WHY CHOOSE PT EXPRESS MONITORING

PT Express Monitoring provides a quick evaluation of the current signaling network protection level. This service helps to discover critical vulnerabilities before they strike and make sure that existing security measures are getting the job done.

Quick
In one month you receive full visibility of your current signaling network protection level

Effective
List of confirmed attack vectors and mitigation advice make you ready for immediate response

Proactive
Perfect kick-off to build mature signaling protection strategy and get ahead of hacker attacks

Know your risks, protect your profits
Start with PT Express Monitoring and grow gradually. With all information at hand about existing threats and relevant vulnerabilities, decide which challenges to address first.
Signaling networks unite mobile network operators (MNOs) around the world and link individuals, businesses, and smart IoT devices into a solid mobile ecosystem. This ecosystem depends on service providers to maintain reliable and protected communication.

However, fundamental flaws in signaling protocols (SS7, Diameter, GTP) and configuration errors in network equipment leave the door open to severe security threats:

- **Network Denial of Service (DoS)**
- **Privacy violation**: call, SMS, and data interception, subscriber location tracking
- **Signaling fraud**

What’s more, the convergence of multiple generations of technology—such as 3G, 4G, and potentially even 5G—brings new vulnerabilities and multiprotocol attack vectors.
Expert security analytics carried out by Positive Technologies show that:

- **ALL** LTE networks are vulnerable to denial of service attacks.
- **4,000+** attacks hit a mobile network operator on average per day.
- **75%** of mobile networks put subscribers at risk of geotracking.
- **67%** of networks fail to prevent bypass of SS7 protections.
- **53%** of call tapping attempts on 3G networks succeed.
- **9 OUT OF 10** of SMS messages can be intercepted.

Diameter vulnerabilities exposure report, 2018
SS7 vulnerabilities and attack exposure report, 2018
PT Express Monitoring draws on the unique expertise of Positive Technologies security researchers and best practices in implementation of GSMA recommendations (FS.11, FS.19, and IR.82). PT Express Monitoring is a first step to building an effective vulnerability management process for MNO signaling networks (Figure 1), as well as protecting your core network, assets, and subscribers from cyberattacks.

Detect. Non-stop real-time threat detection is essential for verifying the effectiveness of network security and supporting rapid detection and mitigation.

Respond. Completely secure your network by addressing both generic vulnerabilities (GSMA) and the threats that actually affect you as part of an ongoing process.

Audit. Auditing provides essential visibility to fully understand your ever-changing network risks.

Figure 1. Vulnerability management process
PT Express Monitoring consists of two parts performed in tandem:

**Passive monitoring** of the signaling network, with threat detection and response by PT Telecom Attack Discovery (PT TAD)

**Active scanning** of the signaling network perimeter from the international signaling network (SS7, Diameter, GTP), with PT Telecom Vulnerability Scanner (PT TVS) (if required and no attack attempts occurred during the test period)

**GOALS**

- Obtain an unbiased independent evaluation of the current protection level of the core network (SS7, Diameter, GTP) from external attacks
- Get remediation advice and roadmap to build an effective signaling security strategy
- Verify compliance with GSMA recommendations (FS.11, FS.19, and IR.82)
INSTANT BENEFITS
WITHOUT DISRUPTION

Be aware of attacks on the core network
PT Express Monitoring passively detects attacks already present on your core network. See the attackers, victims, attack categories, potential impact, and other parameters. Get the answer to the questions on the mind of every telecom operator: Are you under attack right now? How often are attacks attempted? And how many of them are you protected against?

Stay compliant
Strengthen your cybersecurity capabilities. PT Express Monitoring empowers operators to take proactive measures and fix signaling vulnerabilities before they attract the attention of regulators. Assess your compliance level and follow GSMA, GDPR, and other authorities' recommendations to meet regulatory standards.

Maintain network availability
DoS attacks strike telecom operators harder than any other sector. Denial of service degrades network capacity, disrupts customer services, pushes subscribers to find alternative providers, and leads to costly fines. Our research shows that attempts to cause disruption have very high success rates. Reduce exposure to DoS attacks by discovering exploitable flaws and enabling effective response.

Protect subscribers and core network
PT Express Monitoring helps to quickly assess the current security level of your signaling network, with the ability to identify possible attack vectors against the core network and subscribers. Such attacks can lead to call and SMS interception, subscriber location tracking, signaling fraud, and degradation or even disruption of services.
INSTANT BENEFITS
WITHOUT DISRUPTION

Stop privacy violations
Secure customer trust and strengthen ongoing engagement by protecting personal data from existing and emerging threats. Manage critical signaling vulnerabilities and get ahead of hackers. Prevent malicious attempts to track subscribers’ location, intercept private communications, redirect traffic, or access email and social network accounts.

Reduce fraud risks
Flaws in signaling networks allow fraudsters to bypass billing systems, transfer money using forged USSD requests, steal funds with mobile banking, and hack digital wallets. In each case, revenue is lost and reputation jeopardized. Safeguard your business by detecting critical vulnerabilities before they cause financial losses.

Become a trusted IoT ecosystem
Attacks will proliferate as the threat surface widens to encompass connected homes, vehicles, and other smart devices in the Internet of Things. As the role of the IoT grows in daily life and critical infrastructure, corporations and governments will demand greater stability in the telecom networks that connect them. Businesses will choose carriers who take IoT security seriously.

Build effective signaling security strategy
Enhance visibility into signaling network vulnerabilities that threaten your core network, assets and subscribers. By improving your knowledge of signaling infrastructure, threats, and adversaries’ action patterns, you can develop an effective signaling security strategy and reduce incident risks to acceptable levels.
Based on the results of testing with PT Express Monitoring, including any successful attacks detected by PT Telecom Attack Discovery and results of GSMA FS.11, FS.19, and IR.82 compliance checks, the MNO receives an unbiased assessment of the overall protection level of the signaling network.

Management and technical reports also outline:
- Confirmed real-life security incidents during the monitoring period
- Exposure level to potential cyberattacks on signaling networks
- High-level remediation advice and suggestions on signaling security strategy

You also receive independent benchmarking of your current signaling core protection level:

The technical report contains full information about test cases to verify compliance of the MNO’s signaling network with GSMA recommendations (FS.11, FS.19, and IR.82).

You also receive full visibility of real-world security status from PT Telecom Attack Discovery, our signaling threat detection and response solution.
Snapshots from PT Telecom Attack Discovery of illegitimate activity

Figure 4. Attack heat map

Figure 5. Top 10 attack types

Figure 6. Top 10 attack sources

Figure 7. Top 10 source operators
Positive Technologies is a leading global provider of enterprise security solutions for vulnerability and compliance management, incident and threat analysis, and application protection. Commitment to clients and research has earned Positive Technologies a reputation as one of the foremost authorities on Industrial Control System, Banking, Telecom, Web Application, and ERP security, supported by recognition from the analyst community. Learn more about Positive Technologies at ptsecurity.com.

When real-life attacks are detected by PT Express Monitoring, incident investigation starts right away. Results are included with the overall PT Express Monitoring report.

Interested and want a free test drive? Contact us at info@ptsecurity.com to check out PT Express Monitoring, receive an unbiased assessment of your current protection level, get remediation advice, and verify your compliance status.

About Positive Technologies

Positive Technologies is a leading global provider of enterprise security solutions for vulnerability and compliance management, incident and threat analysis, and application protection. Commitment to clients and research has earned Positive Technologies a reputation as one of the foremost authorities on Industrial Control System, Banking, Telecom, Web Application, and ERP security, supported by recognition from the analyst community. Learn more about Positive Technologies at ptsecurity.com.

© 2019 Positive Technologies. Positive Technologies and the Positive Technologies logo are trademarks or registered trademarks of Positive Technologies. All other trademarks mentioned herein are the property of their respective owners.