



splunk> .conf2017

IT'S NOT
MAGIC.
IT'S SPLUNK.™

FIVE KEY TAKEAWAYS

from Splunk .conf2017

THE KEY ELEMENT IS DATA.

Another year, another .conf in the books. This year's event was jam packed with killer demos, adult beverages, and amazing stories of companies leveraging machine data.

But as with every major conference, there's so much to take in (and not enough time), the biggest thoughts can get lost. Well you're in luck - we've compiled the top five takeaways from .conf2017 so you don't have to spend time searching through notes or trying to recall what happened on that busy day in D.C.

TOP 5 TAKEAWAYS

- 1 **Machine Learning: Your New BFF**
- 2 **Metrics and Event Analytics are SO Hot Right Now**
- 3 **Security Success: Striking a Nerve**
- 4 **Innovating with Machine Data: The Airport of the Future**
- 5 **Data Can Make the World a Better Place: A Case Study**



1

KEY TAKEAWAY

Machine Learning: Your New BFF

Is Machine Learning a buzzword? Yes. But is it useful and valuable to you? Also yes.

Rather than focus on the buzzword, let's focus on why you should care: machine learning lets you analyze, act on, and even predict the future outcomes from your machine data.

BUT WHAT DOES THAT REALLY MEAN?

There are things humans are good at and things machines are good at. Bringing these together is the magic of machine learning - and also why data scientists are in such high demand (not to mention paid so much).

BUT I'M NOT A DATA SCIENTIST!

Step 1: Take a deep breath and say "it's going to be okay - Splunk has my back."

Step 2: Look into Splunk IT Service Intelligence and Splunk User Behavior Analytics - both machine learning seamlessly integrated to provide you with the answers you need, no data science degree required.

OH WAIT, I ACTUALLY AM A DATA SCIENTIST!

Then check out Splunk's Machine Learning Toolkit (link below), which includes out-of-the-box algorithms and the option to build custom algorithms and apply it to your machine data.

 [Learn more about Splunk Machine Learning](#)



2 KEY TAKEAWAY

Metrics & Event Analytics are **SO hot right now**

WHAT ARE METRICS?

Sets of numerical data sets that come in consistent patterns - the same format at the same rate.

WHY DO I CARE?

Because metrics have a consistent pattern, you can optimize for them.

HOW DOES THIS HELP MY JOB?

Monitoring is super important - but it isn't the end game. You still need to go through investigation and remediation if something has gone wrong.

Metrics can help you quickly identify issues - and when combined with events, you can pinpoint what happened, when it happened, and then dig into the raw data to investigate.

WHAT IS EVENT ANALYTICS?

Think "Event Management 2.0." Where **event management** has focused on addressing alerts from across your environment to find the "smoking gun," **event analytics** uses machine learning and artificial intelligence to help you prioritize which alerts need your immediate attention.

WHY DO I CARE?

Alert paralysis is a real thing. Too many alerts can be just as bad as not enough alerts - you don't even know where to start. Event analytics helps you find and address the most important alerts first.

HOW DOES THIS HELP MY JOB?

Now you can spend your time fixing the issues that matter most. That means you can quickly and easily identify existing and emerging issues, and prioritize how you restore business-critical services.

It's basically using data to make better decisions, rather than your best guess - not that you'd ever make bad guesses, of course.

 [Learn how to make your IT events less eventful.](#)



3

KEY TAKEAWAY

Security Success: Striking a Nerve

IN A WORLD OF UNCERTAINTY, ONLY ONE THING IS CERTAIN: YOU WILL GET BREACHED. IT'S NOT AN IF, IT'S A WHEN.

But it is possible for defense to have an unfair advantage over adversaries - and that advantage is the Security Nerve Center.

The nerve center provides a framework so regardless of who you are, you know your role and how you and your team can quickly move to diffuse the breach.

HOW THE NERVE CENTER SUPPORTS KEY SECURITY ROLES:

- **CISO:** You need situational awareness. You've made some major investments in technology, people, and processes. The nerve center helps you get the most out of your resources.
- **Analyst:** There's so much noise. You need to reduce as much of it as possible - and need a high-fidelity signal (read: reduce the noise) that will enable you to take action when you're ready to.
- **Threat Hunters:** You need to ask questions, to pivot quickly, and to contextualize data as you see fit - that way you can move on to track the target that you're after.

So now the million dollar question: you've just been breached. How do you react?

 [Learn how companies are using Splunk to address modern security challenges.](#)



4

KEY TAKEAWAY

Innovating With Machine Data: The Airport of the Future

Dubai Airport is one of the busiest airports in the world - and is a prime example of how analyzing machine data is creating the airport of the future.

DUBAI AIRPORT BY THE NUMBERS

Top 5 Airport in the World

Accounts for 2.5% of Dubai's total energy usage

A 20% decrease in energy would result in \$25M saved per year

A TRIP THROUGH THE AIRPORT OF THE FUTURE

Security

- Goal: Get passengers through security in five minutes or less
- Sensors in the ceiling measure security lines
- Analyzing this data can predict whether new security lines need to be opened

Wifi

- Dubai has the fastest airport wifi in the world
- Wifi is monitored in real time, with thousands of people online
- Wifi security is a priority, and rogue access points are taken down as they appear

Baggage

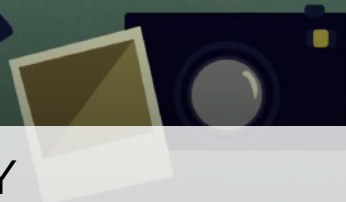
- The entire baggage system is monitored in real time - from ground handler systems to airline check in systems
- 150,000 conveyor belts
- 150 million bags per year
- 200 data points per bag
- The airport can predict bottlenecks up to four hours in advance

The Golden Bathroom

- Two bathrooms are monitored by sensors
- Sinks, stalls, urinals
- Goal is to understand usage
- About 75% of people wash their hands



Not sure what machine data to analyze? [Check out the Essential Guide to Machine Data.](#)



5

KEY TAKEAWAY

Data Can Make the World a Better Place: **A Case Study**

We all know that data has the power to increase your security posture, or to improve your IT operations. But we often forget that data also has the power to have a real impact on the world around us. Global Emancipation Network is a tangible example of how data can be used to make the world a better place.

QUICK OVERVIEW

Who: Global Emancipation Network

What: Using data and technology to counter human trafficking, such as labor, sex, forced adoption, and forced marriage

How: By sharing data to break down data silos across the thousands of nonprofit organizations, law enforcement agencies, and government agencies dealing with human trafficking

Human trafficking affects between 21 million and 43 million people worldwide. These are people who are forced into marriages, unpaid labor, and otherwise exploited - it's modern-day slavery. In some cases, this is a real threat to life, as a lot of victims die from neglect. Thankfully, there are thousands of agencies across nonprofit, government, and law enforcement working to address this challenge.

The Global Emancipation Network is a platform that breaks down the data silos across these organizations in order to share and make data usable.

The goal is to reach a point where data is used to predict where trafficking might occur so it can be stopped.

The idea is to collect as much data as possible to create an encyclopedia of traffic indicators. That means collecting tens of millions of records across text messages, images and human knowledge, then making the information usable for the agencies the organization serves.

“ We want to show the technology community that good is possible in the world with what you do...and you can tackle true evil with what you do.”

Sergio Caltagirone
Technical Director, Global Emancipation Network



[Watch the video on how “Tech Strikes Against Modern-Day Slavery”](#)