Splunking refugees with NetHope and Cisco Meraki

Corey Marshall | Director, Splunk for Good
Satoshi Kawasaki | Splunk for Good Ninja

splunk> .conf19

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or plans 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 may differ materially. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, it may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements made herein.

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 functionalities described or to include any such feature or functionality in a future release.

Splunk, Splunk>, Turn Data Into Doing, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2019 Splunk Inc. All rights reserved.

Bio: Corey Marshall

Director, Splunk for Good

- BA in Political Science from Lewis & Clark College
- Master's in Public Policy from the University of Chicago
- Joined Splunk in 2013
- Advising government and non-profits on open data for more than 15 years, including working with
  - City and County of San Francisco
  - Accenture
  - Office of Chicago Mayor Richard M. Daley
- Lead company’s efforts in social impact
  - Employee service and engagement
  - Community giving
  - Sustainability

Bio: Satoshi Kawasaki

BS in Aerospace Engineering from Georgia Tech

hobbes3

1) **Joined Splunk in 2013**

   3 years in Splunk Professional Services (PS)

   3+ years in Splunk for Good

2) **Previous conf talks:**

   conf14: *I want that cool viz in Splunk!*

   conf15*: Enhancing dashboards with javascript!*

   conf17: *Speed up your searches!*

   conf17: *Splunking to fight human trafficking!*

   conf17: *Splunking the 2016 presidential election!*

3) **This year's conf talks:**

   conf19: *Speed up your searches!*

   conf19: *Splunking refugees with help from NetHope and Cisco!* YOU ARE HERE

   conf19: *Splunking the 2018 midterm election!*

   conf19: *Send your spreadsheets to Splunk!*

Table of Contents

From big data to refugees

1. The organizations
2. The goals with Splunk
3. The data sources
4. The flow of data
5. The software
6. The actual data
7. The possibilities
8. The issues

The organizations

Partnerships to achieve good.

Splunk for Good

Big data can make a big difference

NETHOPE

MercyCorps

INFORMATION TECHNOLOGY • DISASTER RESOURCE CENTER •

- $100 million Splunk Pledge has issued licenses and training worth over $40 million.
- Workforce training initiatives for veterans, students and opportunity youth have reached more than 10,000 people.
- Engaging partners to develop shared solutions for humanitarian response, human trafficking, and more.
- Nearly 150,000 hours of paid volunteer time per year.

NetHope and Cisco

IT connectivity for those in need

- NetHope is a consortium of nearly 60 global nonprofits which collaborate to solve humanitarian challenges using technology.
- Cisco Meraki is a cloud-based IT company known most notably for mid-sized wireless networks.
- Meraki donates hardware, such as the MX model routers and MR model antennas.
- The partnership deploys connectivity to countries and areas affected by disasters.

NetHope and Splunk

Field Network Operations Center

- **Availability and uptime** of global network devices.
- **Usage** of each device - by individuals and members across locations
- **Return on investment** for NetHope members and funders
- Advanced analytics to help inform global response to **humanitarian and refugee crises**

The data sources

Getting all of the "traditional" IT data sources

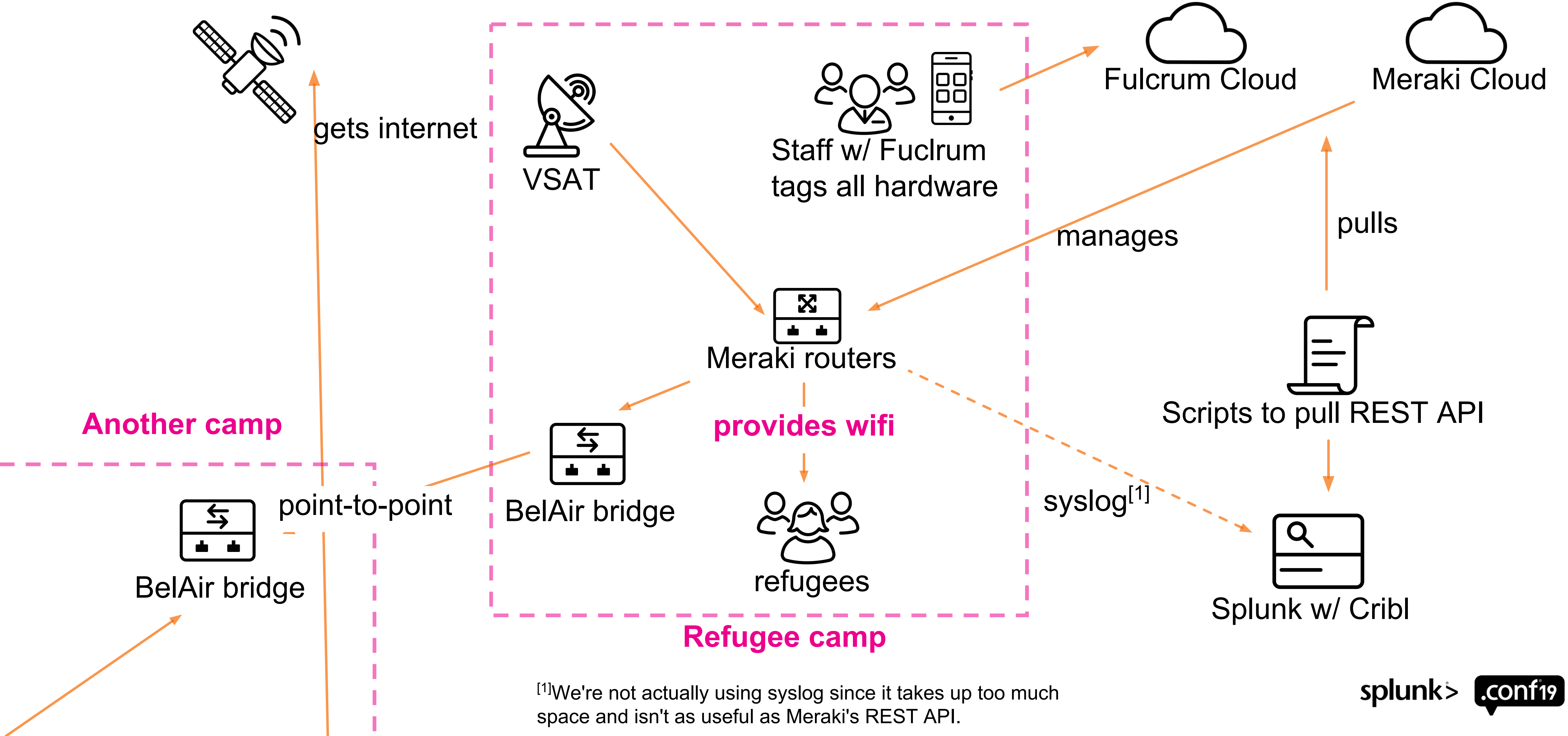
1. Meraki REST API
2. Fulcrum REST API
3. BelAir Networks[1]
4. Ubiquiti Networks[1]
5. VSATs[1]

[1] Potential future implementations.

The flow of data

The IT architecture of a refugee camp

The simplified architecture



gets internet

VSAT

Staff w/ Fuclrum tags all hardware

Fulcrum Cloud

Meraki Cloud

manages

pulls

Meraki routers

Scripts to pull REST API

Another camp

provides wifi

point-to-point

BelAir bridge

BelAir bridge

refugees

syslog[1]

Splunk w/ Cribl

Refugee camp

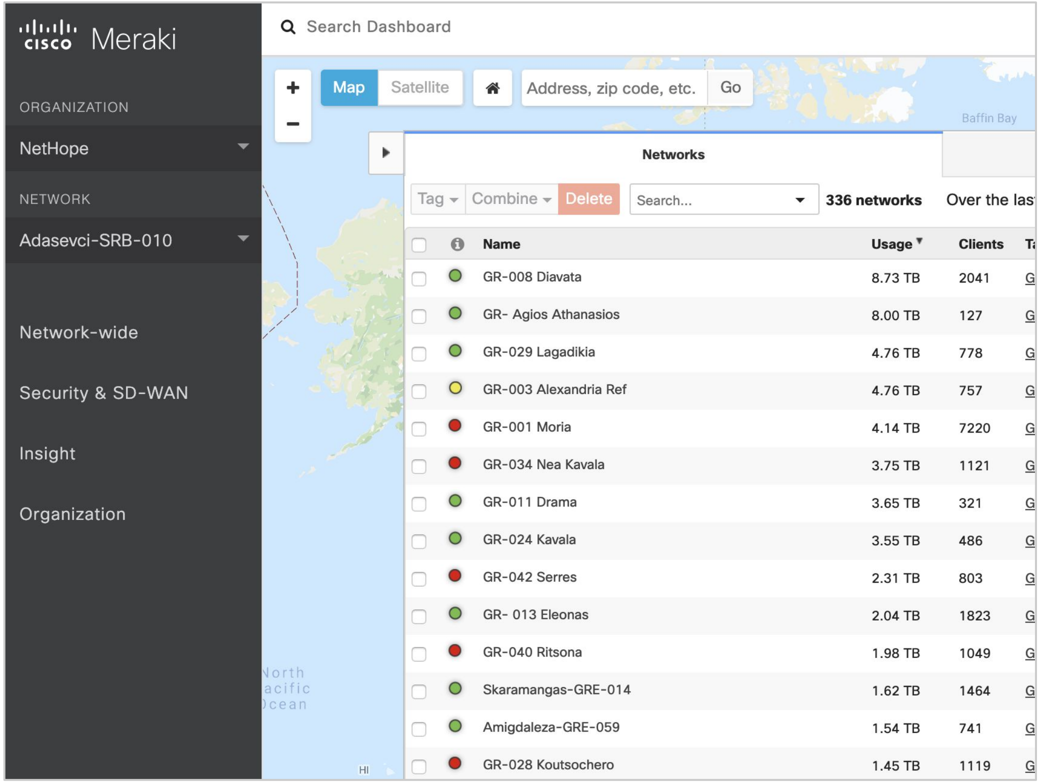
[1]We're not actually using syslog since it takes up too much space and isn't as useful as Meraki's REST API.

The software

Different software. Different purpose.

The cloud-based platforms

Mostly machine data

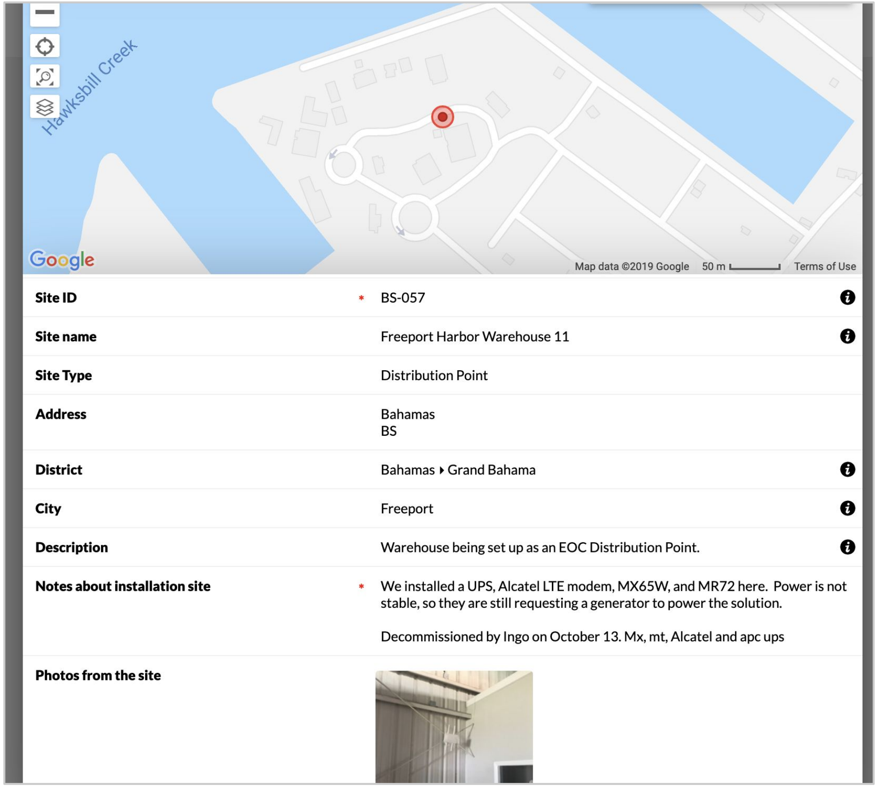


336 networks Over the las

□		Name	Usage	Clients	T
□	🟢	GR-008 Diavata	8.73 TB	2041	G
□	🟢	GR- Agios Athanasios	8.00 TB	127	G
□	🟢	GR-029 Lagadikia	4.76 TB	778	G
□	🟡	GR-003 Alexandria Ref	4.76 TB	757	G
□	🔴	GR-001 Moria	4.14 TB	7220	G
□	🔴	GR-034 Nea Kavala	3.75 TB	1121	G
□	🟢	GR-011 Drama	3.65 TB	321	G
□	🟢	GR-024 Kavala	3.55 TB	486	G
□	🔴	GR-042 Serres	2.31 TB	803	G
□	🟢	GR- 013 Eleonas	2.04 TB	1823	G
□	🔴	GR-040 Ritsona	1.98 TB	1049	G
□	🟢	Skaramangas-GRE-014	1.62 TB	1464	G
□	🟢	Amigdaleza-GRE-059	1.54 TB	741	G
□	🔴	GR-028 Koutsochero	1.45 TB	1119	G

Meraki is a cloud-managed platform that enables network management and configuration.

Mostly human data

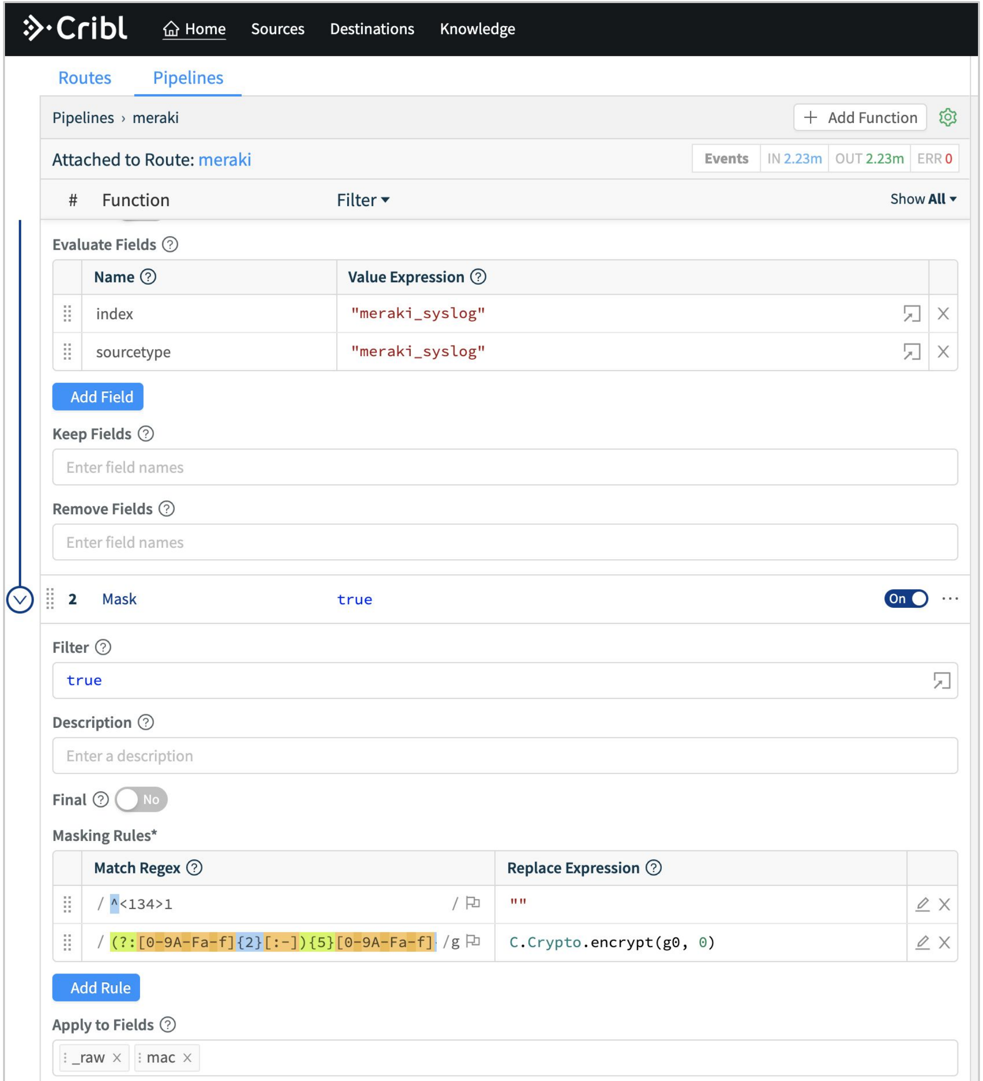


Site ID *	BS-057
Site name	Freeport Harbor Warehouse 11
Site Type	Distribution Point
Address	Bahamas BS
District	Bahamas ▸ Grand Bahama
City	Freeport
Description	Warehouse being set up as an EOC Distribution Point.
Notes about installation site *	We installed a UPS, Alcatel LTE modem, MX65W, and MR72 here. Power is not stable, so they are still requesting a generator to power the solution. Decommissioned by Ingo on October 13. Mx, mt, Alcatel and apc ups
Photos from the site	

Fulcrum is a cloud-managed platform that enables users to build mobile forms and collect data anywhere.

Cribl

The Swiss army knife for data



Attached to Route: meraki

Evaluate Fields

Name	Value Expression
index	"meraki_syslog"
sourcetype	"meraki_syslog"

Keep Fields: Enter field names

Remove Fields: Enter field names

2 Mask true

Filter: true

Description: Enter a description

Final: No

Masking Rules*

Match Regex	Replace Expression
/ ^<134>1 /	""
/ (?:[0-9A-Fa-f]{2}[:-]){5}[0-9A-Fa-f] /g	C.Crypto.encrypt(g0, 0)

Apply to Fields: _raw, mac

Cribl enables routing, securing, enriching, and transforming of log data in motion.

How we use Cribl for NetHope:

- **Encrypt all MAC addresses.** MAC addresses can be decrypted in Splunk via a custom search command.
- **Act as a syslog server** to more reliably listen for syslog and forward them to Splunk.

The actual data

The different types of data

Data correlation

Putting it all together

Meraki REST API	Fulcrum REST API
List of devices	List of all devices (not just Meraki)
Geographical location of devices	Detailed installation notes
Uptime and performance of devices	
Usage of devices	On-site point of contact info
Device serial number	Device serial number
MAC address of devices and clients	

The most important metric

How can traditional IT data be used for refugee analytics?

1 **unique** client MAC address = 1 refugee

The possibilities

Refugee analytics using MAC addresses

- Unique MAC addresses approximate **the number of refugees in a location.**

- Tracking unique MAC addresses at different sites indicates **migration** from camp to camp.

- Client web history can approximate **demographics** (men vs women, adult vs child, etc.) and how they spend their time.

- Splunk mobile solutions can **unlock potential** for impact in remote locations.

The issues

Most problems stem from humans

Human-entered data is **prone to errors and typos.**

- **Accidental entry** of wrong serial numbers (or scanned the wrong barcode).
- Meraki devices with **incorrect geographical locations** (like devices still in California).

Majority of web traffic recorded by syslog is SSL encrypted so **Meraki can only see the host** (and not the path) of a URL.

Syslog is very chatty, so it's a burden on the Splunk license and disk space.

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference and (2) this device must accept any interference received, including interference that may cause undesired operation.

Closing remarks

Corey Marshall | Director, Splunk for Good

splunk> .conf19

Just when you think you know Splunk…

Data to Everything, Everywhere, Everyone

- There are lots of opportunities **to make an impact with data and Splunk:**
- **Same platform** we know and love, new and **different operating context**
- What many of us think of as routine machine data can hold the keys to **powerful insights**
- **Connectivity is the foundation** for critical humanitarian services and resources
- **Splunk is the perfect tool** for the range of needs, users, conditions
- **We can mobilize** our entire ecosystem of partners and customers

There is **always** more we can do:

- **What other causes could benefit from Splunk expertise?**

Q&A

Corey Marshall | Splunk for Good Director
Satoshi Kawasaki | Splunk for Good Ninja

splunk> .conf19

.conf19

splunk>

Thank You!

Big thank you to
John Crowley from NetHope, the
Cisco Meraki and TACOPS teams,
and the entire **Cribl team**!

Go to the .conf19 mobile app to

RATE THIS SESSION