



Combating Cyber Threats against Airborne Assets

Paul Vout
Solutions Architect
paul.vout@elastic.co

DISTRIBUTION STATEMENT A: Approved for public release. Distribution is unlimited.





Paul Vout, CISSP
Solutions Architect at Elastic
paul.vout@elastic.co

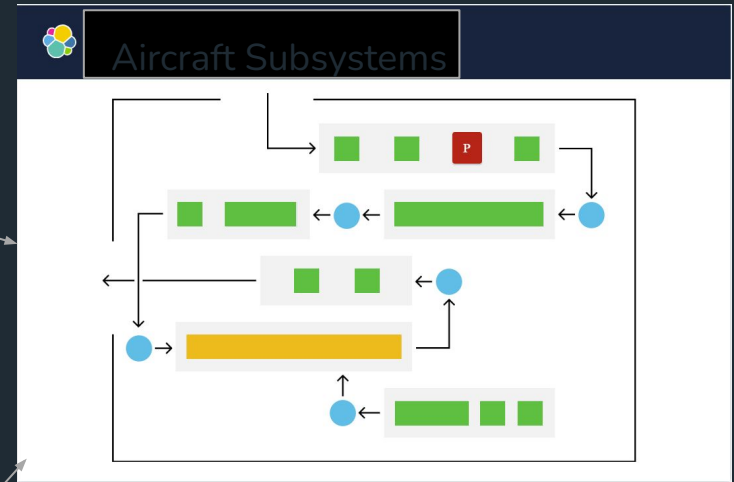
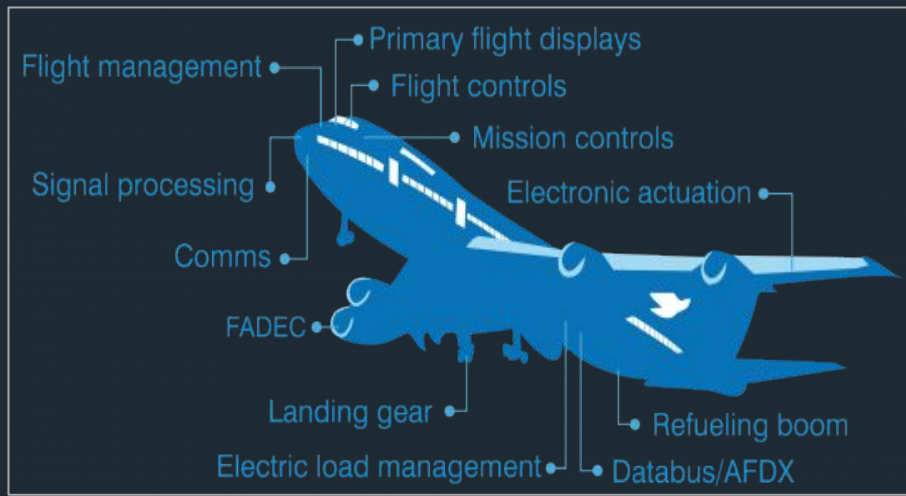
- **Solutions Engineer/Architect/Gopher for 25+ years**
- **Currently support mostly US Air Force & DoD customers**
- **Previously at Endgame / ArcSight / Integrio**
- **Ran a team of Cyber Analysts/Engineers for seven long years :-)**
- **Majored in Computer Science and Business at Old Dominion University**
- **Commercial Pilot flying for the VA / Red Cross / Airborne Express**
- **Subject Matter Expert for ISC(2) and CompTIA**

Airborne Assets

- **Fixed-wing: Fighter/Bomber/Transport/Other**
- **Rotor-wing**
- **Unmanned Aerial Vehicle (UAV)**
- **Unmanned Aircraft Systems**
- **Satellites**
- **Space vehicles**
- **CVA/H in KC-46 / B-52**

Threat Vectors

- **Supply Chain: Blueprint compromise, malicious chips,**
- **1553 protocol impersonation / modification**
- **Maintenance - MRO - Major / minor - STARTEX**
- **GPS jamming: resulting in positional offset /confusion**
- **Ground station timing variance - subtle**
- **Post-flight data analysis & exploitation**
- **Single or weak crypto**
- **Air Traffic Control / Air Traffic Management**
- **PAX records**
- **Malicious Insider - Probably least likely but most disruptive**
- **Machine Learning: DCO & OCO -**



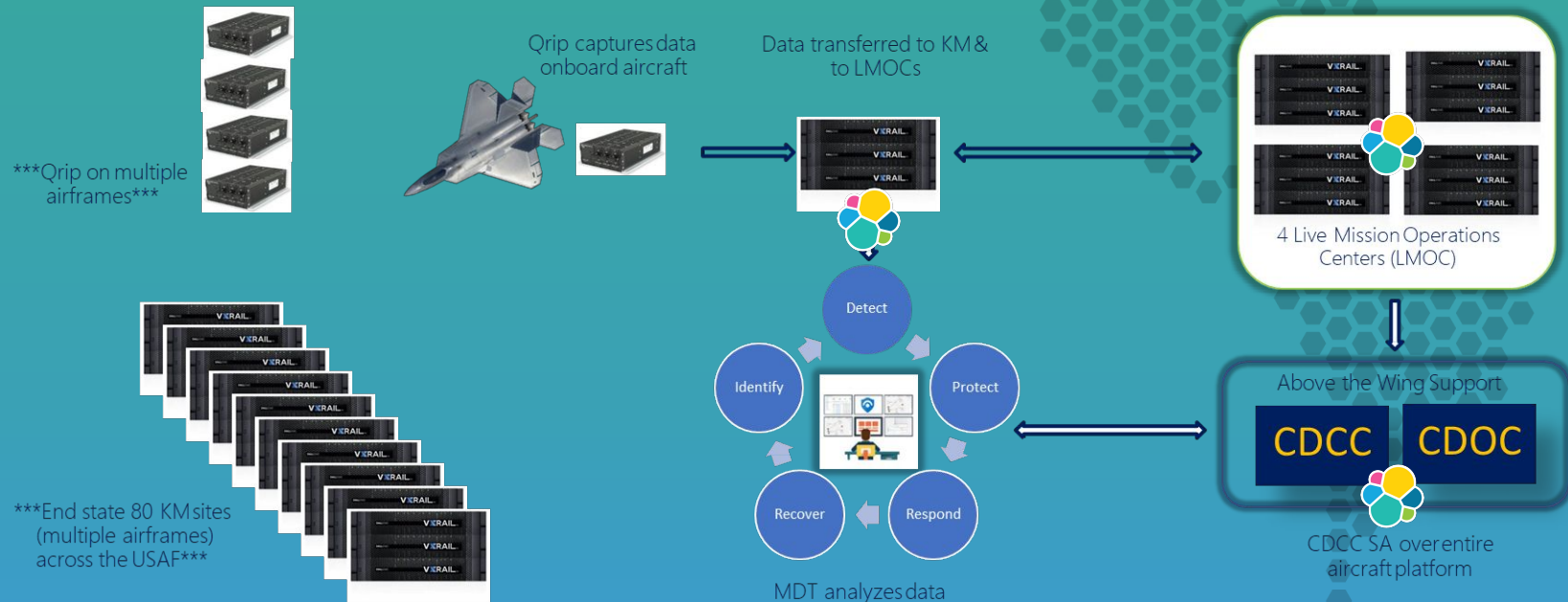
Data types to monitor:

- MIL-STD-1553 A/B
- ARINC-429 / 661
- IP-based systems
- other...



1553 Details

Elastic Integration Architecture



Elastic Aircraft Data Bus Integration

Current Elastic Aircraft Data Bus Integration Protocols:

- 1st – 3rd Gen Airframe and Unmanned Platforms – ARINC 429
- 4th Gen Airframe – MIL-STD-1553
- 5th Gen Airframe – MIL-STD-1553, IEEE 1394b, Fiber Channel
- 6th Gen Airframe – MIL-STD-1760

Outcomes

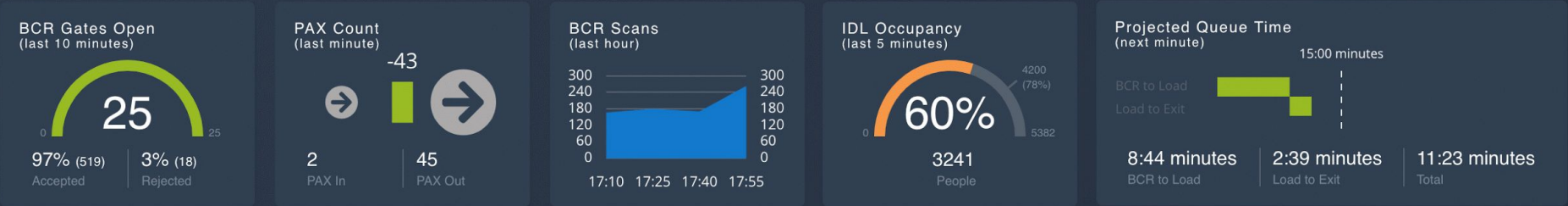
- Phase 1 - Detect Anomalies with Elastic ML
- Phase 2 - Commander Battle Map Integration
- Phase 3 - Real-Time Monitoring in Flight



IDENTIFY • PROTECT • DETECT • RESPOND • RECOVER

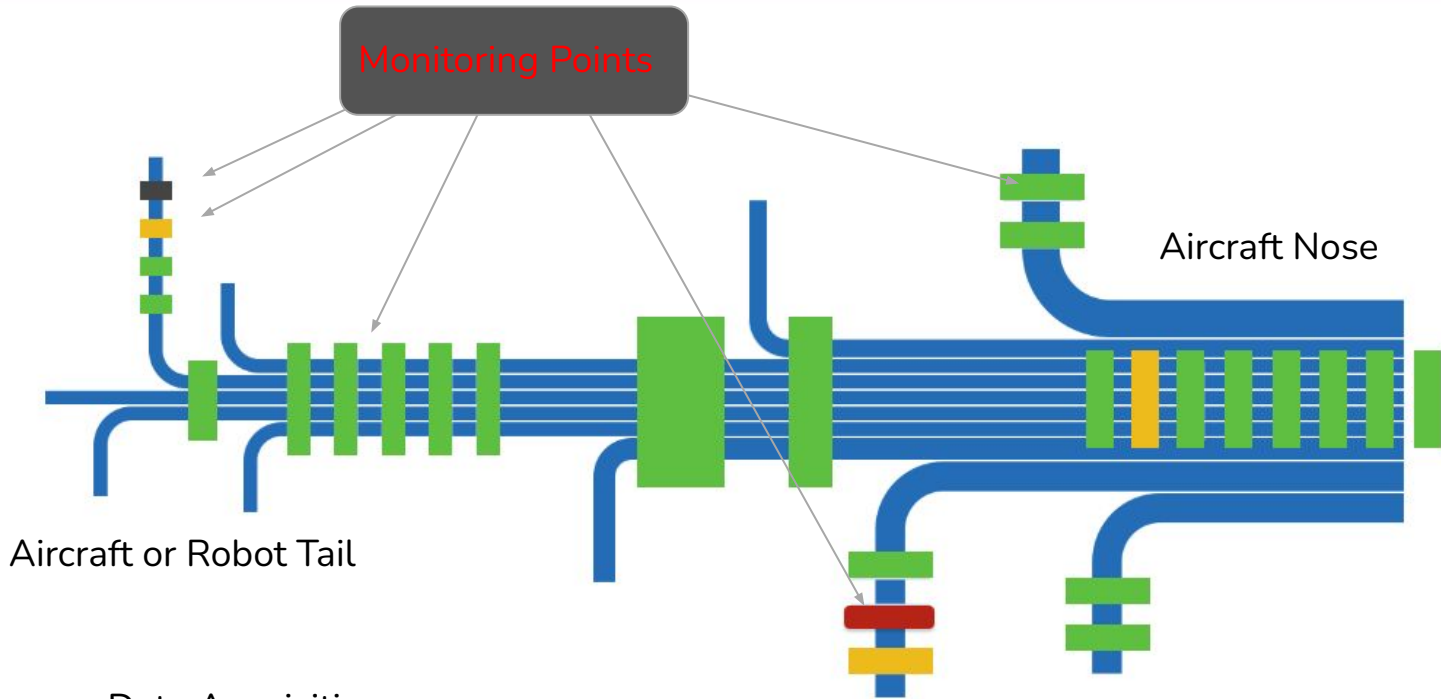


Aircraft Bus Systems





Aircraft Components / Busses



Data Acquisition:
1553, 1394, TSPI, IP, GPS, RF



Pump 1

Elastic IoT Dashboard

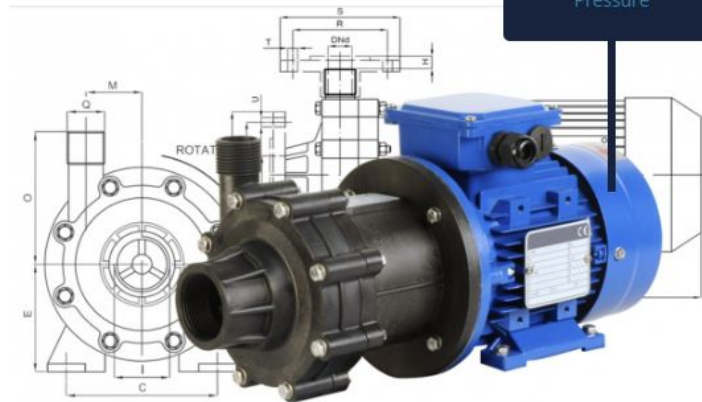
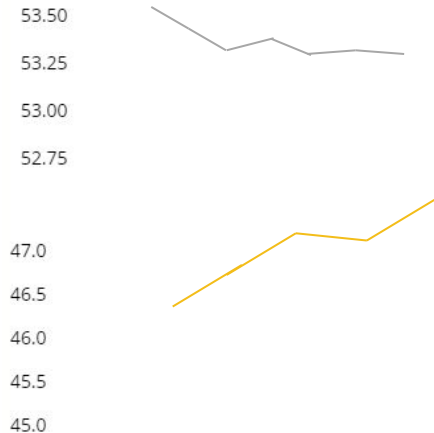


Error detected!

Recommended action: Start cleaning process



- Monitoring Point
- Hydraulic / Oxygen / Fire Suppression
- Near Real-time Monitoring
- Impact Level & other systems affected
- Trend and predictive analysis (e.g. **MTBF**)



979.01
Pressure

65.63 °C



53

RPM



38

Suction



2

Errors



15

Liters per Second

GOTS specific assistance from Elastic ESRE

The Hidden Troubles of the F-35

When the F-35 blows a tire, it can set off a chain reaction of potential failures

By Valerie Insinna

Jun 12, 2019



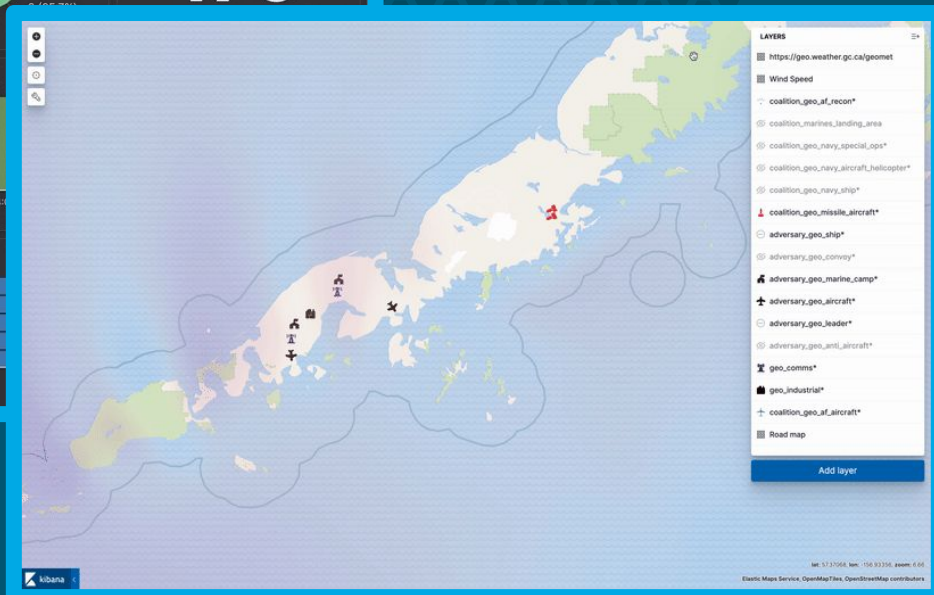
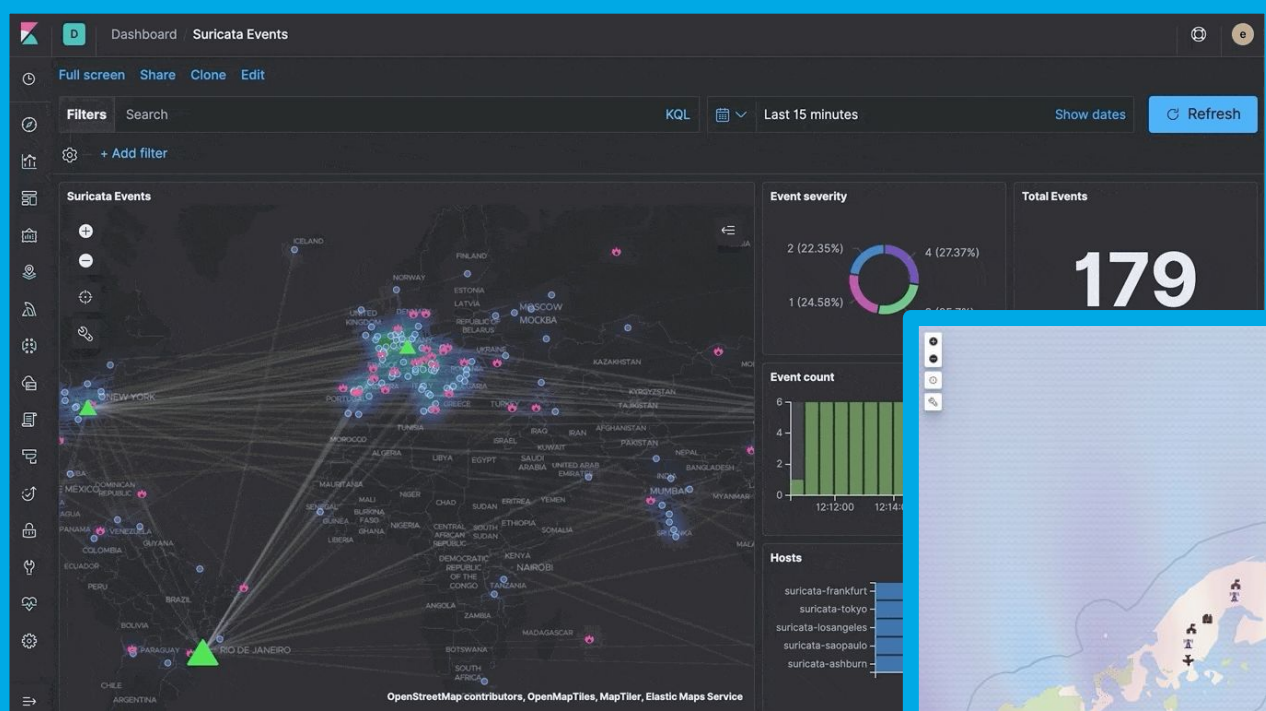
My F35 tire blew out but it seems like other issues occurred as well. What happened

....

Hydraulic Brake Systems also malfunction on version "A" and "B" of the F35. Any F-35C carrier version requires a bug fix for this issue to be resolved. These 4 F-35C aircraft have had such bug fixed

...

Actionable Intel = Your Global Data Mesh Visualized in GEO



Data acquisition demo -10 mins max



Thank You

www.elastic.co/federal
paul.vout@elastic.co

