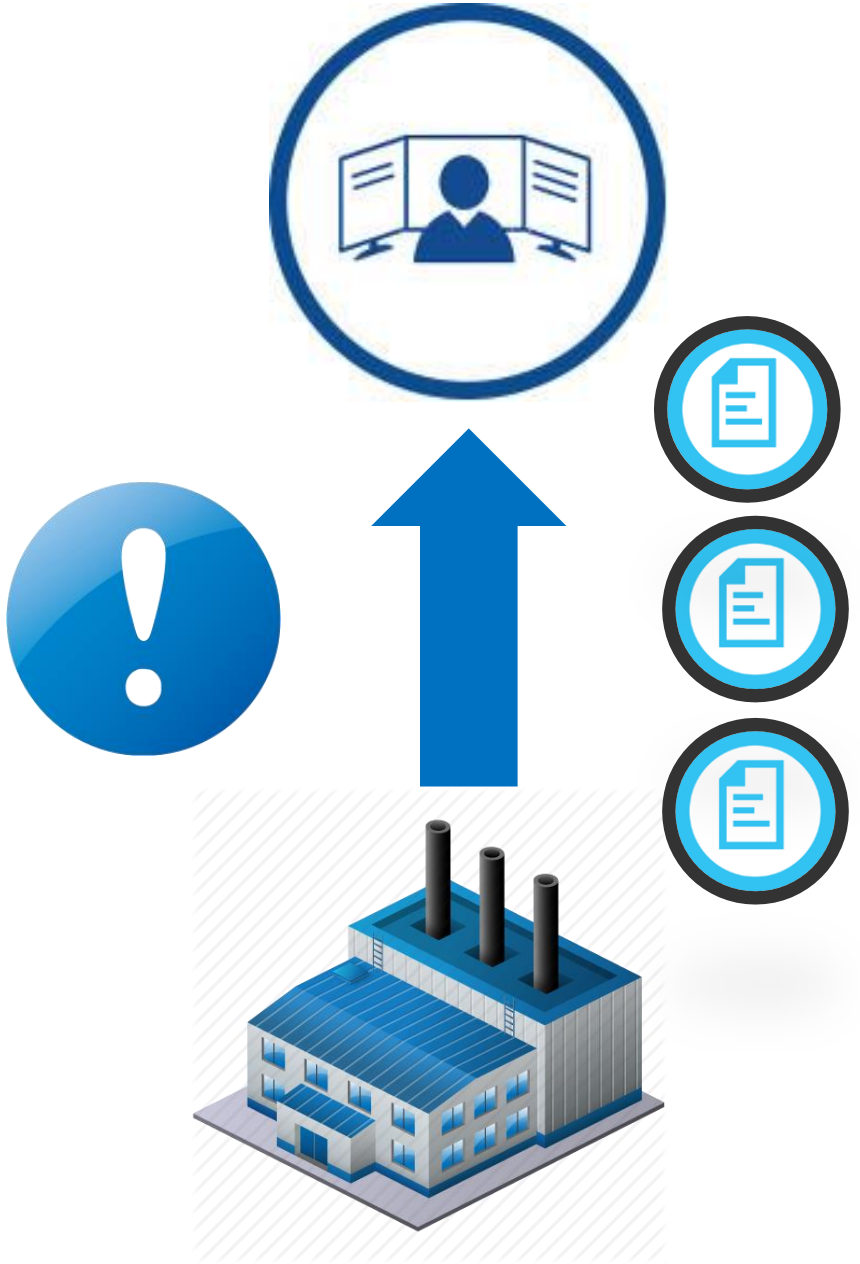
Energizing people and ideas to create even more opportunity from our resources

Agenda

- Why monitor OT?
- Approach
- Best Practices
- Why MLKT?
- Use Cases
- Road ahead & Challenges
- Takeaways
- Q&A

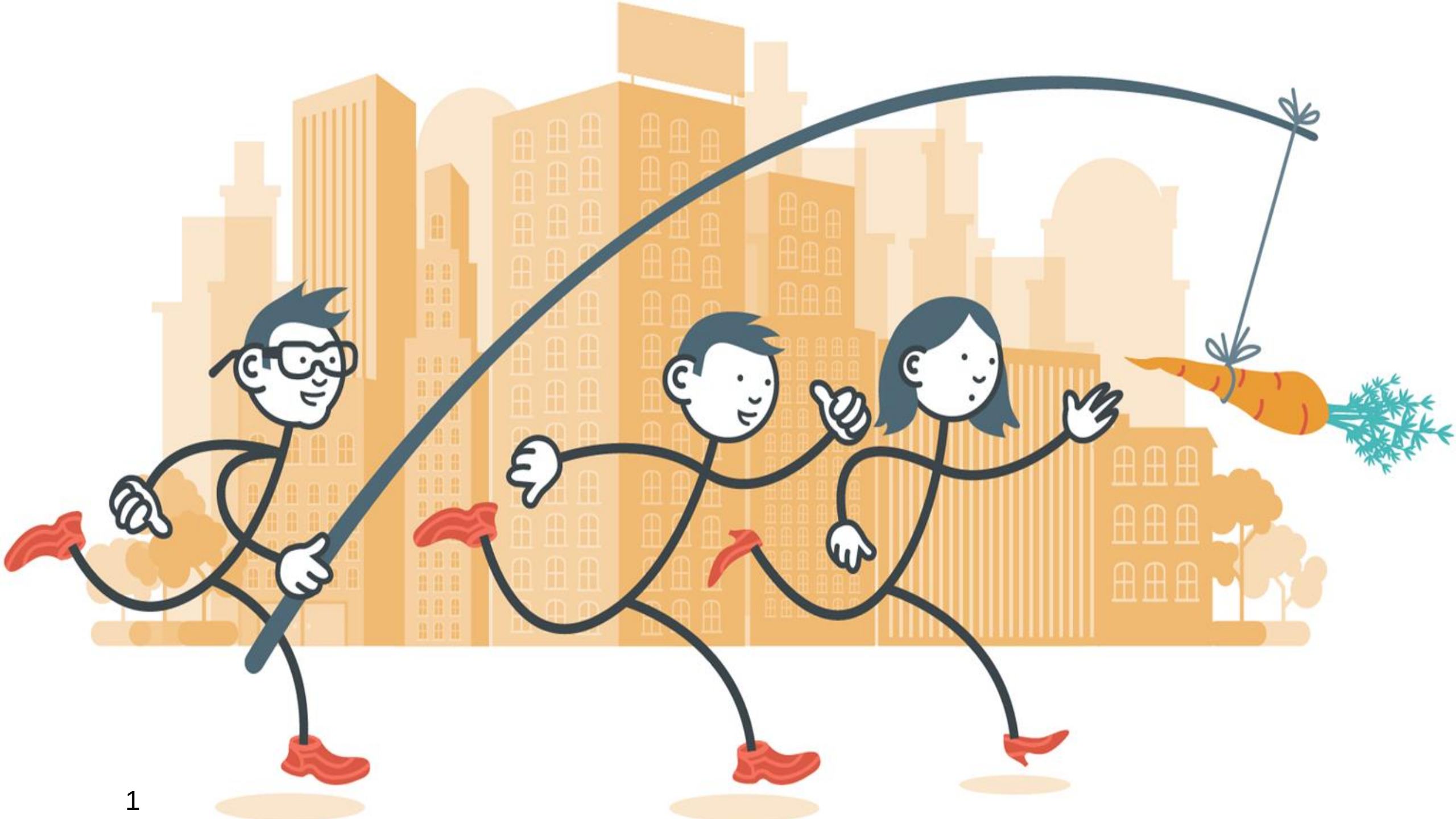
Why monitor OT?

- Threats are growing
- Enhance security
- Visibility
  - Internal Malfunction
  - Insider threats and Vendor misuse
- Compliance
- Availability



Approach

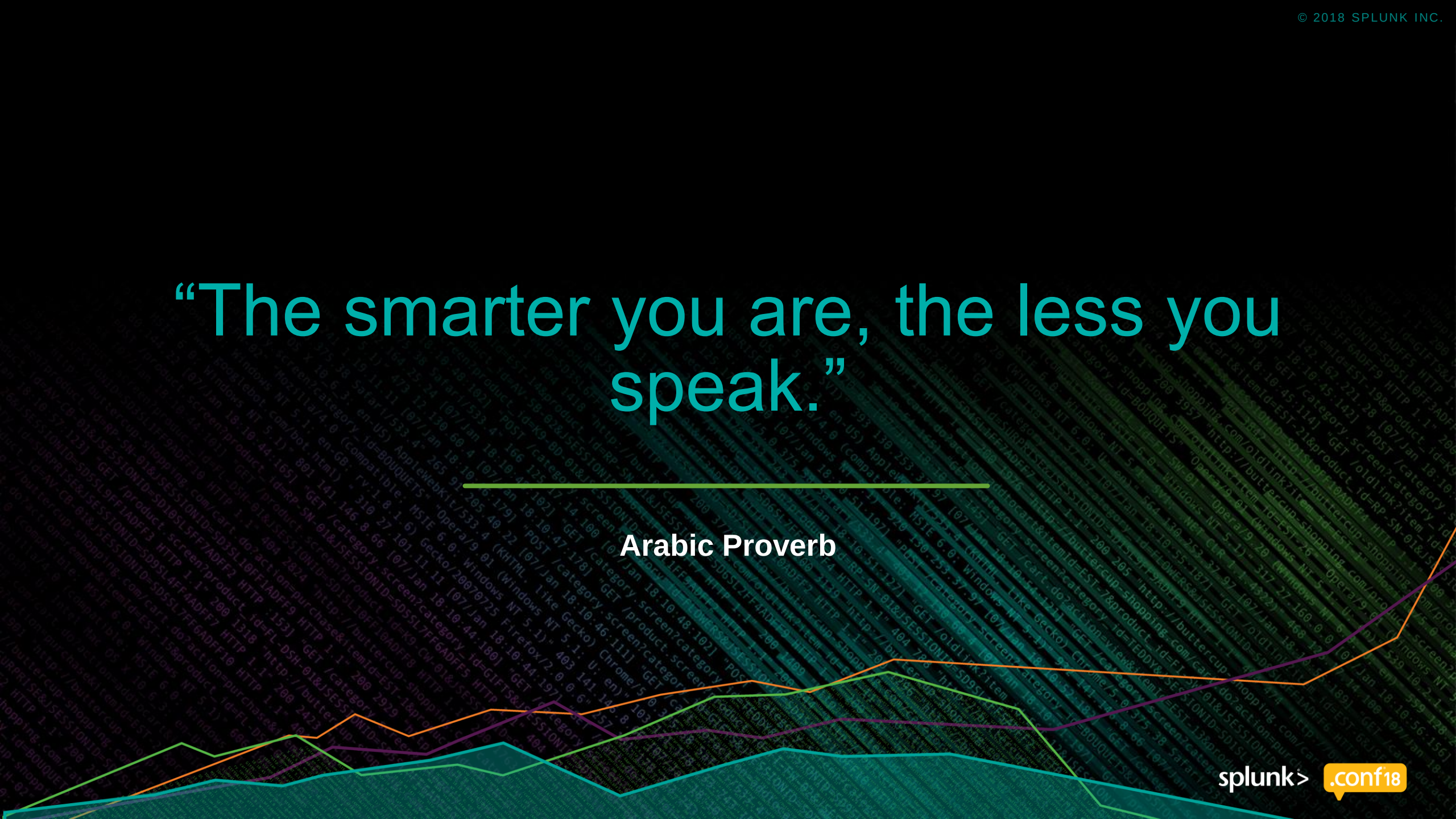
What made us go forward with monitoring OT?




splunk>
I like BIG data
& I cannot LIE
CALENDAR

“The smarter you are, the less you speak.”

Arabic Proverb



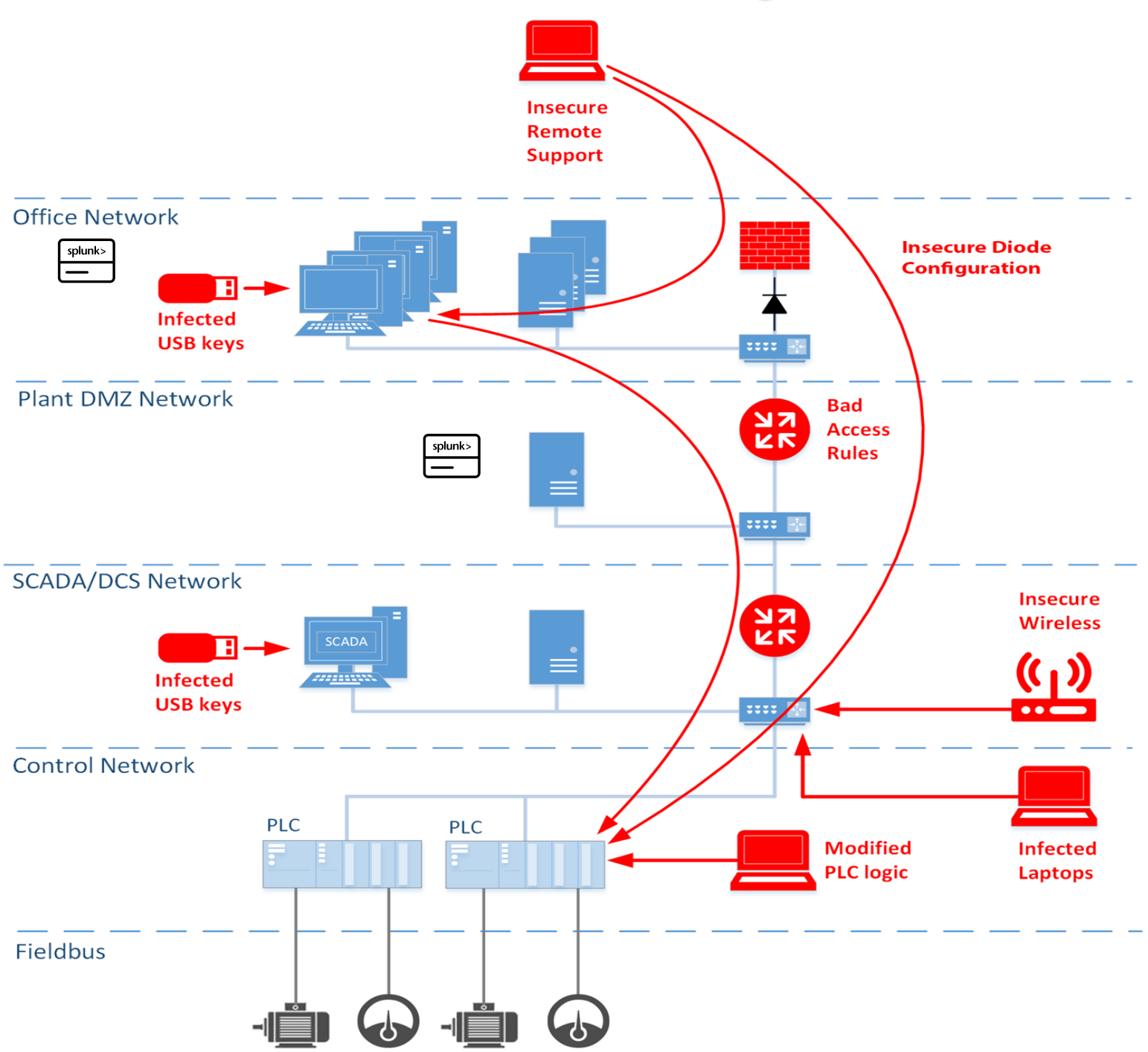
Implementing Splunk with MLTK in mind - Best Practice

- Worry about your model
- Assemble the right data
- Try automate identifying logs
- Separate each log source by vendor type and product name
- Tagging the data by unique customers
- Ingest data from L1/L2/L3 to L4
- Test before launching enterprise-wide solution

Why MLTK?

How does MLTK help OT?

- IT Systems within OT:
  - Easy but … so many legacy
  - “Too much data”
  - Eat everything, … filter later …
- ICS Applications Logs
  - Complex
  - Is it possible?
- Large Datasets = Rare updates = MLKT



Typical Architecture of ICS Network

Use Cases

Compliance

Security

Availability

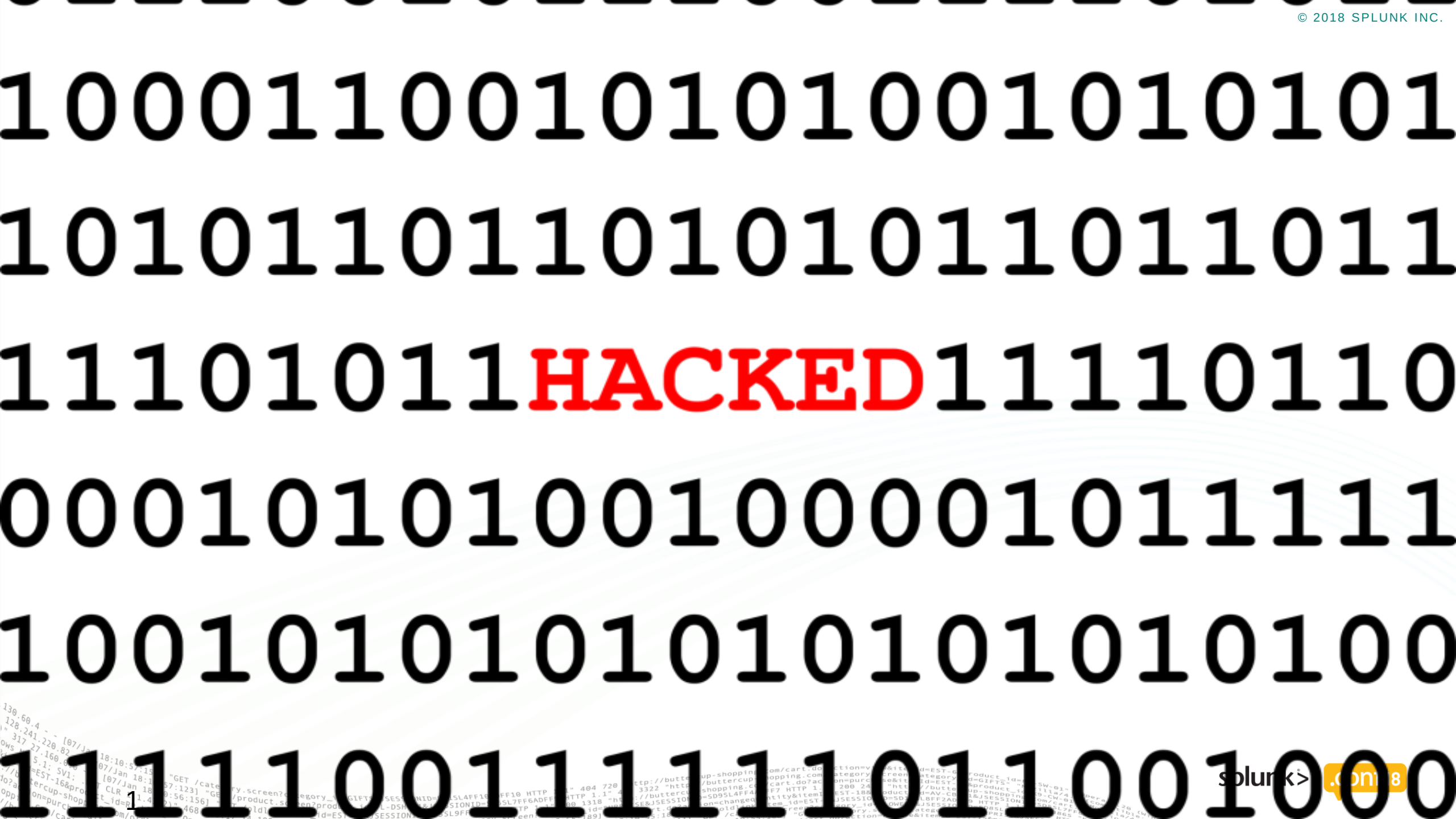

COMPLIANCE
TRANSPARENCY
RULES
LAW
POLICIES
REGULATIONS
STANDARDS
REQUIREMENTS

Compliance

- Are logs even generated?
- Manually process of validation
- Spot Checking

- Use tools to validate logs generation
- Input compliance tools data in Splunk to see logs are coming
- Verify using outlier method between groups of “customers” and types of logs

Are logs coming?

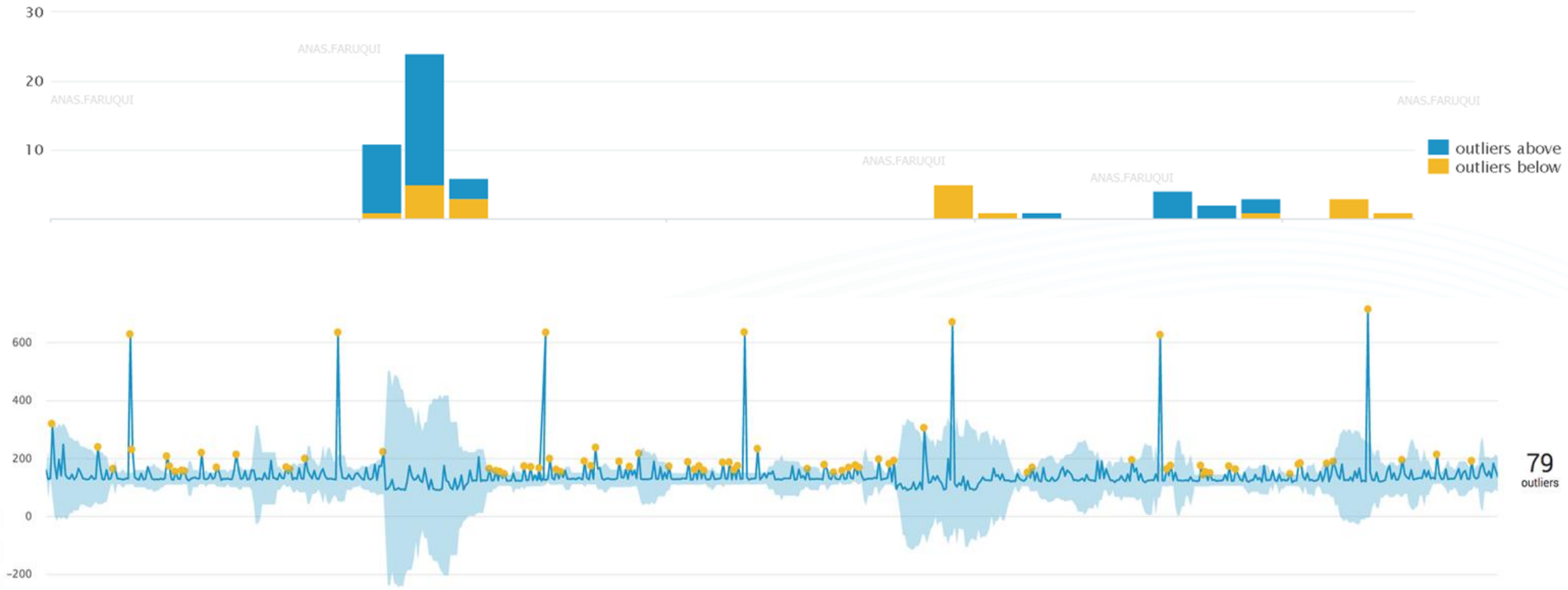


Security

- Too large datasets
- Baseline individual customer is not giving you anything meaningful

- Uncommon patterns, like new malware, brute force login attempts
- Credential behavior and how it works again
- Correlate, Correlate, Correlate datasets from various “customers”

Login failure attempts & Firewall denies




OPEN
24 Hrs

Availability

- Why Failure Occurred
- Manual Spot Checking of Failures
- Holistic view of all logs
- Common Components are health, temperature, disk, memory, etc

Device(s) Temperature

1,239

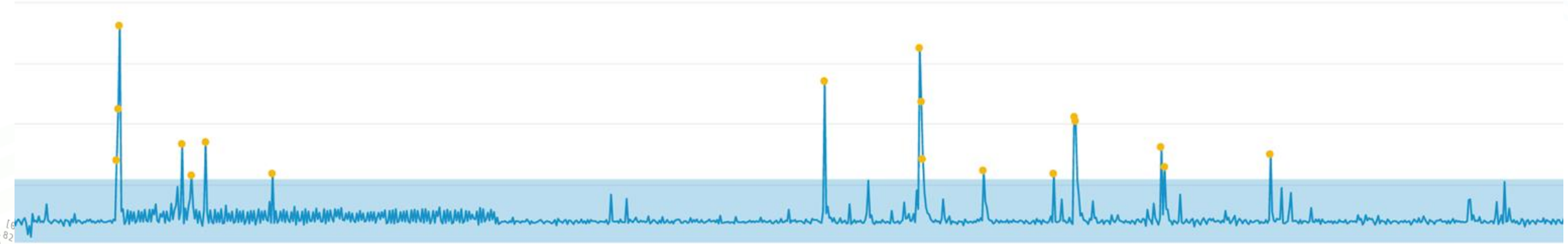
Outlier(s)

Open in Search | Show SPL | Schedule Alert

2,889

Total Event(s)

Open in Search | Show SPL



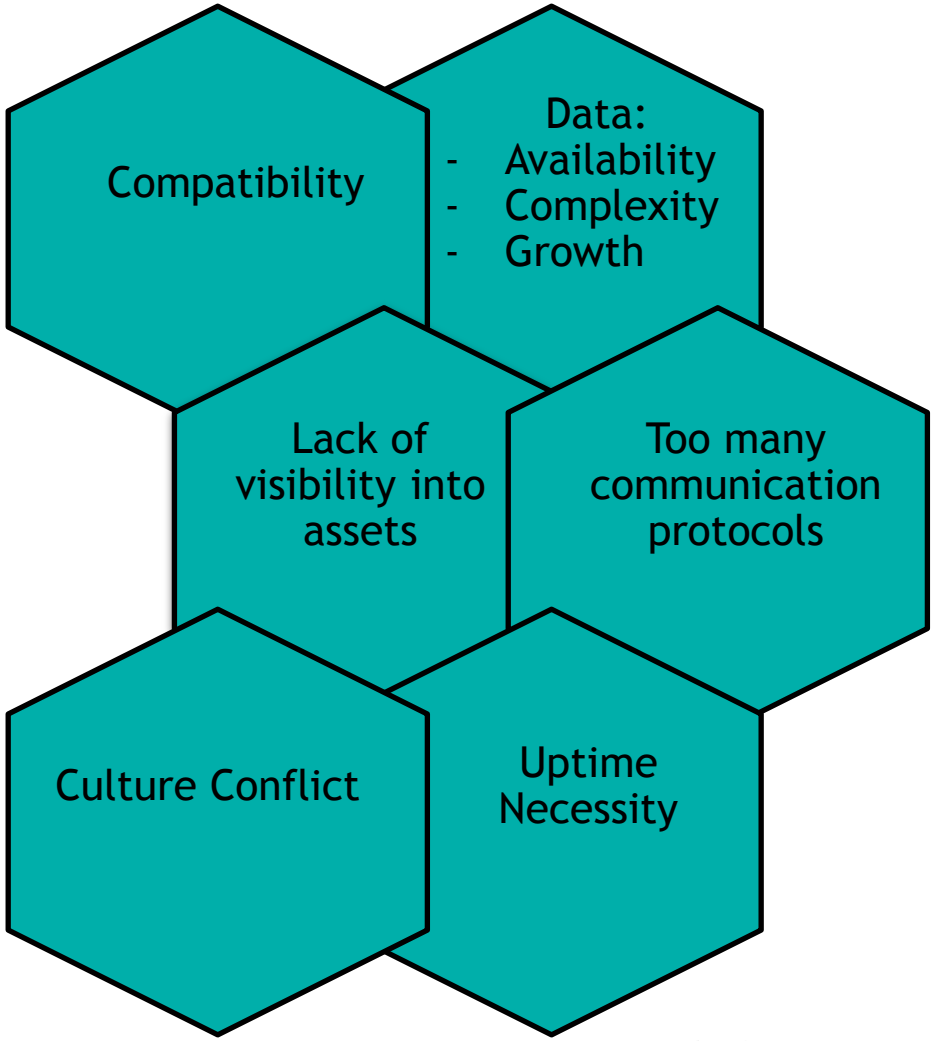
“The ROAD to success is D.O.T.T.E.D. with many tempting parking spaces.”

Crush it Media

splunk> .conf18

OT Monitoring Top Challenges

the growing concerns in OT monitoring



Key Takeaways
& Future

1. Security Monitoring cannot work without Operational & Performance monitoring
2. MLTK Optimization is required constantly
3. Leverage other tools to augment OT monitoring
4. Culture conflict resolution

Q&A

Saleh Al-Ghamdi | IT Security Manager, Saudi Aramco

Anas Faruqui | IT Security Analyst, Saudi Aramco

splunk> .conf18

References

- Slide 4 - https://www.ndtv.com
- Slide 5 - https://www.inc.com
- Slide 8, 9, 10 - https://www.engageandprosper.com/
- Slide 11 - directapproachdesign.co.uk
- Slide 13 - ics-cert.kaspersky.com
- Slide 15 - www.iconfinder.com
- Slide 16 - trustweaver.com
- Slide 19 - globalcyberlawyer.com
- Slide 22 - www.mediaconnectpartners.com
- Slide 25 - commons.wikimedia.org

Thank You

Don't forget to rate this session in the .conf18 mobile app