ENEA
AdaptiveMobile Security

SERVICE OVERVIEW

AdaptiveMobile SIGIL - Signalling Intelligence Layer

It has been well publicised in recent years that mobile operators' networks have been under attack through exploits in the mobile network signalling system.

These attacks have included subscribers' locations being accurately pin-pointed, eavesdropping on personal phone calls and messages, network & subscriber data being modified, billing avoidance by subscriber impersonation, and user privacy and revenues from key services coming under threat.

Now attacks are migrating from SS7 to exploit Diameter and GTP, where security standards are no better, and have the potential to damage an operator's brand and inhibit 5G take-up.

Many mobile operators have made some changes to infrastructure to deal with threats including network equipment updates and signalling firewall deployments.

However, there are still problems: new rules and detection methods are slow to be applied; there is a lack of signalling security knowledge and personnel; operators struggle to find the 'real' malicious attacks in the overall suspicious activity detected; and attackers, including highly skilled and well-funded nation state actors, are circumventing GSMA and industry implementations. AdaptiveMobile Security has already observed this in real-life, with this trend expected only to increase.

A Global Threat Requires A Global Response: by using the AdaptiveMobile SIGIL - Signalling Intelligence Layer solution, operators can protect themselves by understanding what is really happening, predict future attacks and so defend their network and subscribers from signalling threats.

Typical Applications

- Defence against hostile (criminal/corporate/state) advanced signalling threats on national infrastructure
- Provides a view on who and what exactly is attacking your network
- Additional level of reassurance if using a third party signalling firewall by using AdaptiveMobile's industry leading signalling intelligence
- Comply with national security requirements by doing everything reasonable to identify attacks
- Advanced security preparation for successful 5G rollouts

Operator Benefits

By feeding into SIGIL- a Global Analytics system, and by taking both reports and auto-generated Signalling Intelligence Feeds, operators can:

Understand

- Identify sources of advanced attacks in the 'noise'
- Categorise the Threat Actors attacking their network
- Use the value and expertise of AdaptiveMobile's industry-leading Threat Intelligence team
- Determine if their network is being impersonated elsewhere*
- Know if their firewall misses attacks originating from the home network*
- Discover if subscribers are being targeted by suspicious activity while roaming*

Predict

- Monitor & block, ahead of time, known sources of malicious attacks observed globally
- Detect, in advance, previously unseen types of attacks from known sources of suspicious activity

Defend

- Make decisions on what sources to block and what to allow based on Threat Analysis
- Block sources of previously unrecognised attacks on their network
- Overlay an additional layer of Intelligence on existing signalling defences
- Better protect subscribers in case of determined attackers
- Have knowledge to provide if requested by Regulator/National Security

*Upcoming features - subject to change

Solution Architecture

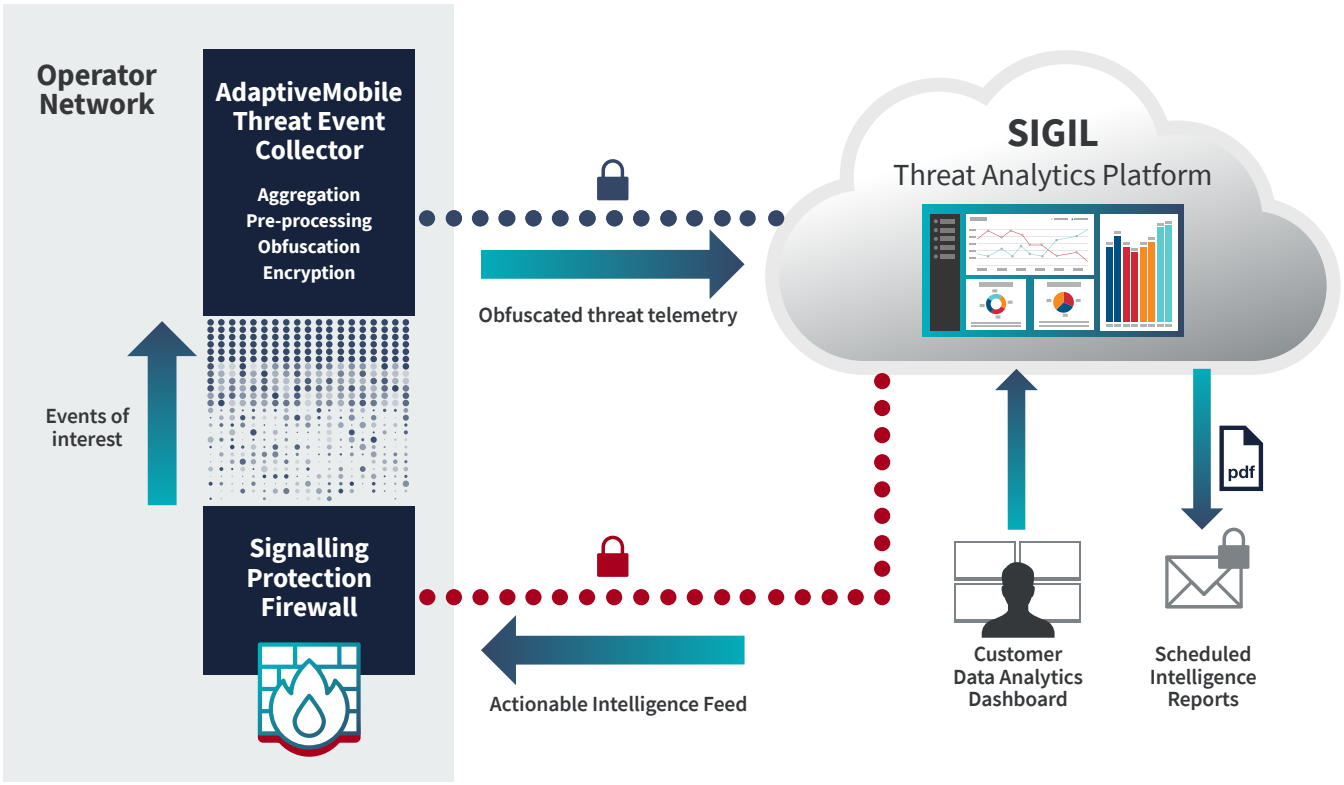


Figure 1: SIGIL Solution Architecture

Functional Components

Signalling Protection Firewall

AdaptiveMobile Signalling Protection.
Blocks suspicious traffic before damage occurs.
Simply overlays onto existing Signal Transfer Point (STP) network infrastructure.
Placed at signalling Interconnect points to secure network against attacks.
3rd party Signalling Firewalls also supported.

AdaptiveMobile Threat Event Collector

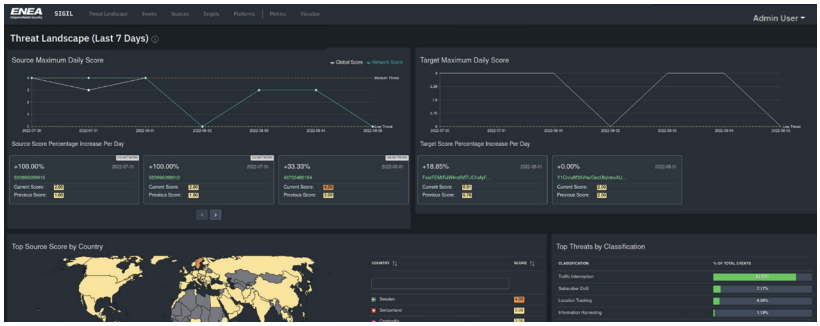
Subscriber Anonymity/Obfuscation within event data

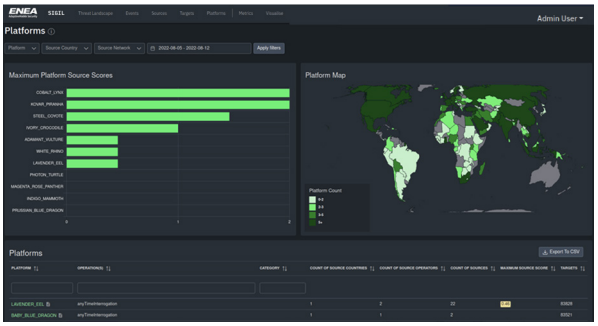
The SIGIL Threat Event Collector consumes messages from the message bus in the reporting module, then modifies the subscriber field to ensure subscriber anonymity prior to forwarding data to the cloud.

SIGIL Threat Analytics Platform

The cloud based SIGIL threat analytics platform consumes messages from all edge devices regardless of operator. Multiple indicators, automated algorithms and machine learning are used to determine problematic GT's. Dashboards, scheduled reports, ad-hoc queries and alerts are tailored per-customer via data restriction, ensuring privacy.

Customer Data Analytics Dashboard





Key Features

SIGIL Automated Analysis

- SIGIL uses a set of proprietary indicators to allocate a Threat Score to each GT/Node that triggers a firewall rule (CAT1/CAT2/3 or blacklist)
- Threat Scores are generated Daily to alert of new bad Nodes and track the threat trend over time.
- Groups of suspect sources we call 'Platforms' are automatically formed according to their behaviour.
- We track Platform and Node activity on a daily and historical basis.
- Gives security analysts the full, continually updated picture of signalling misuse.
- Worldwide view of current signalling threats, reviewed and annotated daily by AdaptiveMobile Security Threat Intelligence Unit (TIU).

SIGIL Environment

- Capable of taking log files from any firewall
- Multi-tenancy, highly scalable
- Secure data transmission to cloud
- All MSISDNs, IMSIs can be optionally encrypted to keep subscribers anonymous
- Series of dashboards providing insight and drilldown to event level.
- Schedule outputs, reports and alerts.

Advantages of SIGIL

The most advanced analysis of Signalling attacks available anywhere

Operators get access to the world's best collection of information on Signalling security and results of industry leading research.

Can use combination of known activity seen around the world and analytic techniques

Dimensioned to investigate detected anomalies (not all traffic) on network.

Companies offering Policy Enforcement Points (PEPs) do not have same breath of analysis – to them a rule is sufficient

Quick deployment if integrated with AdaptiveMobile Signalling Protection

TIU Investigation Services also available to investigate further directly from the system incident of note

NB. AdaptiveMobile Signalling Protection Service available as an additional purchasable service

Can also be deployed in markets where Operators do not use the AdaptiveMobile Signalling Protection solution

Additional integration required for 3rd party signalling firewalls

About Enea AdaptiveMobile Security

Enea AdaptiveMobile Security is a world leader in mobile network security, everyday protecting over 80 Mobile Operators and billions of mobile subscribers and devices globally from fraudsters, criminals and nation states. We have the strongest 5G core network security team, who are designing, planning and building the very best in 5G core network security solutions focussing on threat-intelligence, security heritage and protocol correlation.

Enea AdaptiveMobile Security brings a unique security perspective on real-time mobile network traffic. The global insight provided by our 5G, Signalling and Messaging thought leaders, security specialist teams and Threat Intelligence Unit, combined with our signalling and network protection software that sits at the heart of the network, ensures Enea AdaptiveMobile Security remains at the forefront of the latest advancements in mobile networks and their security, and continues to be the trusted partner of many of the world's largest Mobile Operators.

For more information on how Enea AdaptiveMobile Security can help you protect your communications infrastructure, subscribers and revenues, please contact **sales@adaptivemobile.com**.

Legal Notices

HEAD OFFICE

Ferry House, 48-52 Lower Mount St, Dublin 2.

Contact: sales@adaptivemobile.com

www.adaptivemobile.com

REGIONAL SALES CONTACT NUMBERS

US, Canada, Latin America Sales: +1 972 377 0014

UK Sales: +44 207 049 0421

Middle East Sales: +97144 33 75 83

Africa Sales: +27 87 5502315

Asia Sales: +65 31 58 12 83

European Sales: +353 1 524 9000

REGIONAL OPERATIONAL SUPPORT CONTACT NUMBERS

UK: +44 208 584 0041

Ireland: +353 1 514 3945

India: 000-800-100-7129

US, Canada: +1 877 267 0444

LATAM: +525584211344