SITCH
v3.3

Inexpensive, coordinated GSM anomaly detection

About Me

- 2000: Technology career started (I can get paid for this??)
- 2003: Started building with Linux
- Came to infosec through systems and network engineering, integration
- Security tools and integration (SIEM, HIDS, etc...)
- Current: R&D

About You

- Background in systems and network engineering
- Interested in GSM threat detection
- Tinfoil hat not required... but not unwelcome!

“Thoughts and opinions expressed are my own. If you take anything away from this talk and act on it, I’m not responsible if you go to jail, become a pariah, or your dog stops liking you. Know the laws you’re subject to and operate accordingly.”

–Ashmastaflash

What We're Covering Today

- Why Care?
- Current Threat and Detection Landscape
- Project Goals
- SITCH: MkI
- SITCH: MkII
- Service Architecture
- SITCH: MkIII
- Lessons Learned / Future Plans
- Prior Art
- Q&A

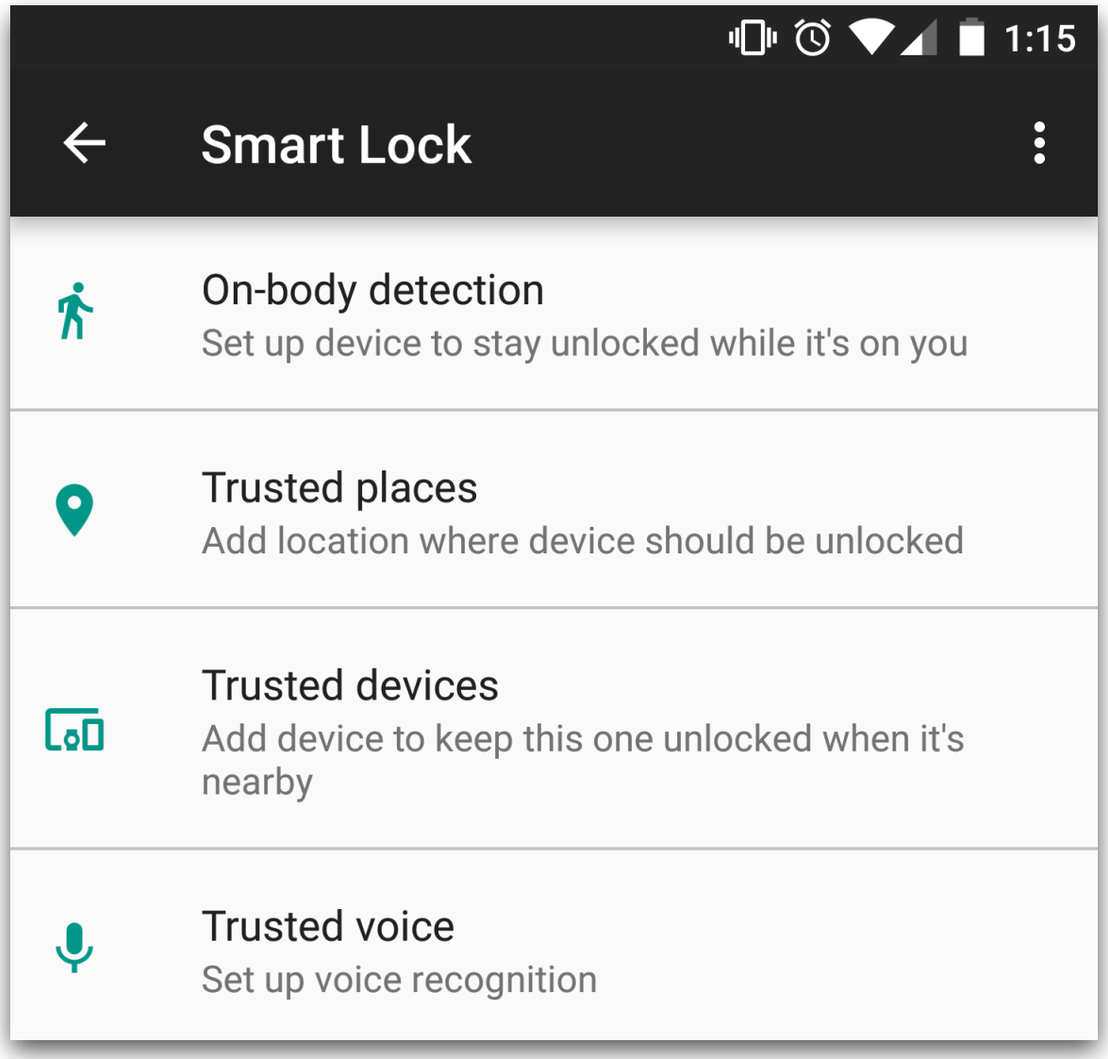
Why Care?

- Invasions of privacy are bad, even when they're unnoticed.
- Industrial espionage costs money and jobs.

WTF Is Under All That??

Is Anybody Home?

Why would you even...



...think about geo-unlocking

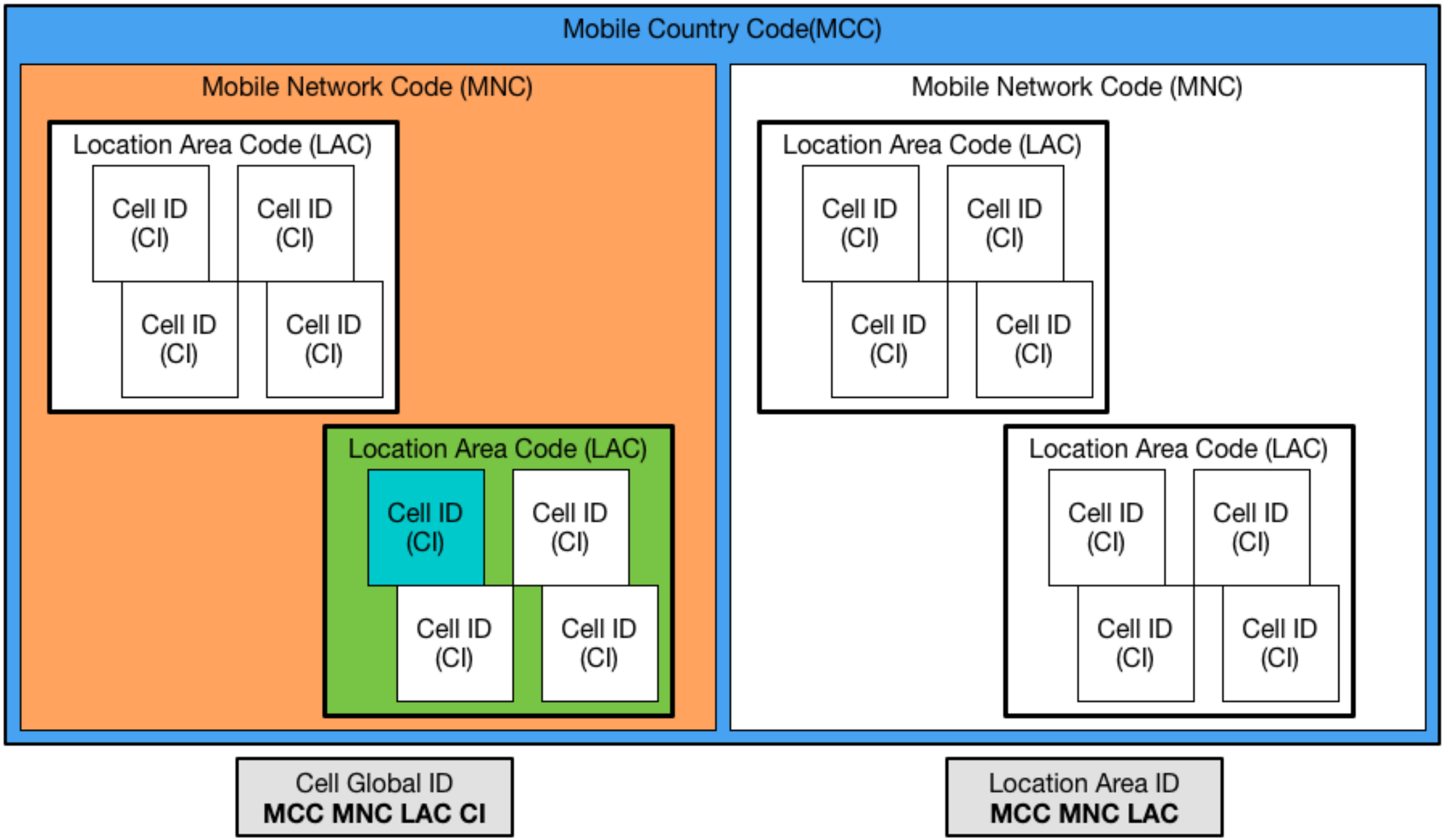
DEF CON 23

- Low-cost GPS Simulator - GPS Spoofing by SDR
  - Lin Huanh, Qing Yang from Qihoo 360 Unicorn Team
  - Use SDR (USRP, BladeRF)

Terminology

- Software Defined Radio (SDR): Using software to perform signal processing in concert with an adjustable-frequency RF receiver
- ARFCN: Absolute Radio Frequency Channel Number
- BTS: Base Transceiver Station
- CGI: Cell Global ID (MCC + MNC + LAC + CI)
    - MCC: Mobile Country Code
    - MNC: Mobile Network Code
    - LAC: Location Area Code
    - CI: Cell ID
- LAI: Location Area ID (CGI minus Cell ID)
- IMSI: International Mobile Subscriber Identity

GSM Addressing



Threat and Detection Landscape

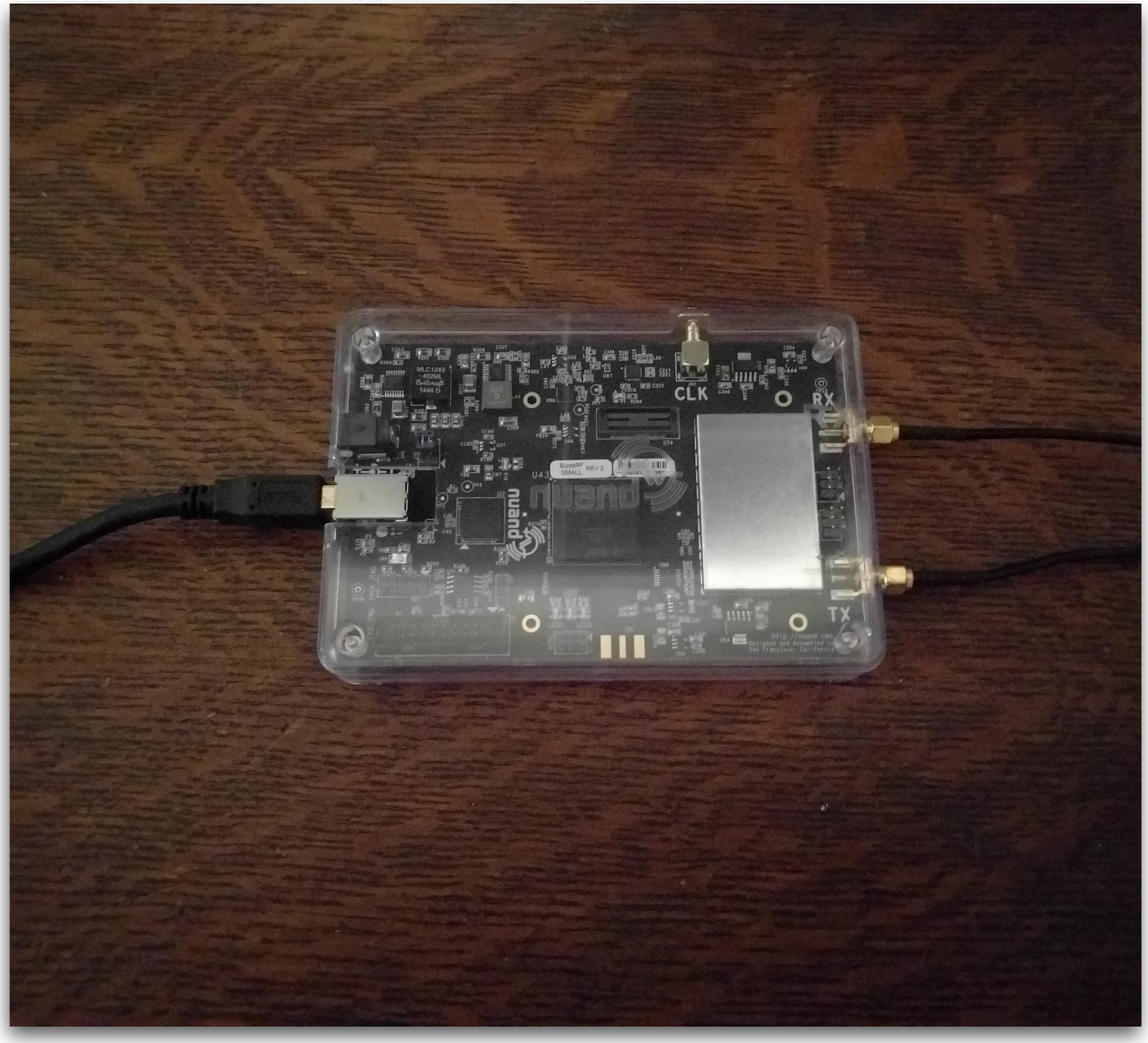
- Malicious Devices
- Indicators of Attack
- Existing Detection Methods

Hacked Femtocell

Trusted part of provider's network
Your phone doesn't know it's evil

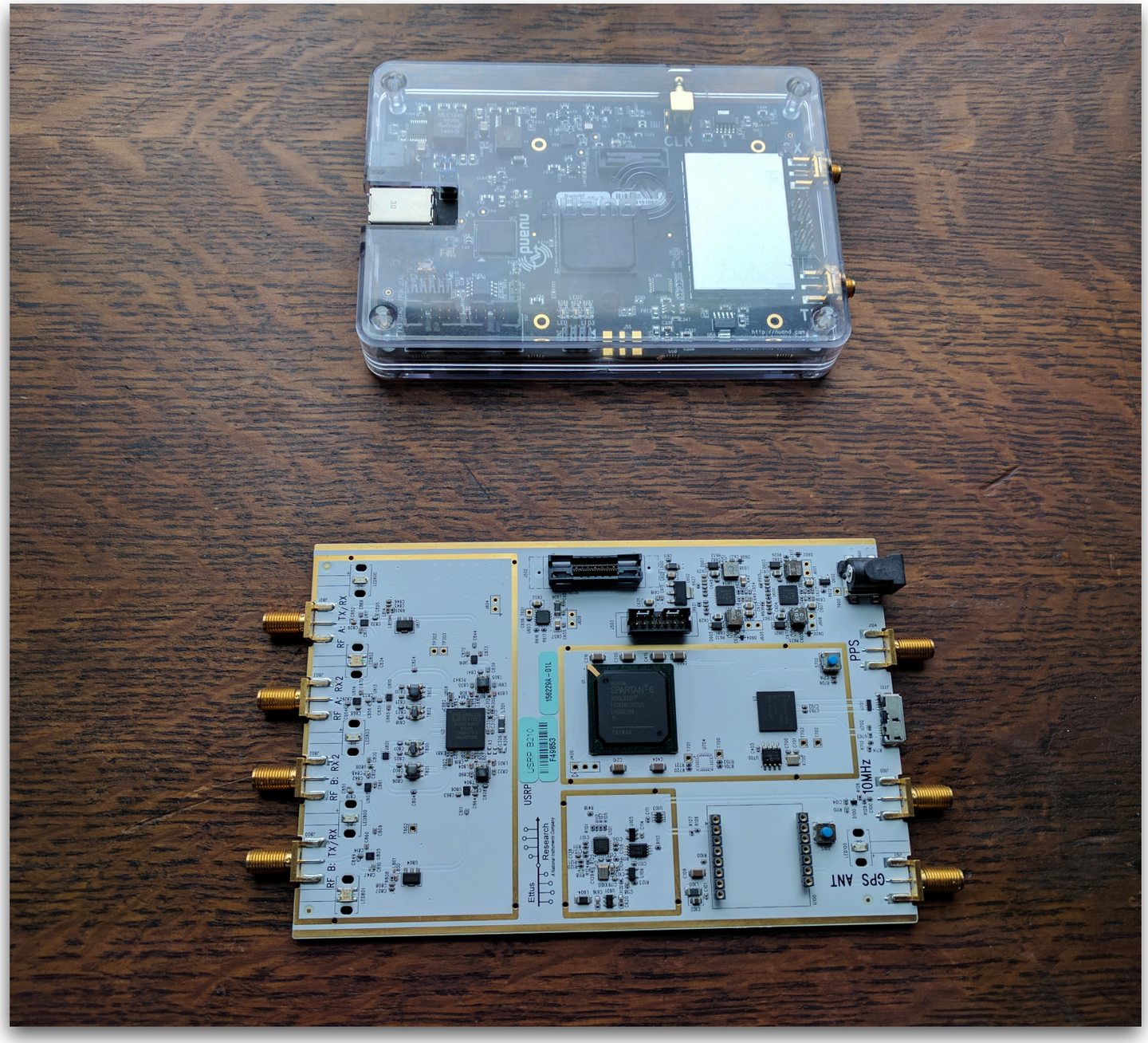
Evil BTS

Handset will automatically associate, unable to assert trustworthiness



GPS Simulator

Causes clock drift and incorrect location detection



Indicators of Attack

- ARFCN over threshold
- ARFCN outside forecast
- Unrecognized CGI
- Gratuitous BTS re-association
- BTS detected outside of range

Detection Methods

- Commercial Options:
  - Pwnie Express
  - Bastille Networks
- Open Source:
  - Fake BTS
  - AIMSICD
  - Femto Catcher

Project Goals

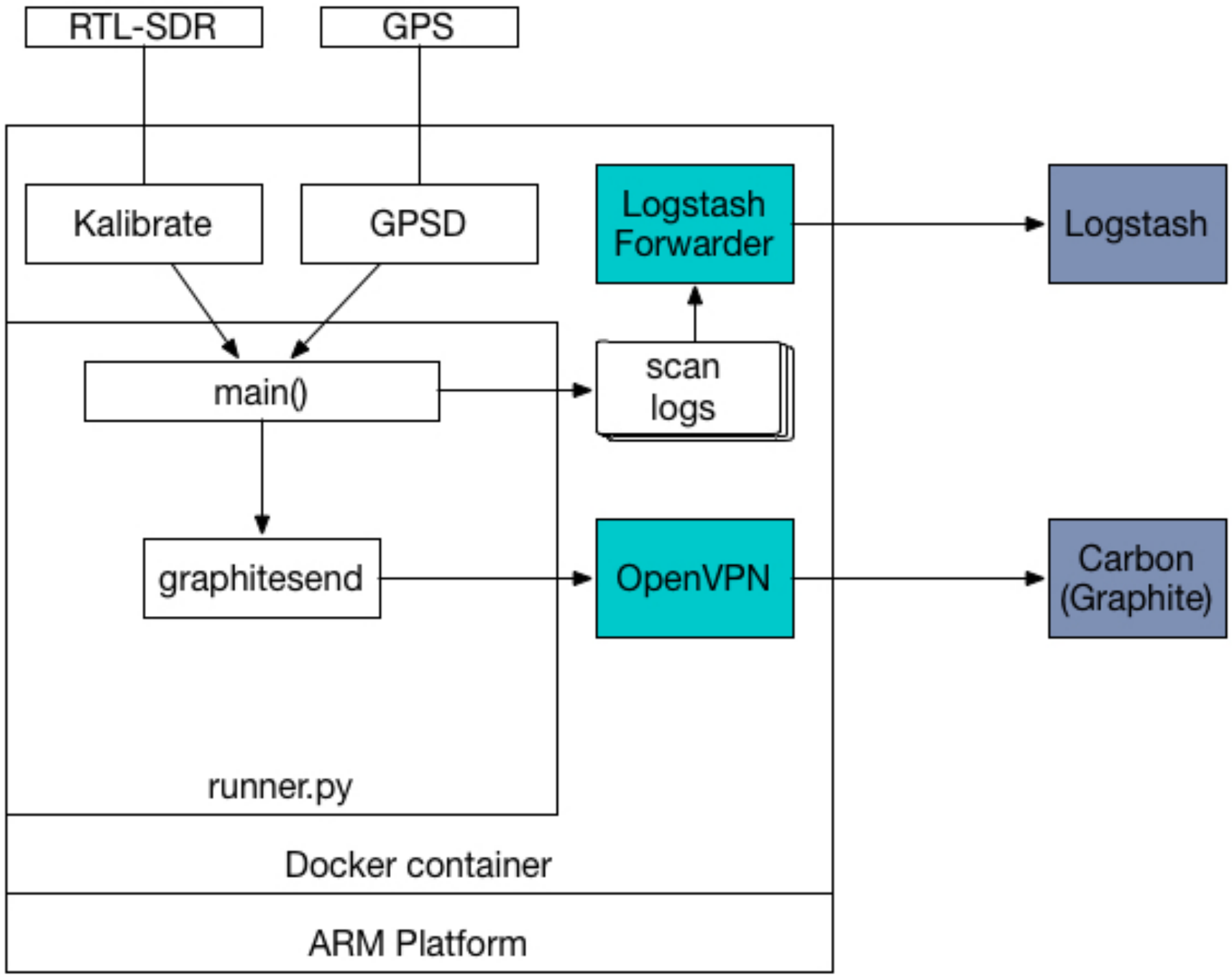
- Inexpensive
  - Cost < Price of malicious device
- Small footprint, low power requirements preferred
- Functional Targets: Indicators of Attack (IOA) Coverage
- Centrally managed software and configuration


NooElec
NooElec

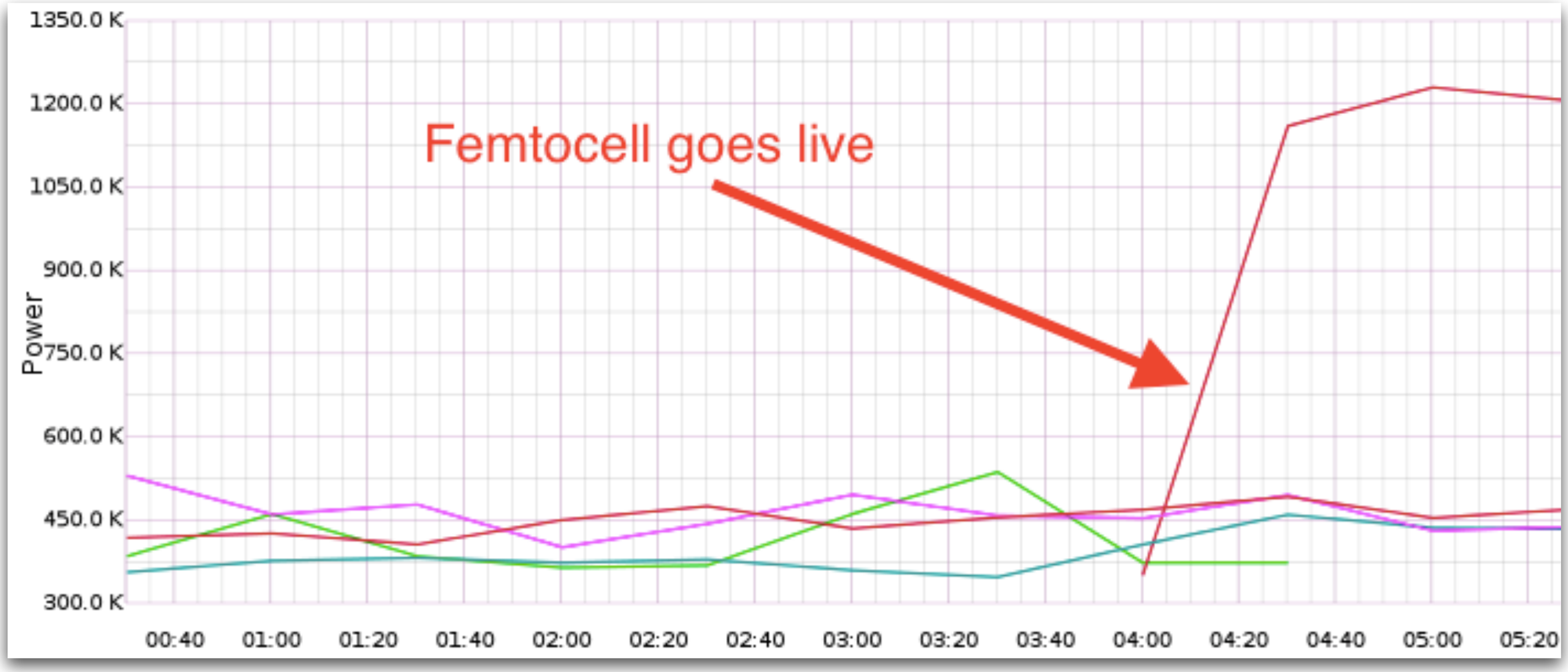
SITCH

Situational Information from Telemetry and Correlated Heuristics

SITCH Sensor MkI



SITCH Sensor MkI



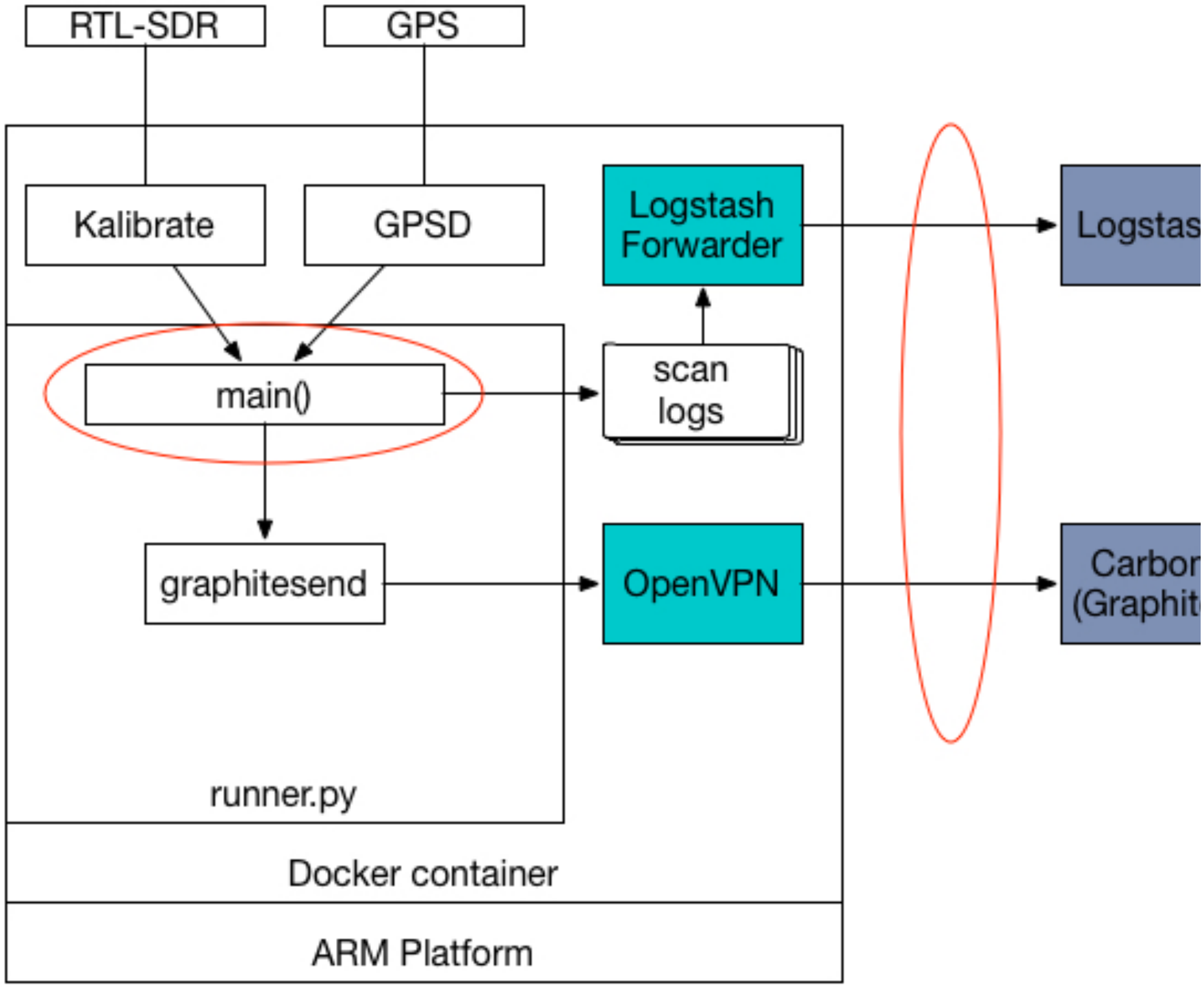
MkI Results

Targets	MkI Coverage
ARFCN over threshold	YES
ARFCN outside of forecast	YES
Unrecognized CGI	NO
Gratuitous BTS re-association	NO
BTS detected outside of range	NO
Price	~$100

Releasing MKI?

No.

What's wrong with MkI?

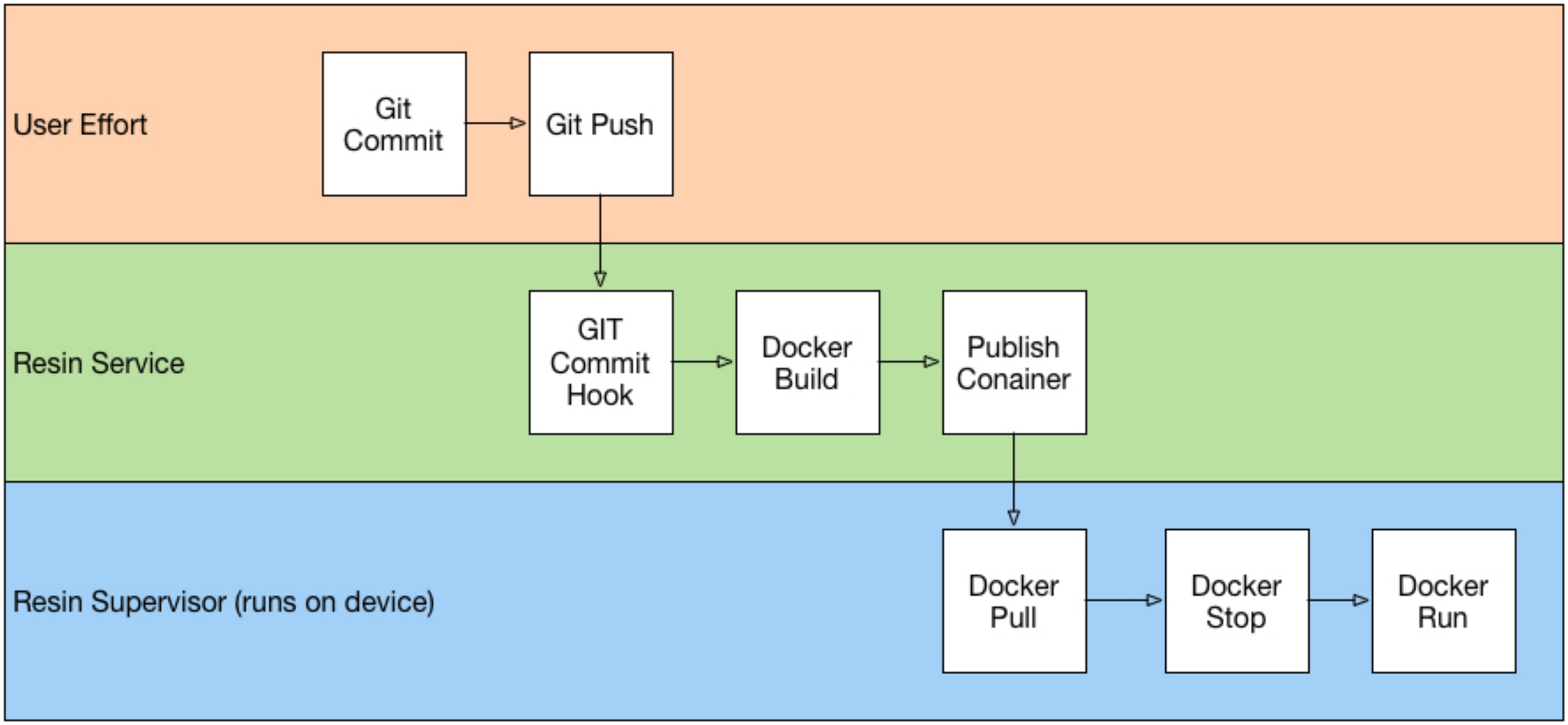


Live demo?

- Friday the 13th
- Holiday weekend
- Last night: full moon


MakeAGIF.com

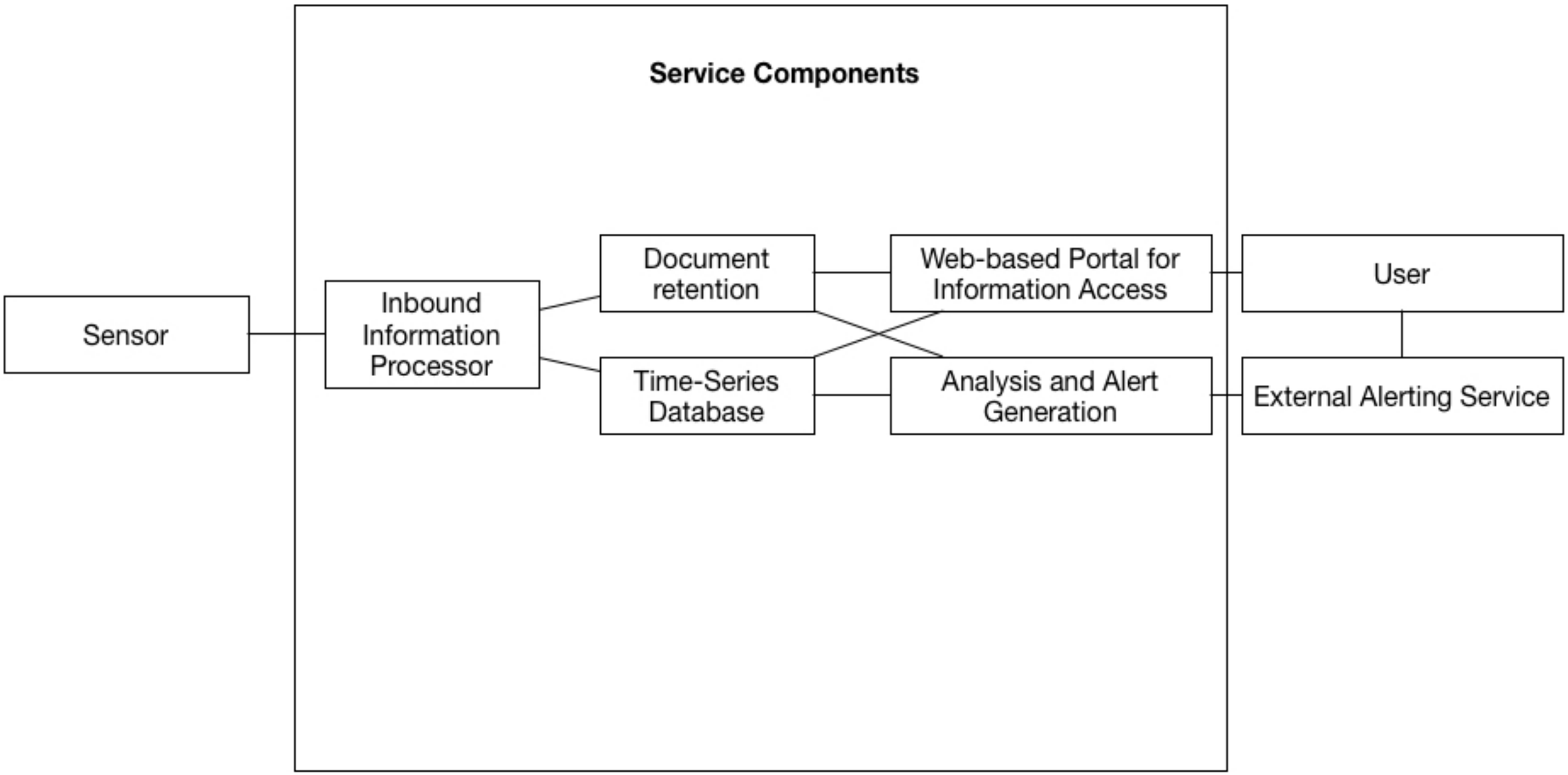
Deployment Pipeline



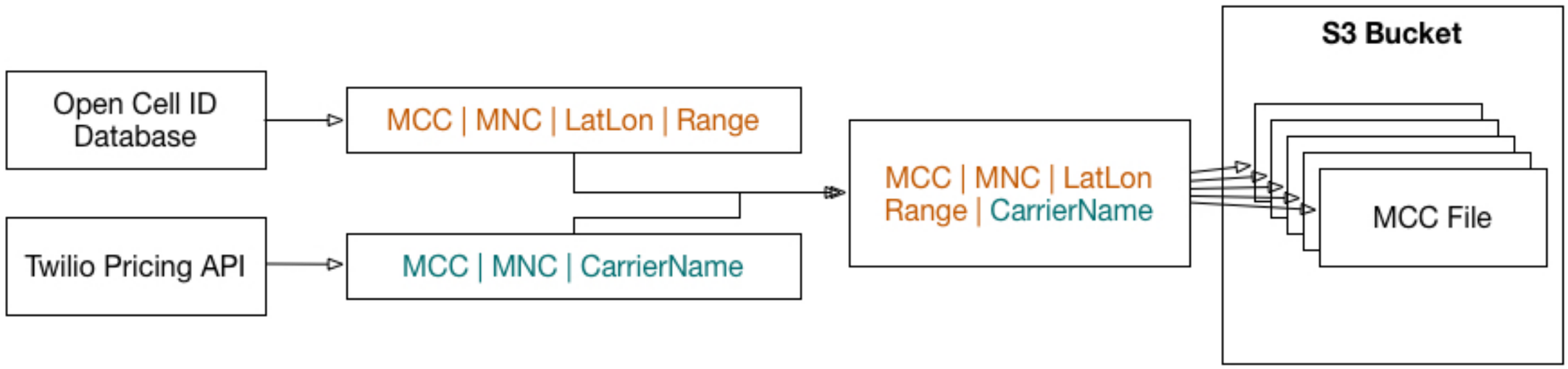
Service-Side Software

Tool	Purpose
Logstash	Inbound Information Processing Alert delivery
Elasticsearch	Scan document retention
InfluxDB	Time-series database Statistical analysis of time-series data
Kibana	Browse scans
Chronograf	Dashboard for InfluxDB
Telegraf	TSDB alerting (replaces graphite-beacon)
Vault	Secret management
Resin	Sensor software management
Slack	Notifications

SITCH Service Architecture

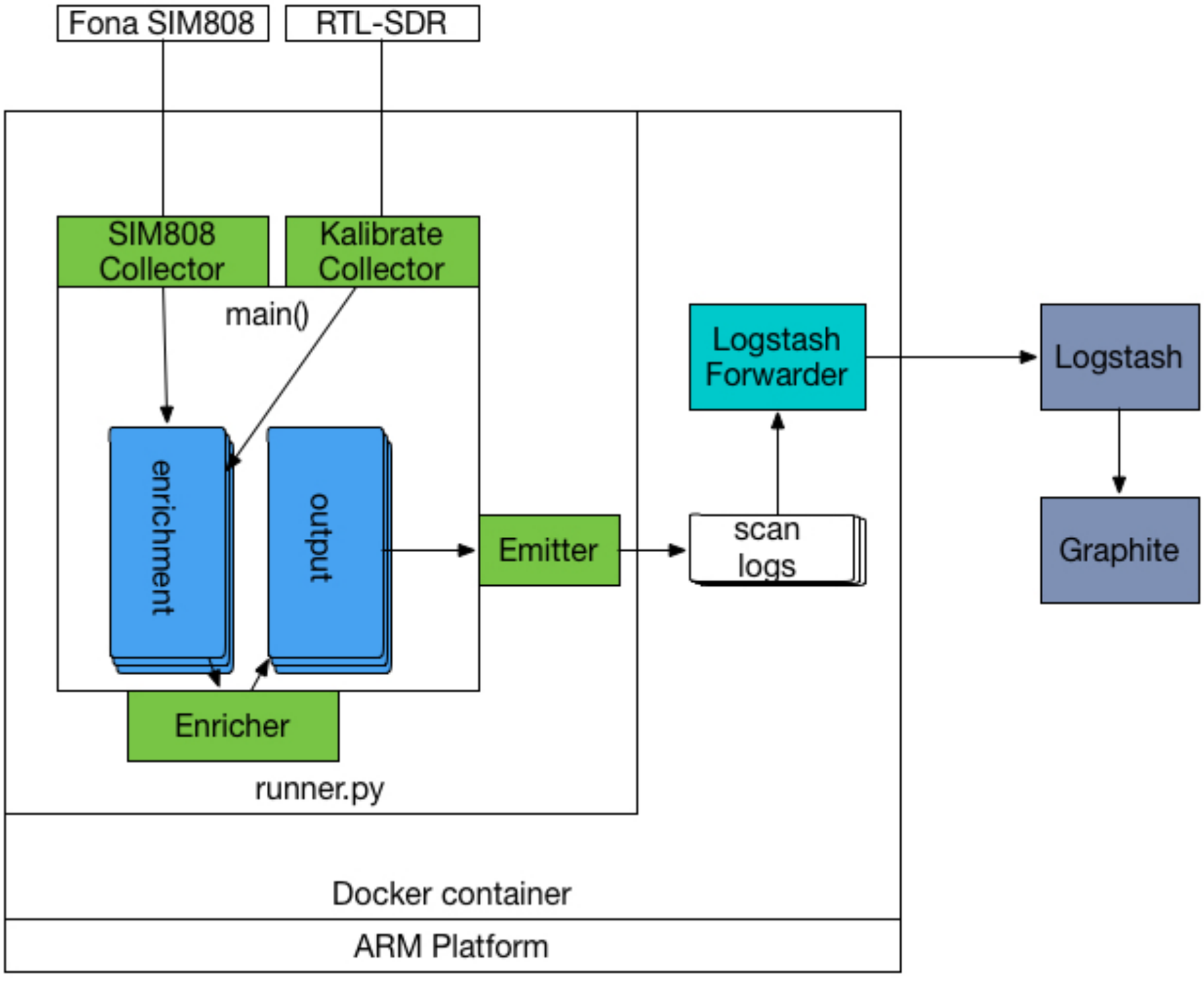


SITCH Intelligence Feed

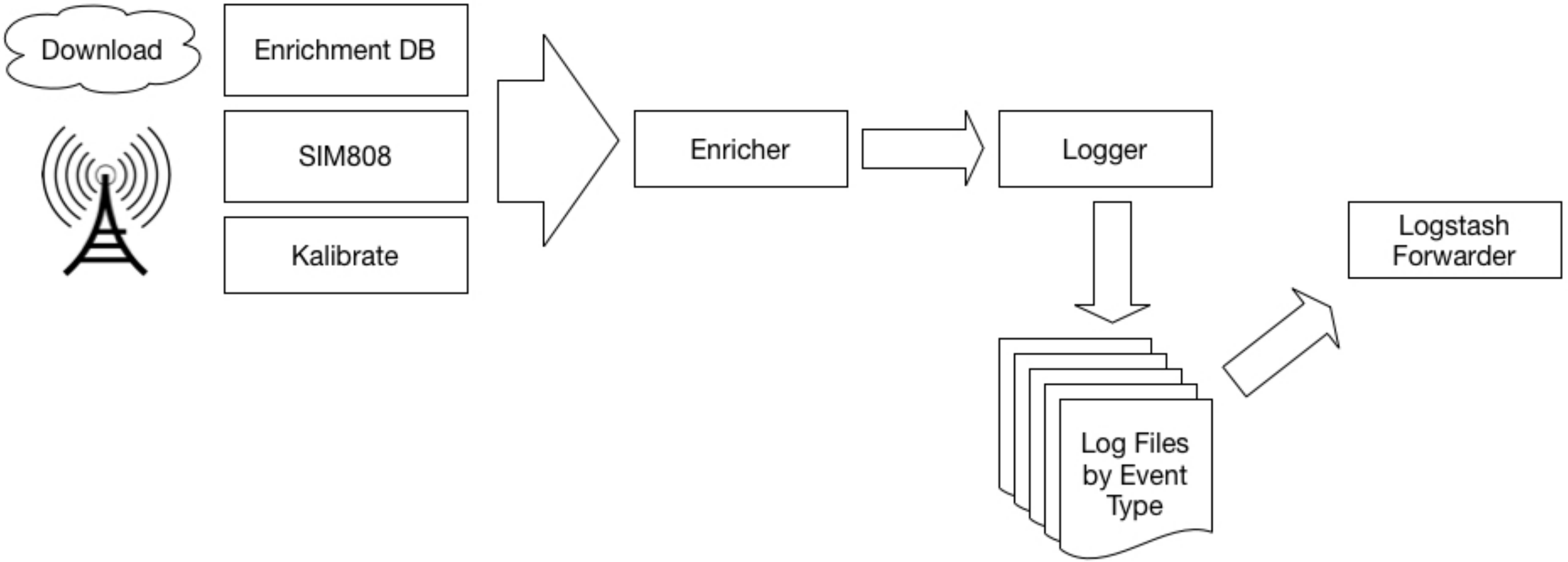


- OpenCellID Database:
  - MCC, MNC, Lat, Lon, Range
- Twilio:
  - MCC, MNC, CarrierName

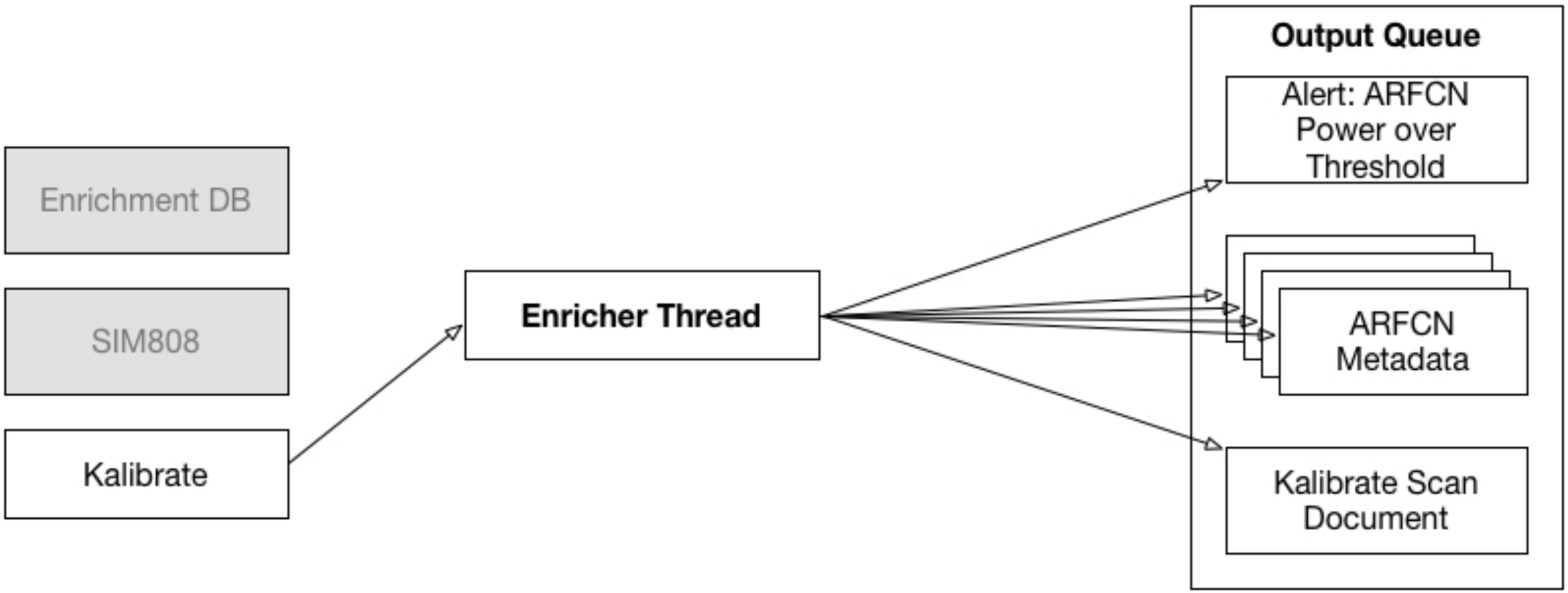
SITCH Sensor MkII



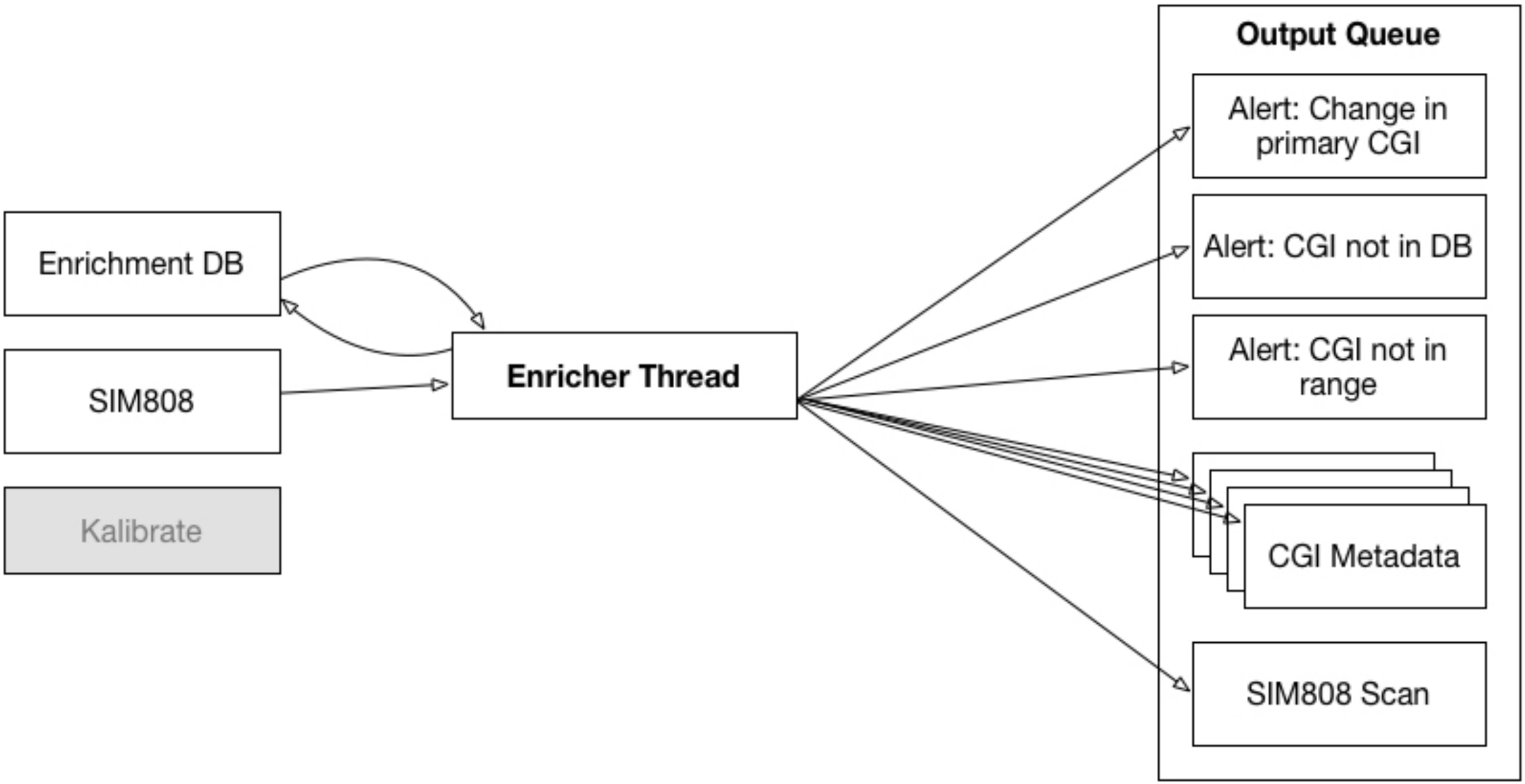
SITCH Sensor MkII



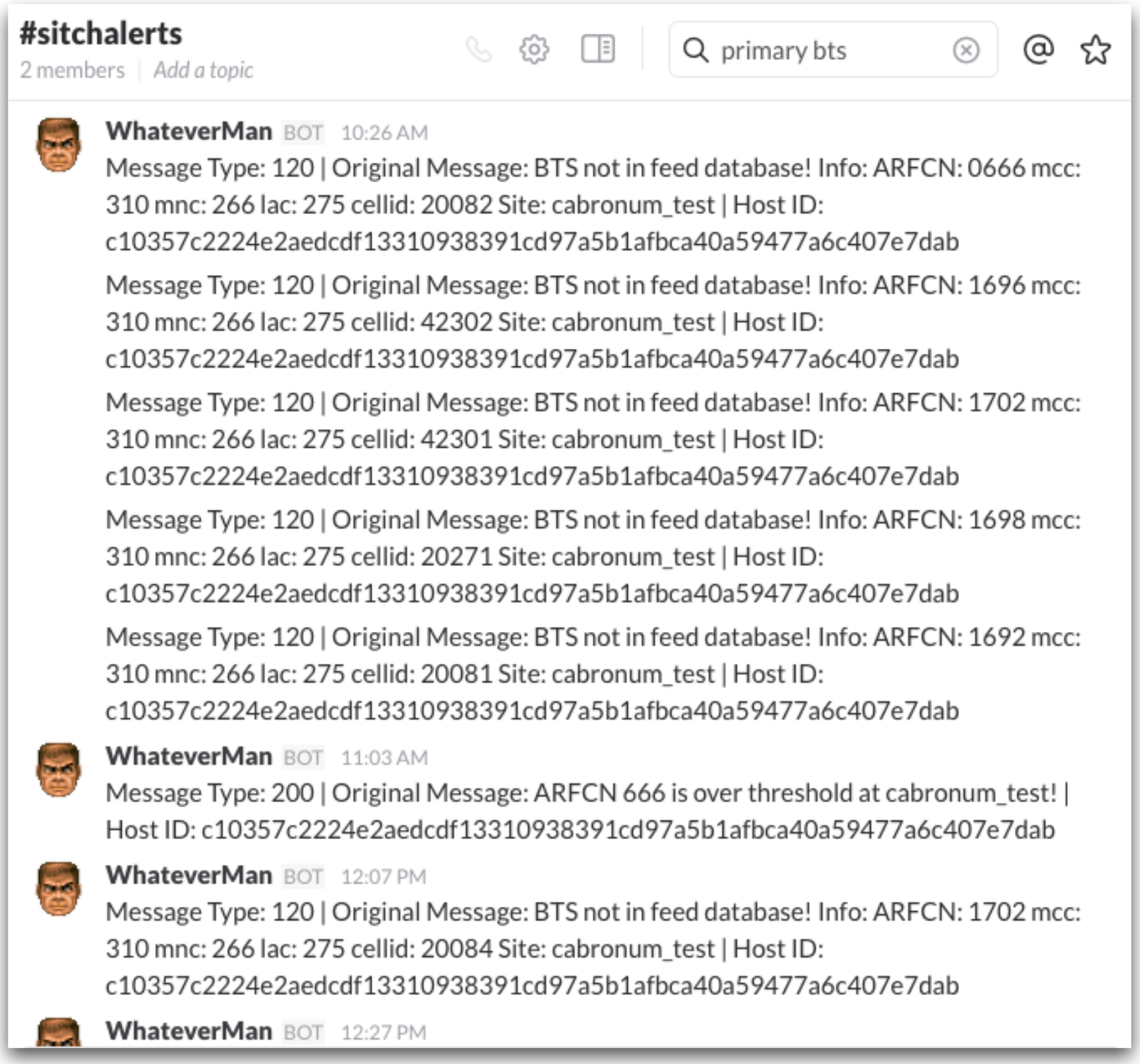
SITCH Sensor MkII



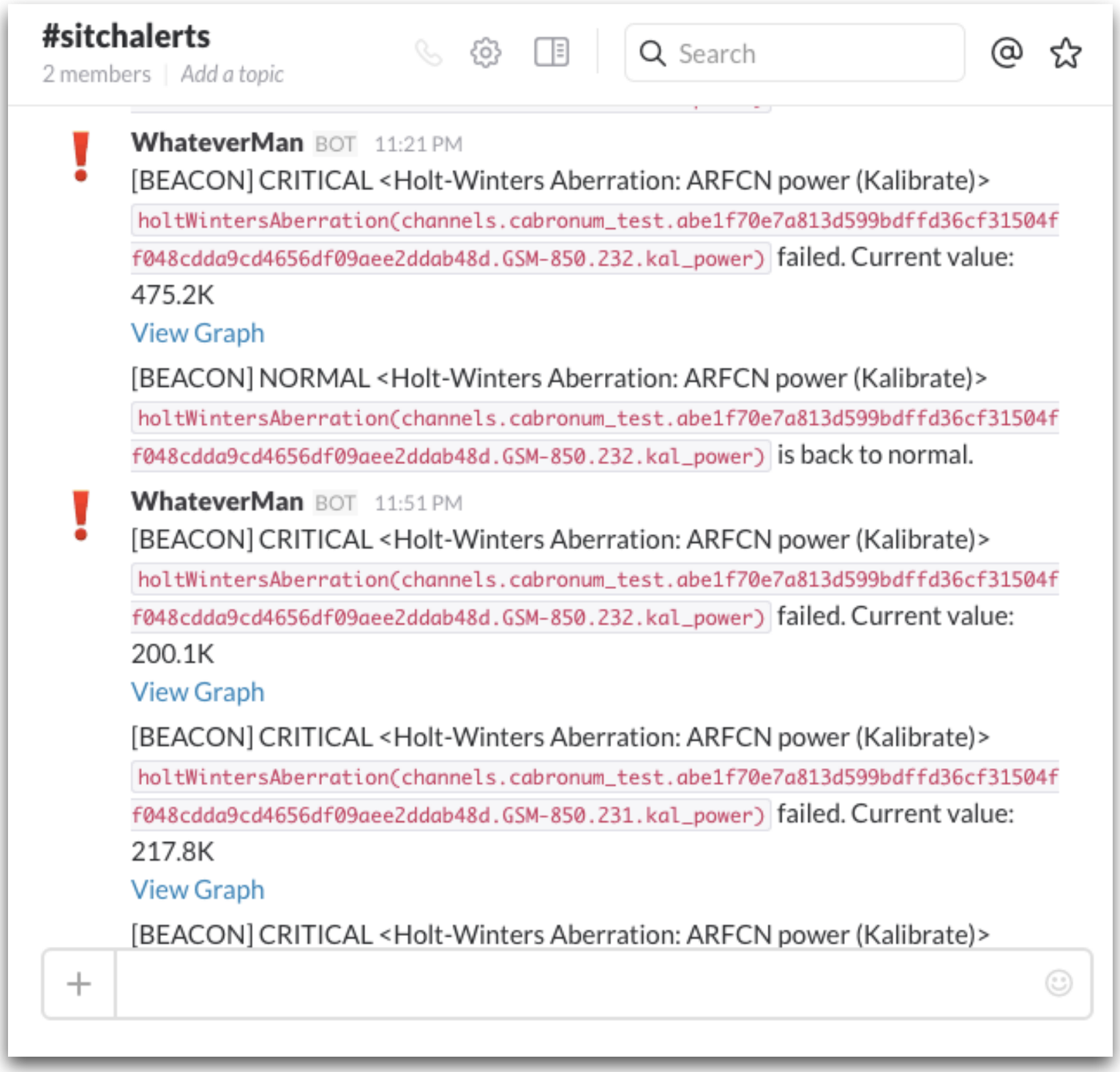
SITCH Sensor MkII



SITCH Sensor MkII



SITCH Sensor MkII



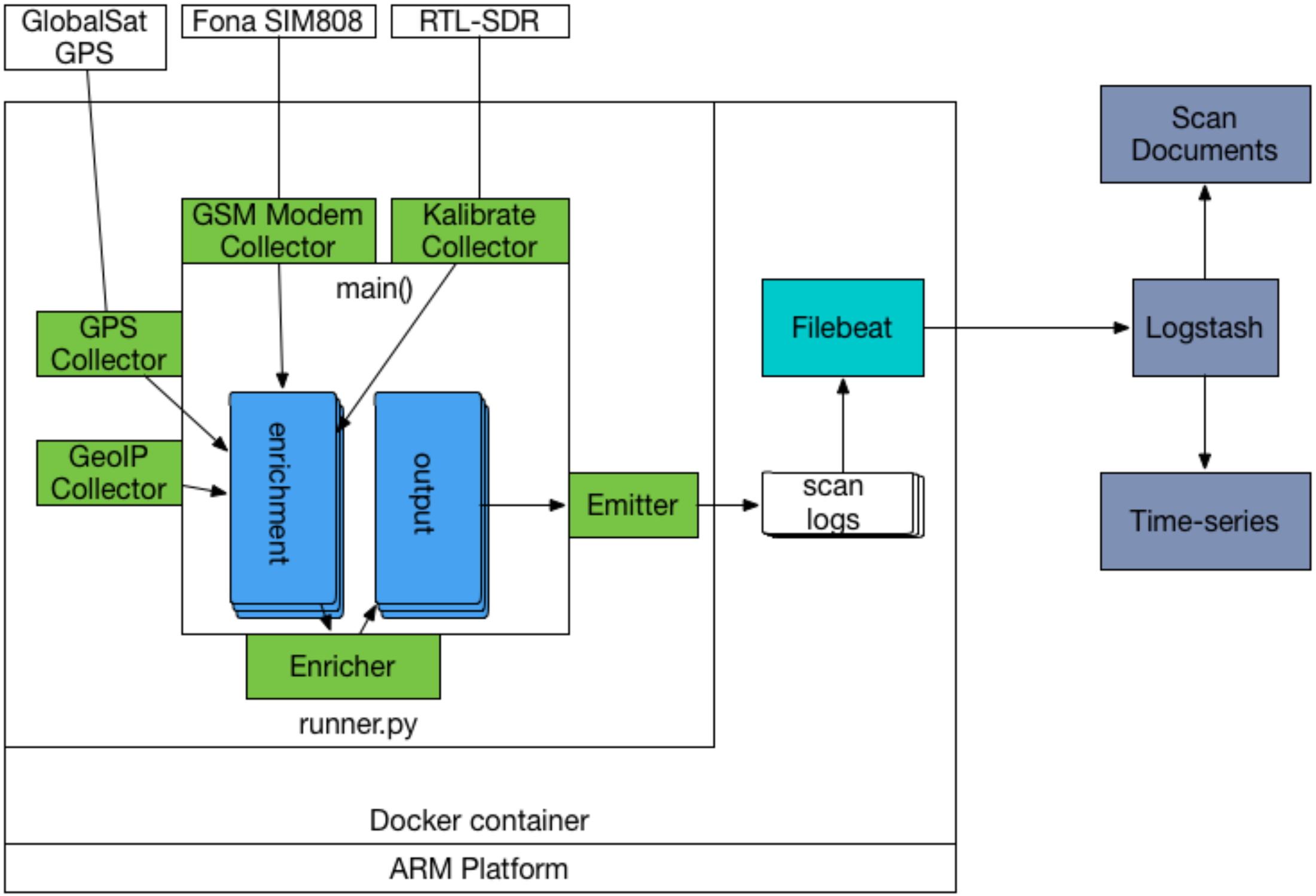
Return to Demo!

- Slack alerts
- Chronograf visuals
- Kibana scan search
- Resin logs

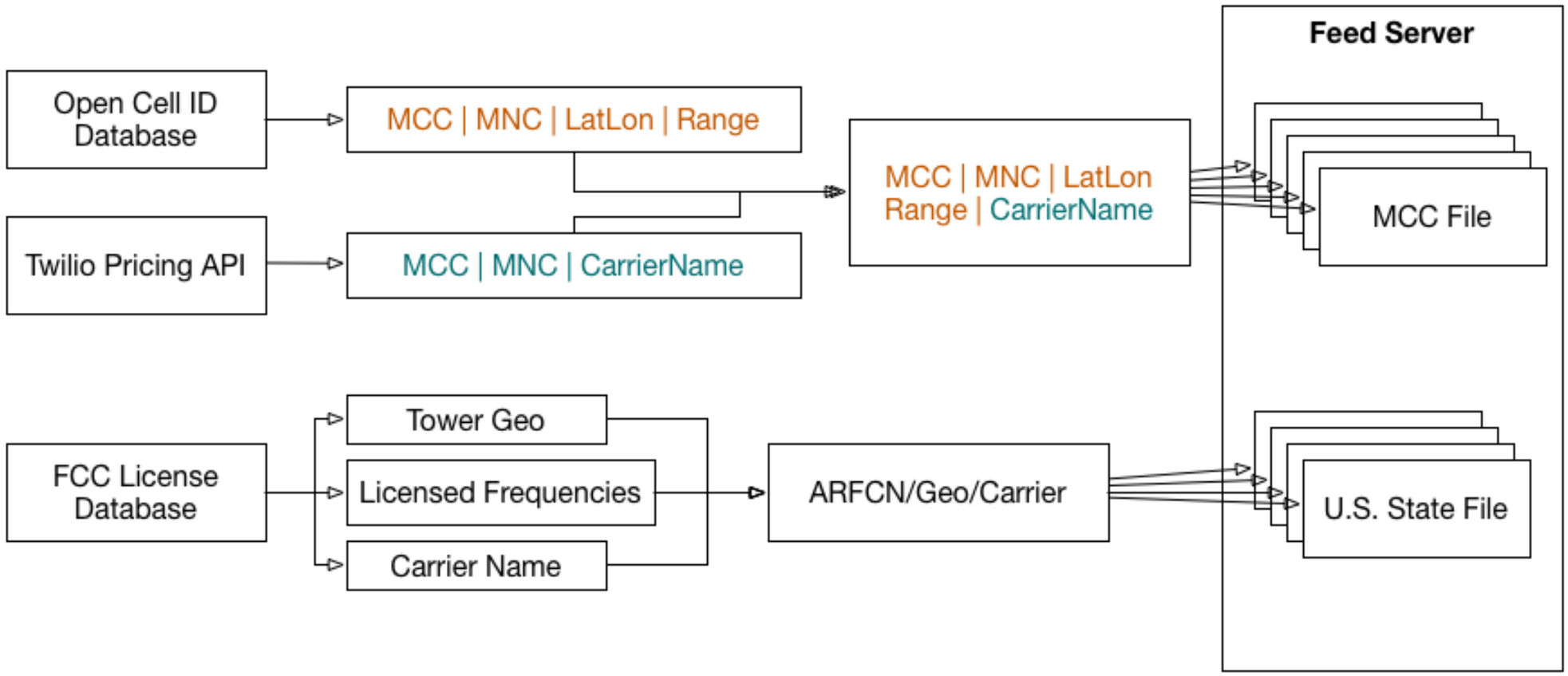
MkI, MkII Summary

Targets	MkI Coverage	MkII Coverage
ARFCN over threshold	YES	YES
ARFCN outside of forecast	YES	YES
Unrecognized CGI	NO	YES
Gratuitous BTS re-association	NO	YES
BTS detected outside of range	NO	YES
Price	~$100	~$150

SITCH Sensor MkIII



SITCH Feed (current)



- OpenCellID Database:
  - MCC, MNC, Lat, Lon, Range
- Twilio:
  - MCC, MNC, CarrierName
- FCC DB:
  - Tower Geo, Licensed frequencies, Carrier name

MkI, MkII, MkIII Summary

Targets	MkI	MkII	MkIII
ARFCN over threshold	YES	YES	YES
ARFCN outside of forecast	YES	YES	YES
Unrecognized CGI	NO	YES	YES
Gratuitous BTS re-association	NO	YES	YES
BTS detected outside of range	NO	YES	YES
Unlicensed ARFCN	NO	NO	YES
Geo drift	NO	NO	YES
Service heartbeats	NO	NO	YES
Price	~$100	~$150	~$180

Also in MkIII

- USB TTY interrogation
  - Detects and assigns GPS, GSM modem
- GSM modem configuration to Elasticsearch
- More verbose device initialization messages

Lessons Learned

- Feeds for CA:USA are around 100MB
  - 1.8MB is California FCC records
- OpenCellID is interesting... but not reliable
- Signal strength is the most reliable indicator
- Refining the funnel

Going Forward

- OpenCellID —> Mozilla Locations Services API
- Gnuradio = pure SDR
- Geofencing LAI

Prior Art

- DIY Cellular IDS (Davidoff, Fretheim, Harrison, & Price, Defcon 21)
- Traffic Interception and Remote Mobile Phone Cloning with a Compromised Femtocell (DePerry, Ritter, & Rahimi, Defcon 21)
- Introduction to SDR and the Wireless Village (DaKahuna & Satanklawz, Defcon 23)
- http://fakebts.com - Fake BTS Project (Cabrera, 2014)
- How to Build Your Own Rogue GSM BTS for Fun and Profit (Simone Margaritelli)
- Low-cost GPS Simulator - GPS Spoofing by SDR (Lin Huangm Qing Yang)
- Gnuradio (many)
- Gr-gsm (Krysik, et al.)
- Kalibrate (thre.at)

Q&A

Further Info

- http://sitch.io
- Twitter:
  - @sitch_io
  - @ashmastaflash
- https://github.com/sitch-io

#OMW2 Scan Your GSM