Military Equipment: Protection, Behavior Analysis and Fleet Management

Melissa Nealon, A&D Specialist | mnealon@splunk.com

Mike Bradbeer, Sales Engineer, UK Public Sector | mbradbeer@splunk.com

Oct 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

Most important part!

Who are we?

Meet your speakers

Melissa Nealon

- Splunk since Feb 2013
- Is slightly obsessive about airplanes (or aeroplanes if Mike says it)
- Is American but living in Britain so spends most of my time cold
- Still says tomAto and not tomAto

Meet your speakers

Mike Bradbeer

- Splunk since May 2017
- In Splunk years, he's a baby – however his hair colo(u)r and wrinkles give him away
- Is British. Nuff said ….
- Is married to an American and he hates Tomatoes.

Industry challenges

Industry challenges

BRIEFING • DHS

Hacks on a Plane: Researchers Warn It's Only 'a Matter of Time' Before Aircraft Get Cyber Attacked

Honeytrap spy stole secrets of new RAF jet: Female agent hacked airwoman's Tinder profile to target stealth fighter crews involved in the £9bn F-35 project

- A female RAF airwoman has had her Tinder profile hacked by a secret agent
- The spy used the profile to target RAF aircrew involved in the F-35 fighter project
- The plot was foiled after the RAF woman reported her Tinder was compromised
- RAF chiefs have sent a warning to personnel about 'online social engineering'

CYBER TERROR? MH370 was the first 'remote hijacking' and carried out to stop jet delivering secret cargo to China, author claims

...chnology designed to stop a repeat of the ...llowing hijacked planes to be remotely ...have been exploited by cyber-spooks

...d: 12th December 2017, 5:11 pm

Harold C. Hutchison
Jun. 09, 2017 08:18AM EST

Articles →

These soldiers defeated a column of tanks by hacking them

A tank unit deployed to the National Training Center at Fort Irwin, California, for a training exercise had a big surprise when they were ordered to carry out an assault. Their movement was halted not by artillery and missiles, but by ones and zeros.

According to a report by DefenseSystems.com, the assault was thwarted by cyber weapons. While the exact nature of the hacking wasn't disclosed, the report did state that it targeted the radios and wireless communication systems on the tanks.

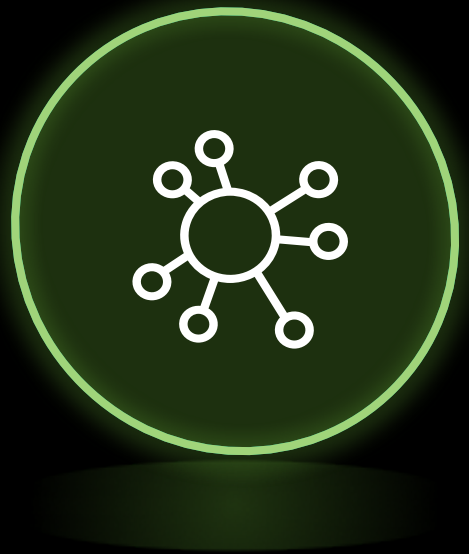
splunk> .conf18

Security: A compounding challenge

splunk> .conf18

Security Challenges are Compounding

EVOLVING THREATS



$3 Trillion

Expected global cost of cybercrime by 2021

LACK OF VISIBILITY

70+

Apps to manage

SKILL SHORTAGE

3.5 Million

Unfilled cybersecurity jobs by 2021
75% YOY increases

Go Beyond the Known

ACTIONS & AUTOMATION

KNOWN

Driven by rules and correlation

Alerts

COMMAND CENTER

ANALYZE
INVESTIGATE
REMEDIATE

Insights

UNKNOWN

Driven by machine learning

splunk> .conf18

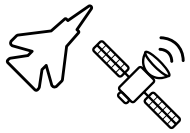
Data Sources and IoT

Data Sources for Mission Operations

Mission Control

Soldier Experience

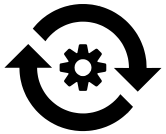
Behavioral Analytics



Mission Operations

Operations

Monitoring, Diagnostics



Asset Performance Management

Security, Safety and Compliance

Preventative Maintenance

Transactional Data

Mission & Operations Intelligence

Digital Intelligence

IT Data

Security Data

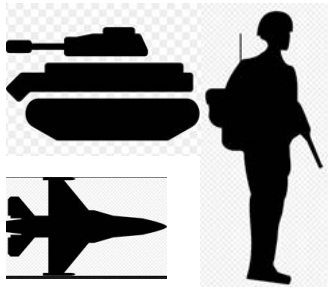
Asset Intelligence

IoT Data

Hybrid is a Critical Capability for Asset Intelligence

Fixed Assets (Industrial)

Mobile Assets (Transport)



Human and Environment

COMMAND CENTER **COMMUNICATIONS** **MILITARY PLATFORM**

End to End Visibility

Cyber Resilience

Health & Preventative Maintenance

Fleet Management

splunk> .conf18

A complex ecosystem to protect

But there is more than just the remote asset to think about

Central Command Center Building

Physical Access
Software Access

Communications

GPS
RF
C/X/Ku/Ka Band

Remote IOT Asset

Relies on external APIs for instruction

Data-Driven Battlefield

Accelerating mission operational efficiencies

Connected vehicles (manned/unmanned)

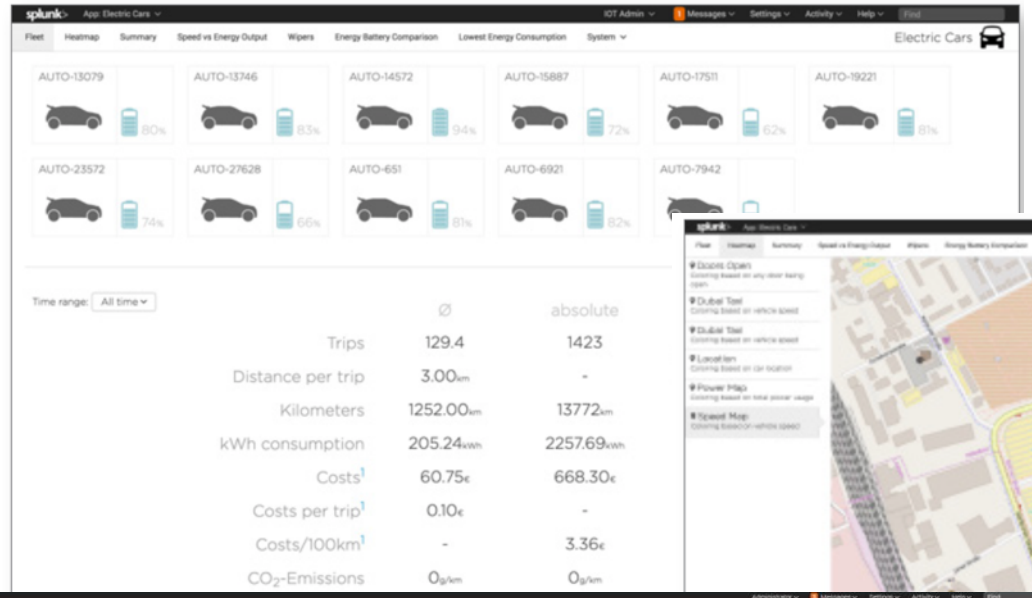
Flying data center / unmanned drones

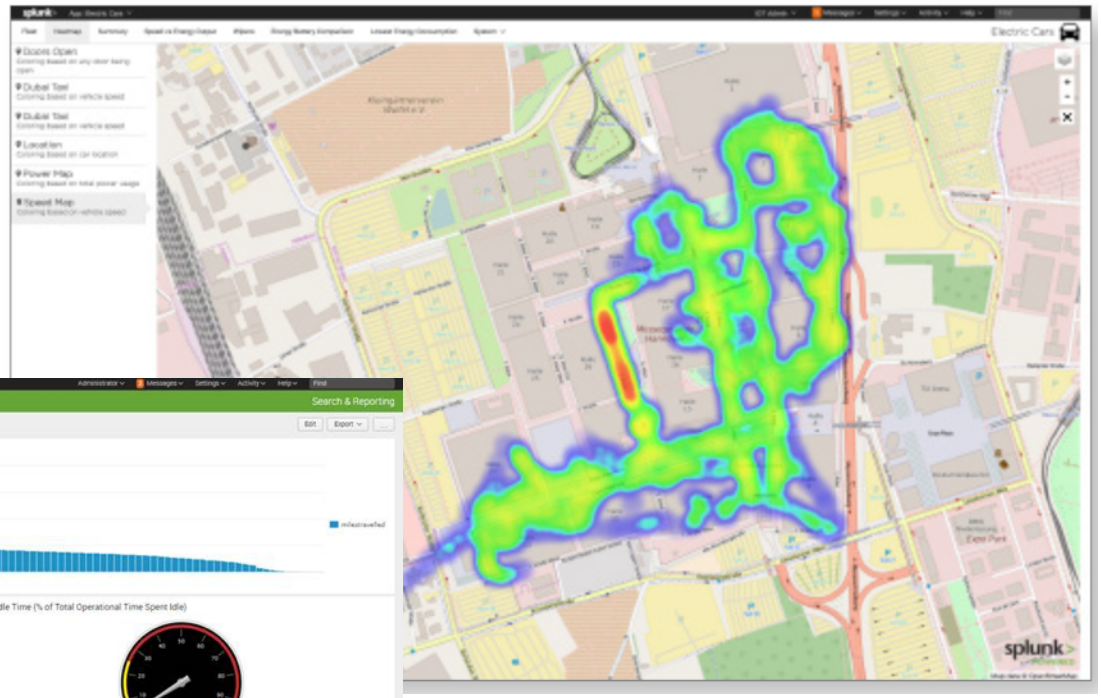
Smart soldier - vital health, location and performance

Satellite and network communications

Connected Vehicles

Metrics gathered and correlated

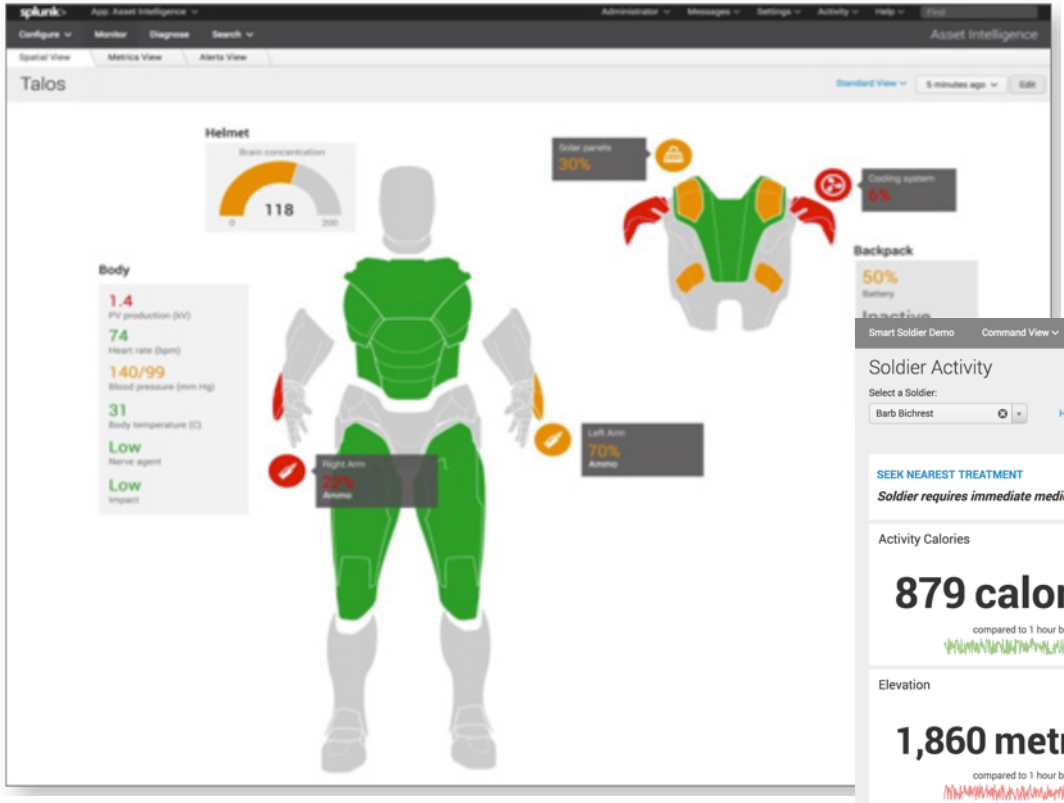


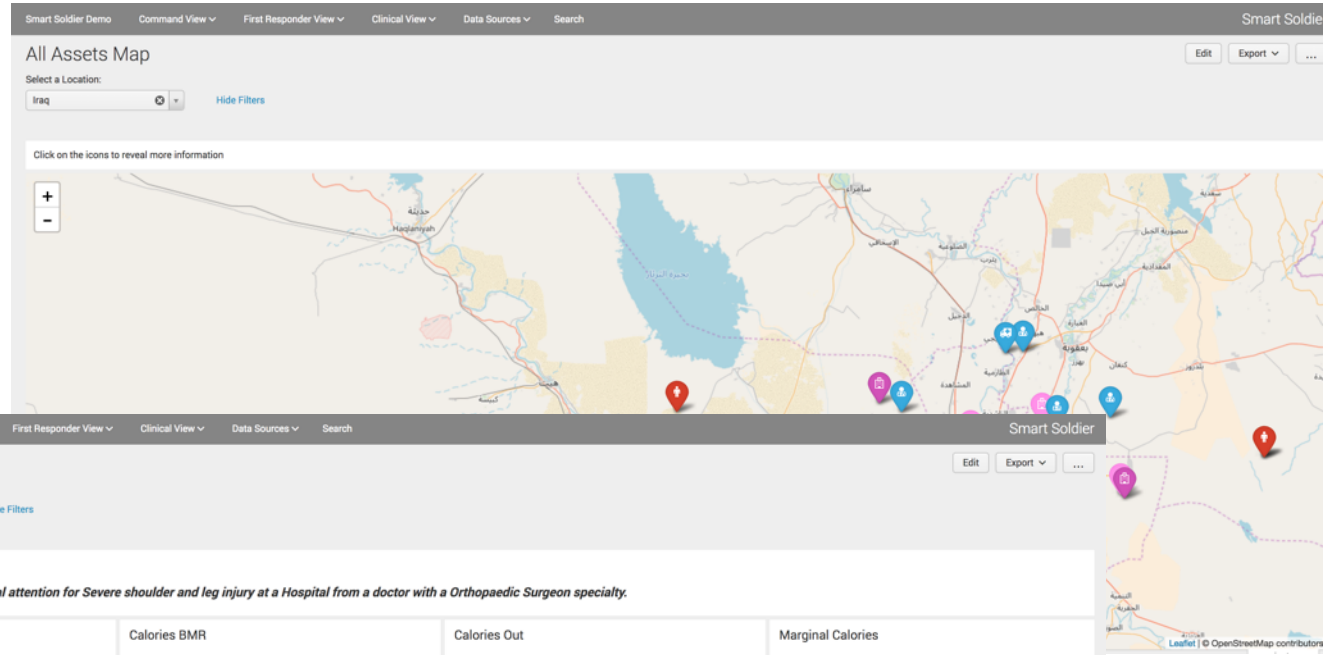


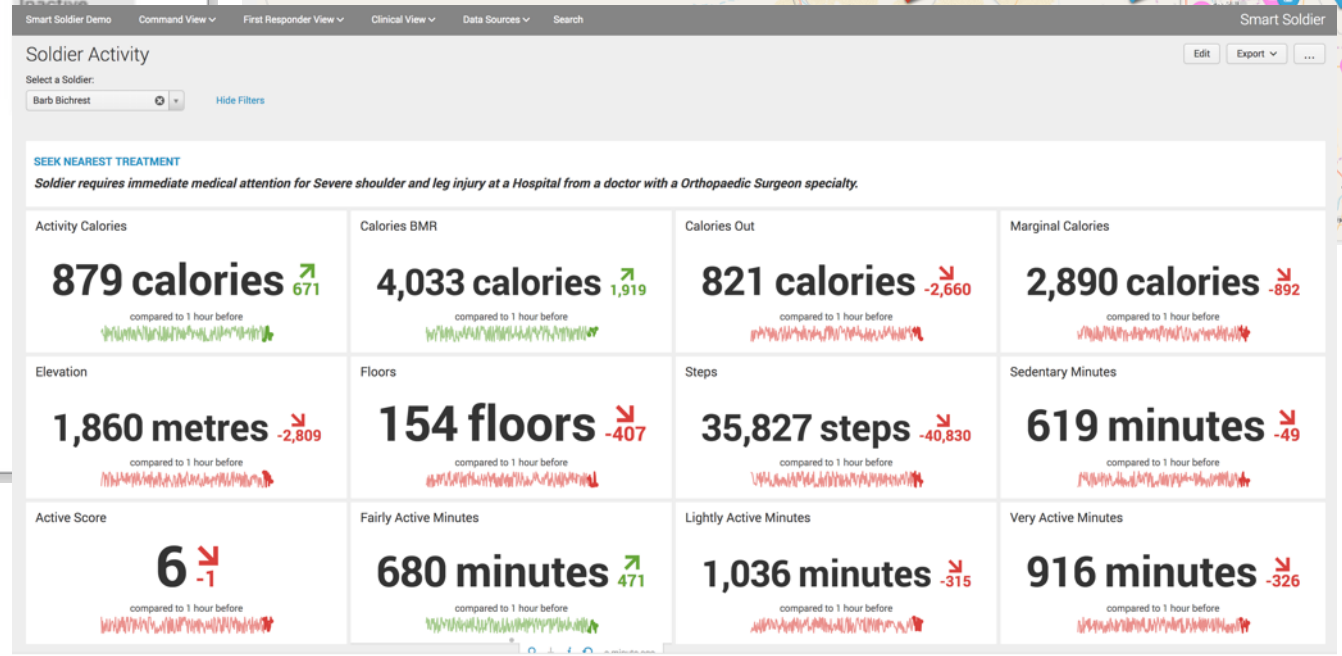
splunk> .conf18

Smart Soldier

Art of the possible



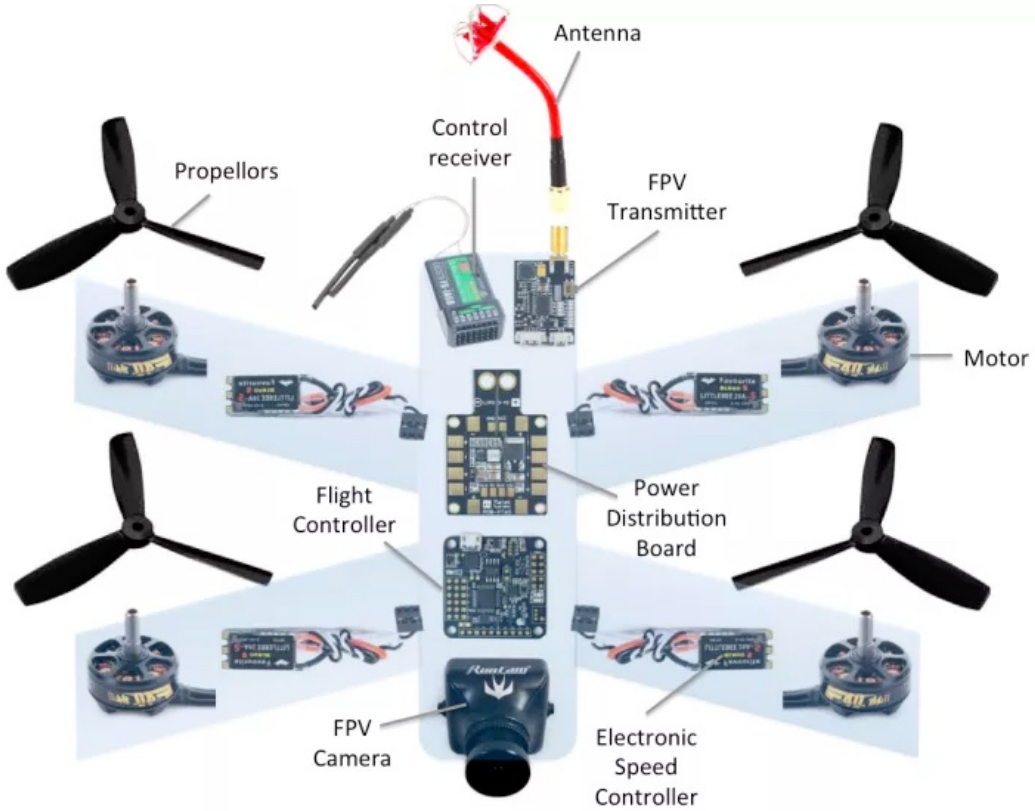




splunk> .conf18

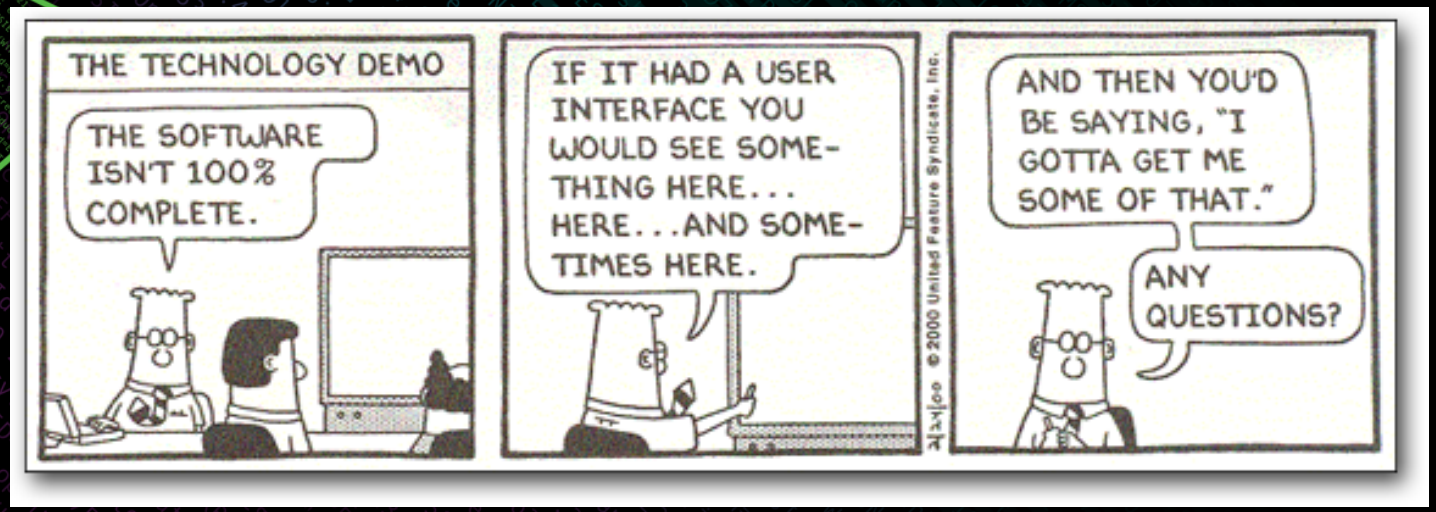
Now … there is lots to a remote IOT device

Where do you start?



- Complex machine
- Multiple parts need checking for intrusion
- External dependencies (APIs)
  - GPS
  - RF
  - LTE
  - WIFI

Demo time



splunk> .conf18

This doesn't look good!

GPS spoofing

Security

If the coordinates of the Internal Navigation Systems vs. GPS system are different, it can hint to a potential security breach in the form of a GPS spoof.

Edit | Export | ...

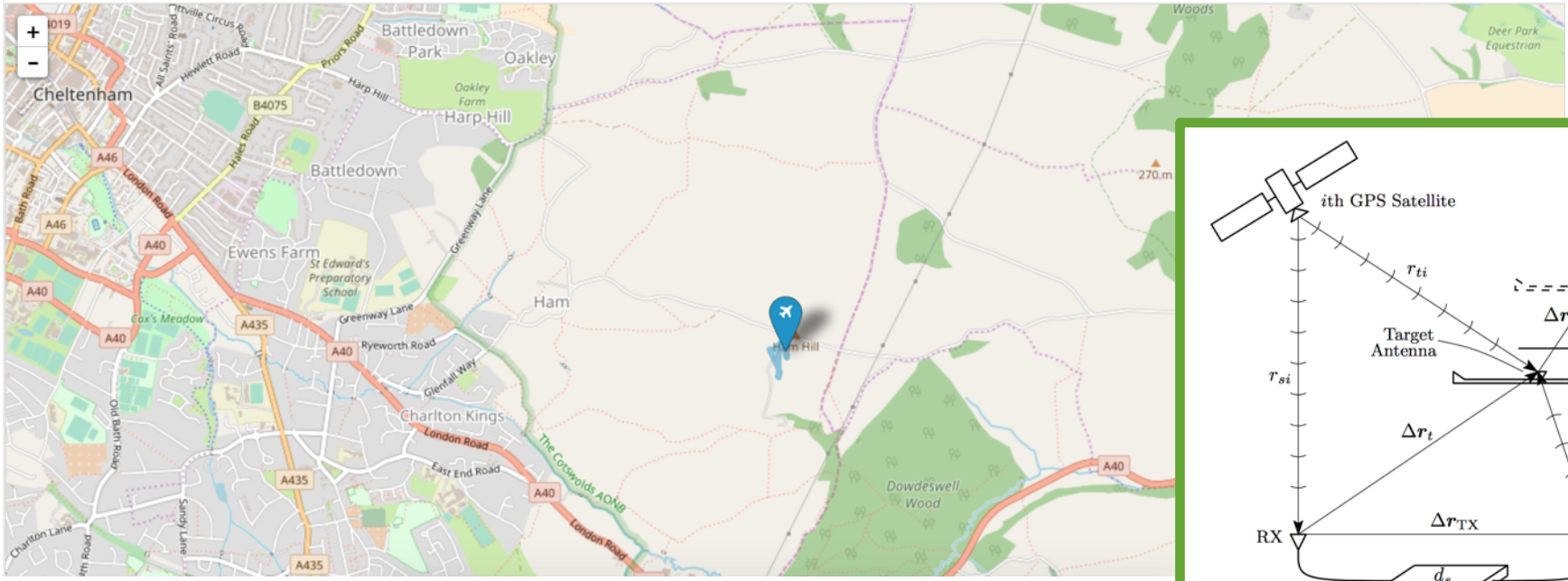
Potential GPS Spoofs

Time Since Spoof	Number of Attempts	Drone Name	INS Latitude	INS Longitude	Variance
0m 0.2s	14	drone1	51.8885418	-2.01918978	12.909

Current Status

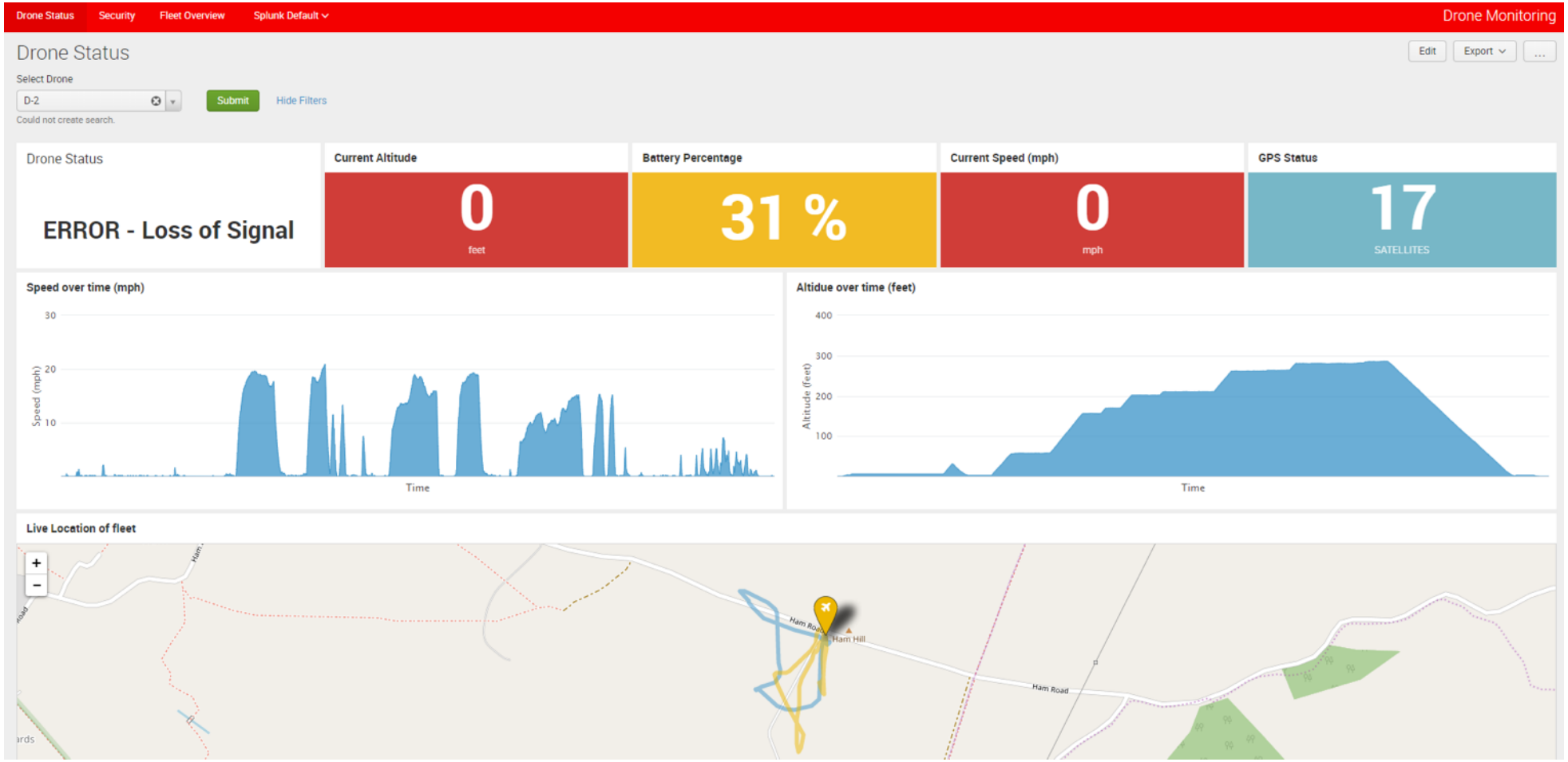
ERROR - Loss of Signal

Live Location of any Security Breached Drones



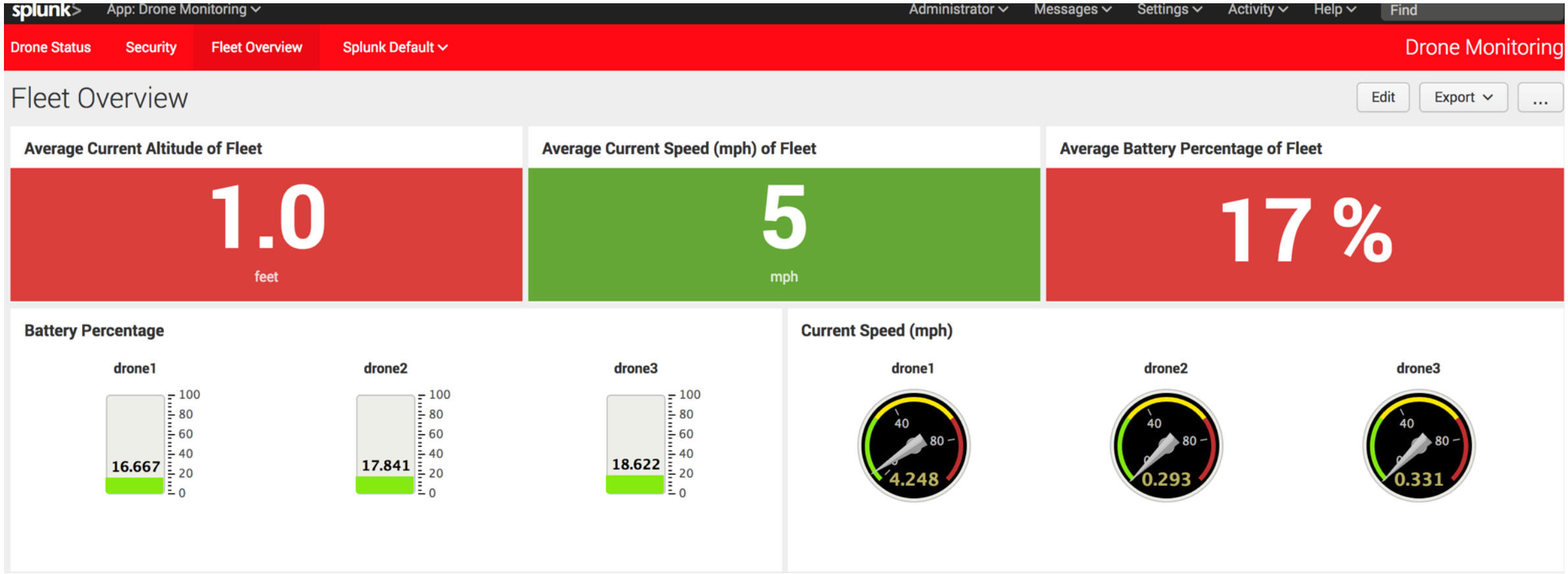
Drone Status

Operational insights



Fleet Management

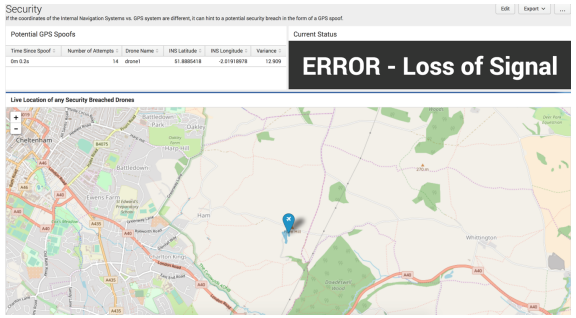
Proactive and predictive



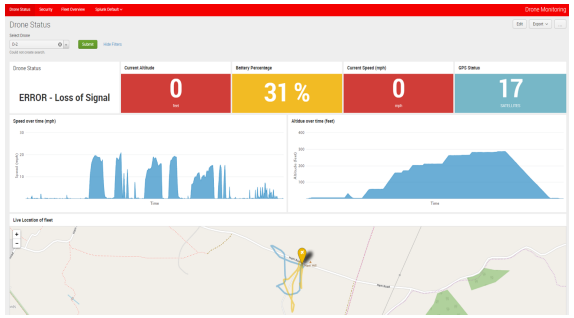
Summary

Global Challenges

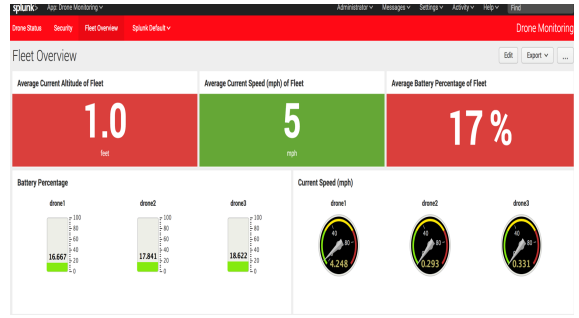
Just Splunk it



Cyber Resilience



Health & Preventative Maintenance Analytics



Fleet Management

Q&A

splunk> .conf18

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