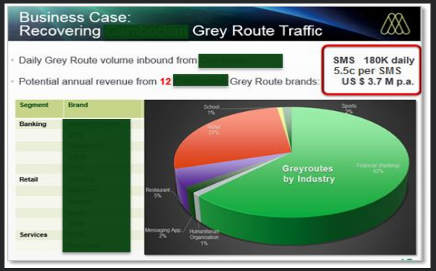
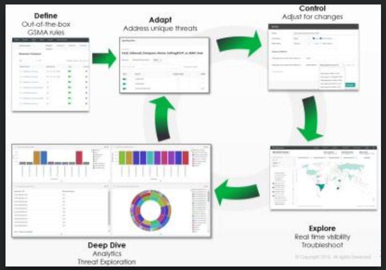
Securing the Network – a way of life!

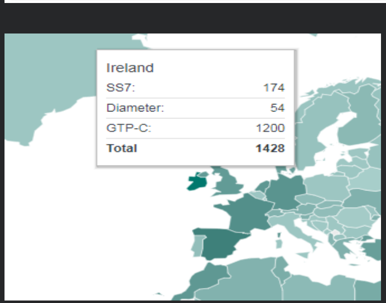


Business Case: Recovering [redacted] Grey Route Traffic

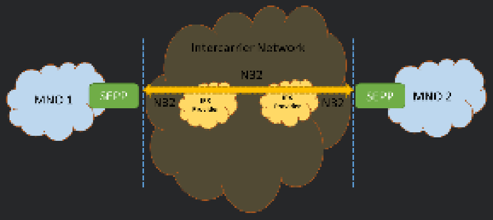
- Daily Grey Route volume inbound from [redacted]
- Potential annual revenue from 12 [redacted] Grey Route brands:

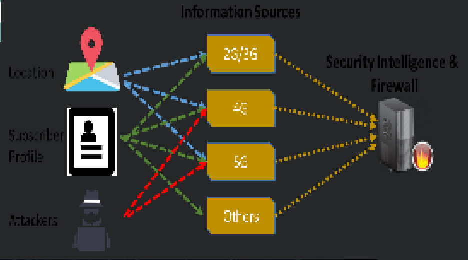
SMS 180K daily
5.5c per SMS
US $ 3.7 M p.a.



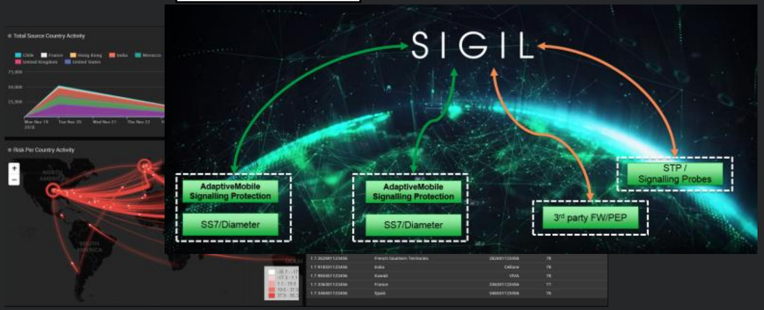


Ireland	
SS7:	174
Diameter:	54
GTP-C:	1200
Total	**1428**





GSMA
SS7 Interconnect Security
GPRS Tunnelling Protocol (GTP) Security
Version 2.0
18 July 2018



SIGIL
Total Source Country Activity
Risk Per Country Activity
AdaptiveMobile Signalling Protection
SS7/Diameter
AdaptiveMobile Signalling Protection
SS7/Diameter
3rd party FW/PEP
STP / Signalling Probes

1. Secure the Interconnect:

- SMS: Home Routing, Greyroute, A2P control, Simbox
- SS7 for 2G/3G : Categories 1/2/3 (FS.11)
- Diameter for 4G/LTE : Categories 1/2/3/LowLayer (FS.19)
- GTP-C across 2G/3G/4G : Categories 1/2/3/LowLayer (FS.20)
- Protocol Correlation (FS.21)
- 5G Roaming

2. Gather and Apply Intelligence

- Pre-empt attacks
- Correlate Cross Protocol for accurate real time decision making
- Learn about the global attacks landscape
- Collaborate in global security intelligence

3. Engage and collaborate in the industry

Get the full picture: Defend, Learn, Adapt, Control!

Increased Attack Sophistication and resourcefulness

- Trojan-Horse attacks to piggy-back onto “normal messages”: **smarten** your firewall

- Attackers can bypass Signalling Firewalls: so **integrate** the firewall correctly!

- Are chameleons in obfuscating their methods and cover their tracks: make sure your firewall **dissects all messages** and act on the patterns of messages

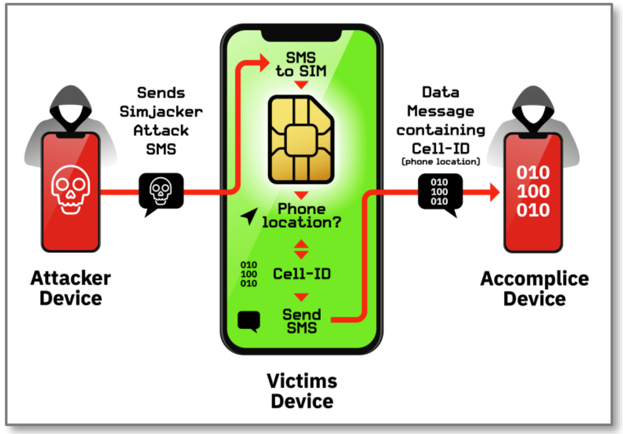
- Adversaries maximise old technologies (SS7) before moving to new (Diameter)

- Coordinated attacks across multiple countries are common place: need global intelligence to defend: IMSI Profiler

- Constantly gather **intelligence**

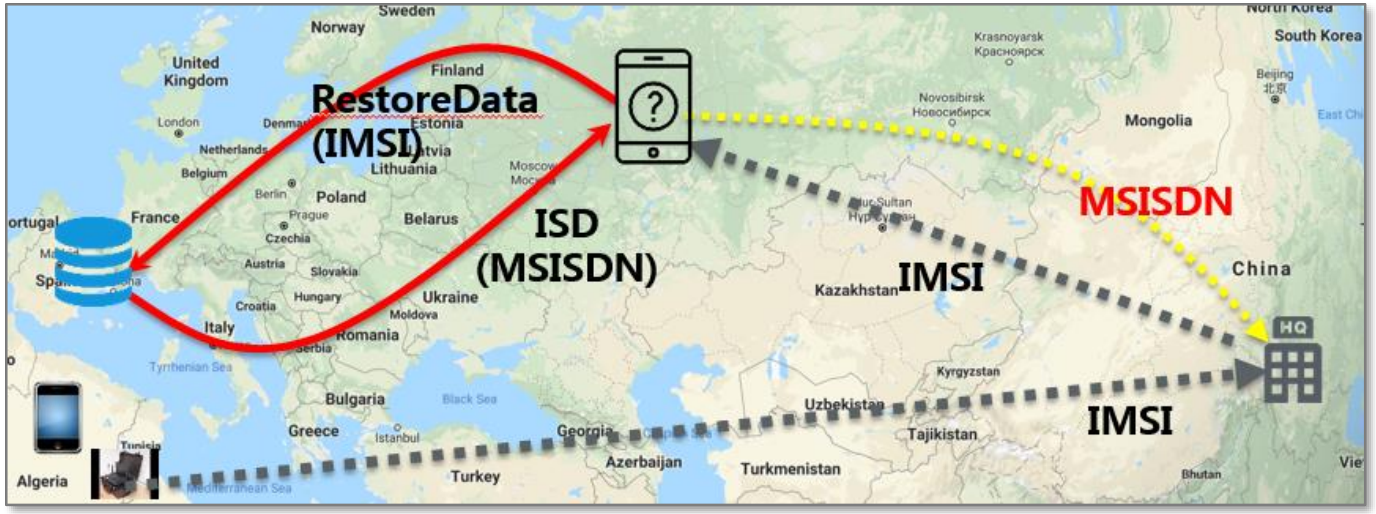
- Nation state attacker: Simjacker ?

- Work with Pentest companies to harden defences and pre-empt real attacks



Simjacker video: https://www.adaptivemobile.com/blog/simjacker-frequently-asked-questions

https://simjacker.com/downloads/technicalpapers/AdaptiveMobile_Security_Simjacker_Technical_Paper.pdf



https://www.adaptivemobile.com/blog/keeping-a-low-profile-detecting-the-presence-of-imsi-catchers-around-the-world

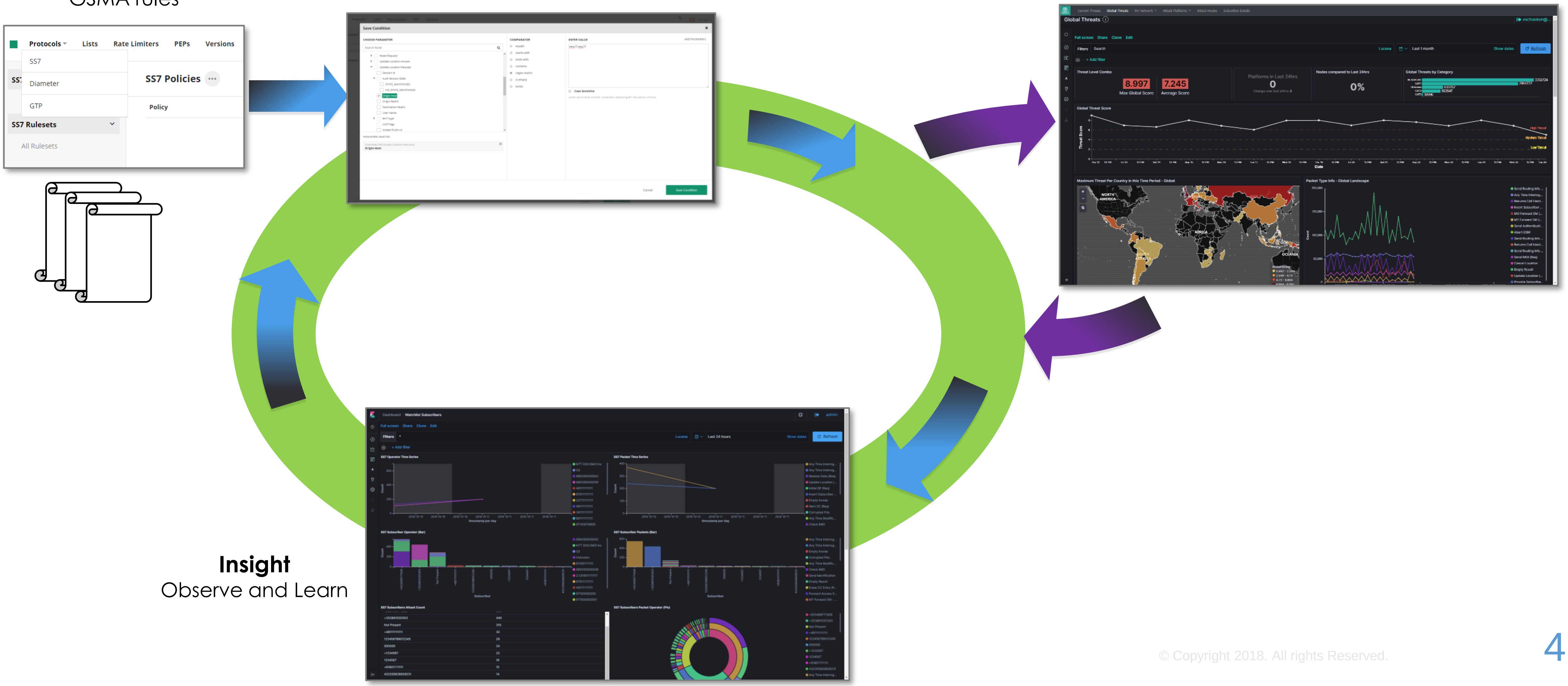
Backup reference

Securing the Network

Baseline
Out-of-the-box
GSMA rules

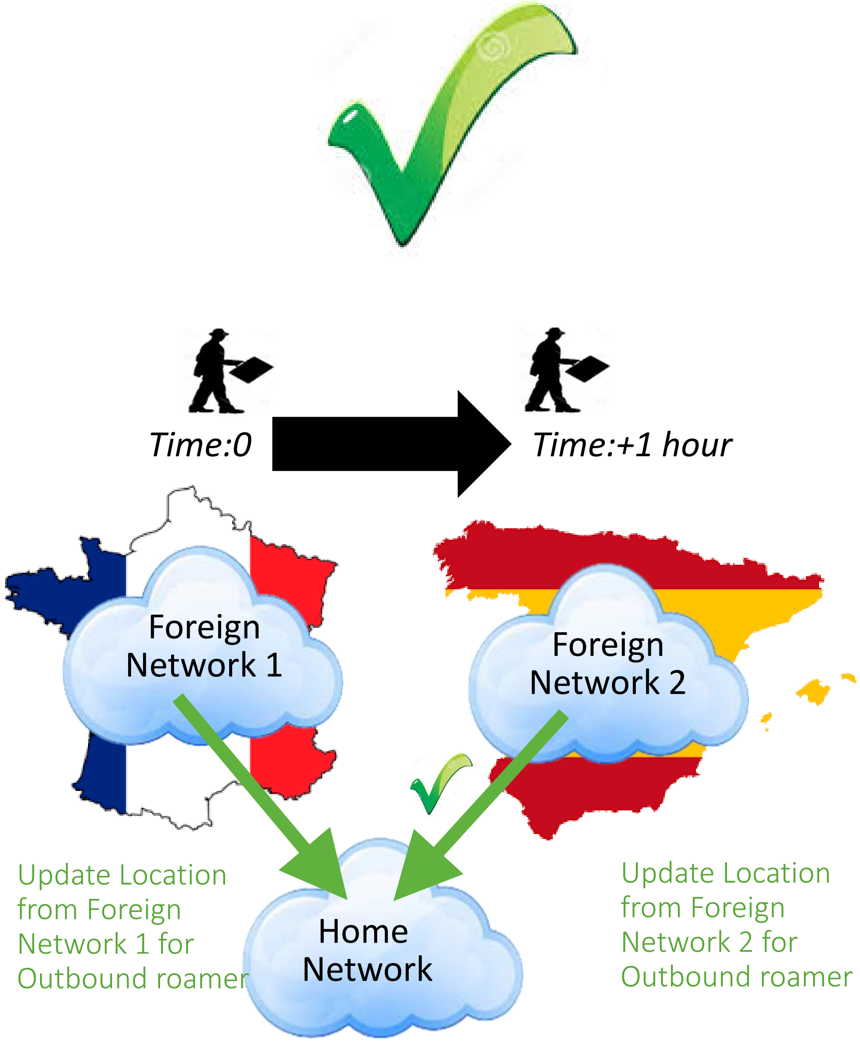
Adapt
Address unique threats

Collaborate
Global Intelligence (ML/AI)



Insight
Observe and Learn

Classic Category 3.2: Trajectory plausibility



Time:0

Time:+1 hour

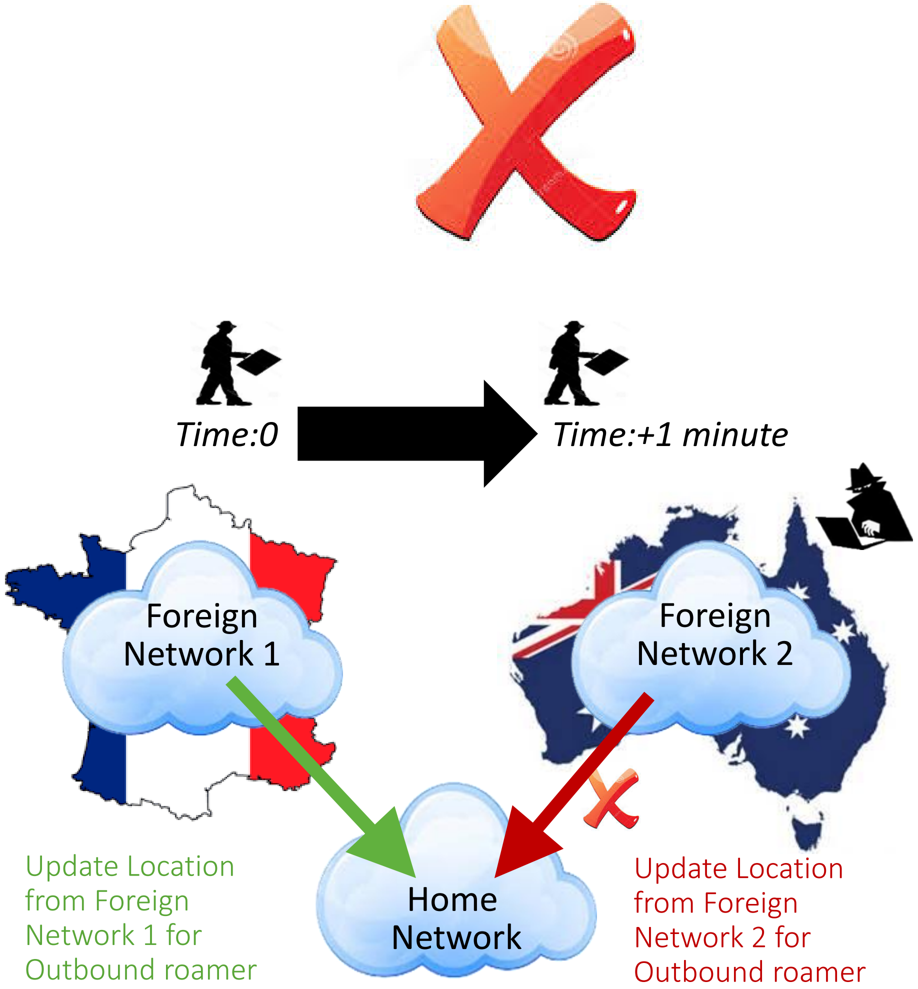
Foreign Network 1

Foreign Network 2

Home Network

Update Location from Foreign Network 1 for Outbound roamer

Update Location from Foreign Network 2 for Outbound roamer



Time:0

Time:+1 minute

Foreign Network 1

Foreign Network 2

Home Network

Update Location from Foreign Network 1 for Outbound roamer

Update Location from Foreign Network 2 for Outbound roamer