

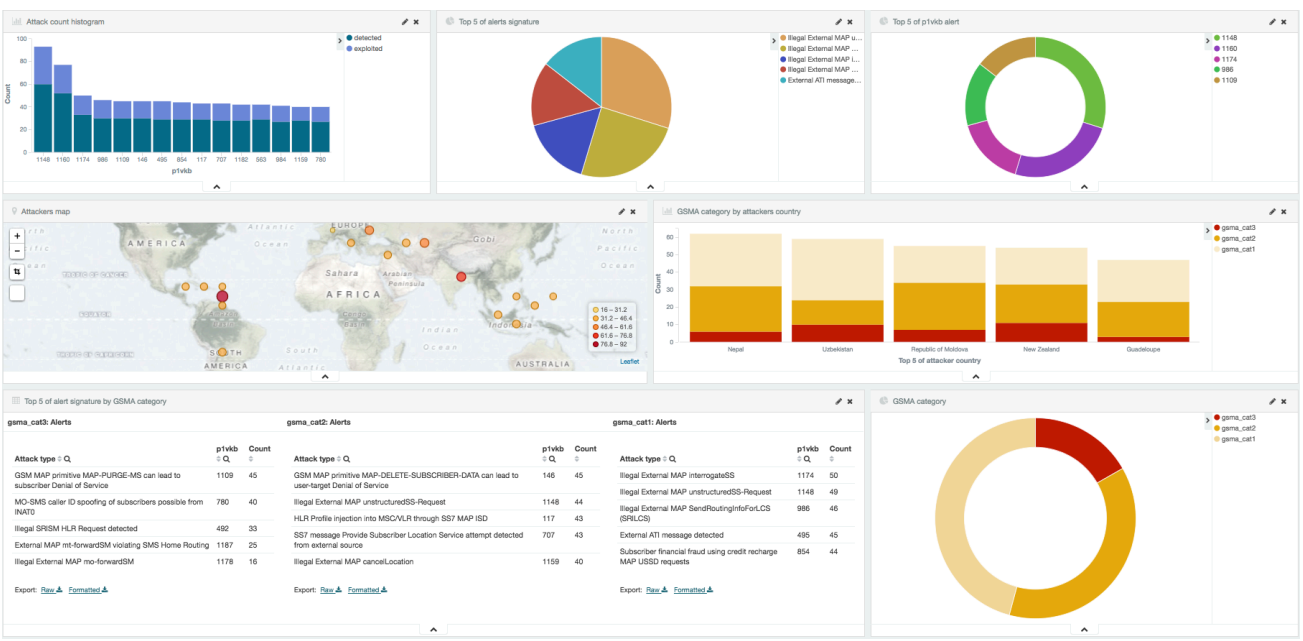
Today, the security situation of **SS7/SIGTRAN, GPRS/GTP-C and LTE/Diameter signaling networks** is identical to the state of TCP/IP networks security in 1994. Few telecom companies have a clear understanding of the vulnerabilities of their signaling networks and the associated risks in terms of Availability, Integrity, Fraud & Privacy. These risks come from new connections being deployed everyday between the Core Networks and the external World, thanks to the Internet and convergent services, 3G, IMS, Femtocells, 4G and 4G Boxes, IoT devices and soon to come 5G. P1 Security offers Mobile Telecom operators, Equipment vendors and Regulators the capability to assess and analyze the security of their Core & Access signaling networks, regardless of their mobile technology, be it GSM, UMTS, CDMA, LTE, WiMAX, UMA or LTE Advanced.

A TELECOM NETWORK SECURITY MONITOR FOR INTERNATIONAL ROAMING

P1 Telecom Monitor (PTM) is an Intrusion Detection System (IDS) specifically designed for Telecom International Roaming signaling traffic.

PTM gives a vision on Telecom signaling networks (in PTM 5.5.1: **SS7 MAP, GTP-C and Diameter**) and reactive monitoring capabilities on signaling issues & attacks. Telecom and Mobile Operators can monitor their International Roaming signaling perimeter the same way they do for their Internet and IP perimeters.

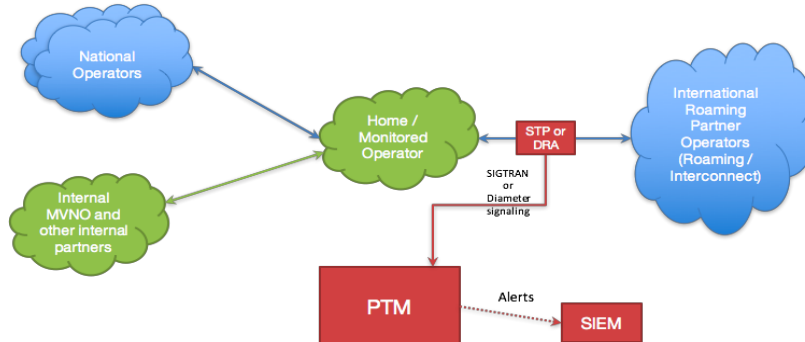
PTM is compliant with GSMA FASG FS.11 “SS7 Interconnect Security Monitoring Guidelines”, FS.19 “Diameter Interconnect Security” and FS.20 “GPRS Tunnelling Protocol (GTP) Security”.



PTM exports generated events in Syslog format and can feed the SIEM system of any SOC.

PTM DEPLOYMENT

PTM is delivered as a **VM instance**. The traffic is monitored on external links, between international roaming partners and the operator's front-end equipment (STP for SS7/SIGTRAN traffic, SGSN/SGW for GTP-C traffic, BGW/DRA for Diameter traffic).



Key Features

- monitoring International roaming
- Telecom protocols
- Attacks & exploits detection (HLR Requests, scanning, illegal incoming messages, spoofing...)
- Dashboard & SIEM integration
- VM deployment

(List subject to changes following ongoing development)

Protocols coverage

- GSM/UMTS (SS7/SIGTRAN)
 - SS7/SCCP & MAP (C, D, E, Gr, Gd)
- LTE (Diameter)
 - S6a, S6d, S7a, S7d, S9, S13, SLg
- GPRS/GRX (GTP-C)
 - Gp, S8
- **Compliant with GSMA FS.11, FS.19 & FS.20**

(List subject to changes following ongoing development)

ABOUT P1 SECURITY

P1 Security has a **recognised leadership** in Telecom and Mobile Security, based on **innovative products & cutting-edge expertise**.

Trainings: TS-201 “Telecom Security hands-on course” (SS7/SIGTRAN & GTP-C), TS-250 “IMS Security & attacking telecom infrastructure”, TS-270 “LTE Security and Insecurity” (Diameter & S1)

VKB (Vulnerability Knowledge Base): unique up-to-date database on Telecom vulnerabilities & threat information

Software solutions: **PTA** telecom vulnerability scanner, to scan Access & Core Networks for SS7/SIGTRAN, GPRS/GTP-C & LTE/Diameter protocols; **PTM** telecom IDS and monitoring system; **PTF** telecom protocols fuzzer, to test the robustness of Network Elements

Vulnerability Assessments: CS Core (SS7/SIGTRAN), PS Core (GPRS/GTP-C), EPC (LTE/Diameter), eUTRAN, IMS Core, IMS Independent Access, VoLTE & VoWifi

P1 Labs: R&D branch of P1 Security, leading the SS7map & SigFW initiatives

*P1 Security is a **Vendor independent**, neutral Company with established references in Europe, Americas, Africa, Middle East, Pacific and Asia.*

P1 Security is an Associate member of the GSMA, since 2015.



Associate
Member

Learn more about P1 Security products & services
Contact us at contact@p1sec.com
Visit us online at www.p1sec.com