SecurityGen

Telecom Security. Transcending Generations.

Telecom Security Assessments

Securing networks in an evolving landscape

www.secgen.com

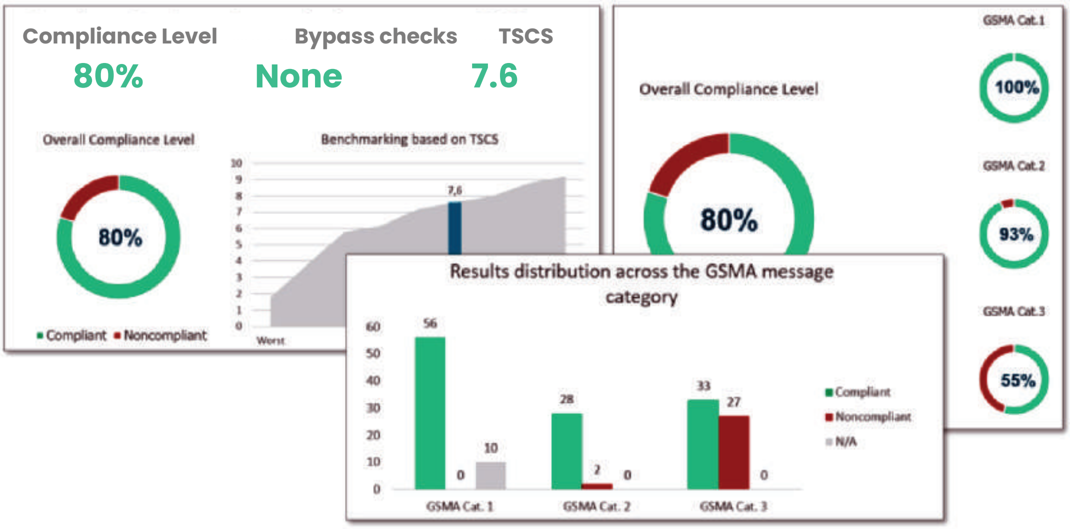
SecurityGen offers a comprehensive range of telecom security services aimed at assessing networks, mitigating potential cyber flaws, and enhancing revenue and subscriber trust. This comprehensive Telecom Security Assessment program has been developed by our expert team with decades of experience and expertise in deploying global telecom security projects. This Program covers testing across the telecom network ecosystem - signalling network, SIP deployments, RAN, SIM cards and VoLTE.Our Telecom Security Assessment (TSA) program provides complete visibility into the actual state of signaling protection across SS7, Diameter, and GTP protocols. These detailed assessments meticulously highlight potential attack vectors on signalling networks and other associated risks.

SecurityGen Telecom Security Assessment (TSA) covers:

1) Signalling Security Assessment

Our Telecom Security Assessment (TSA) program provides complete visibility into the actual state of signalling protection across SS7, Diameter, GTP protocols. These detailed assessments highlight potential attack vectors on signalling networks and other risks.

Knowing which attacks are potentially successful, SecurityGen Telecom Security Assessment (TSA) is the key to building a management process that handles signalling vulnerabilities in a way that keep both networks and subscribers safe.



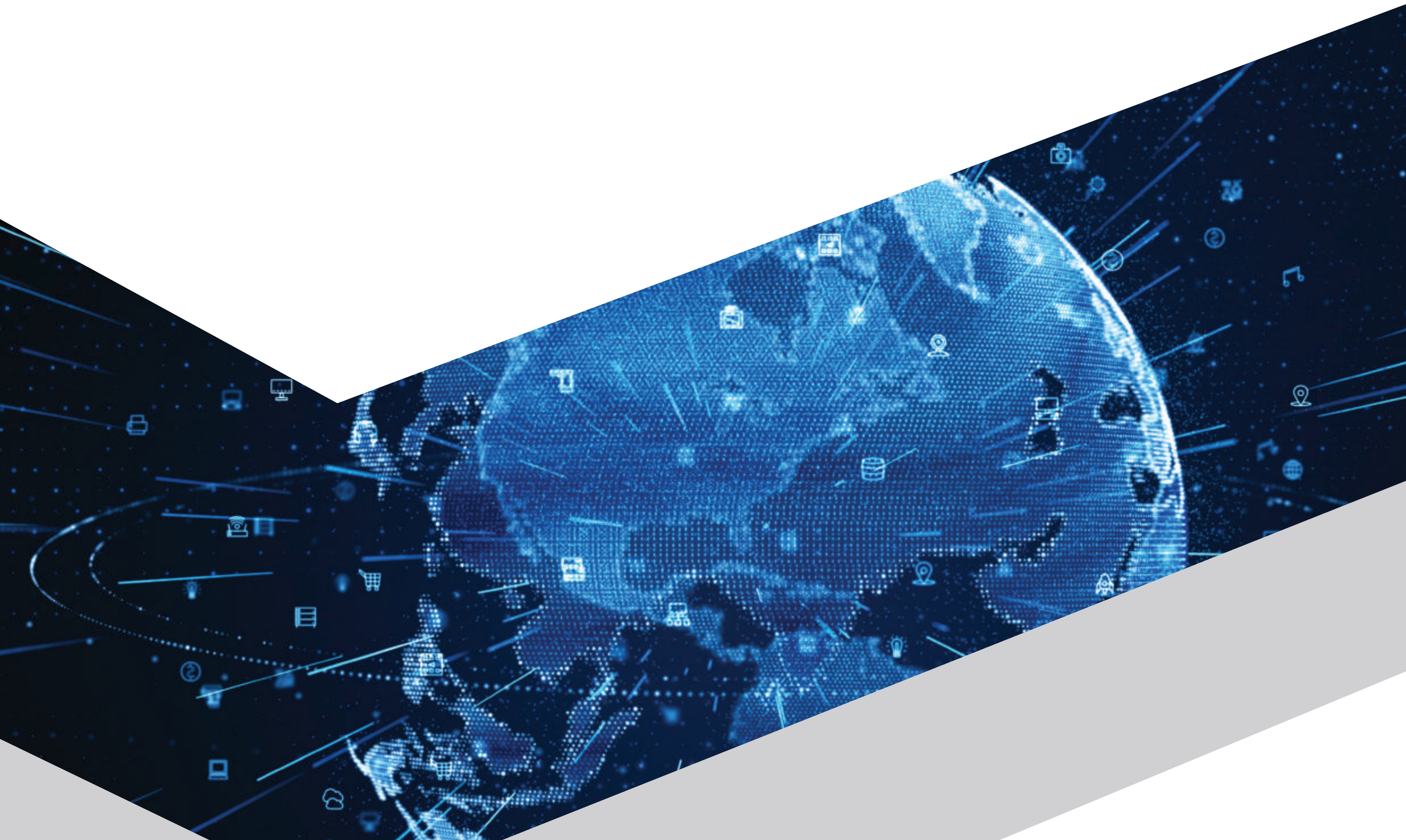
2) VoLTE/VoWiFi Security Assessment

These services use SIM-enabled equipment to access the mobile network but utilize different connection mediums. As with SIP assessments, there has been a substantial amount of investigation into VoLTE testing that reflects all details and threats highlighted in GSMA FS.22, GSMA FS.38 other relevant documentation for access using SIM-enabled SIP devices. This assessment requires onsite presence of our specialists.

3) RAN Security Assessment (onsite)

Adversaries can exploit the Radio Access Network (RAN) that connects subscriber mobile devices with the core wireline network through attack vectors that can interact, capture, replay and inject signals. These attacks may range from eavesdropping on conversations between mobile devices and Base Stations (BS); cloning of mobile subscribers to use network resources without paying, creating fake BSs, enticing users to camp at these phony BSs, to 'denial of service' attacks on the RAN and social engineering against subscribers.

To ensure that security controls are in place against such attacks and to evaluate their effectiveness, Communication Service Providers (CSPs) execute a range of test cases on the end customer's RAN from two designated sites identified and approved by the end customer.The goal of these tests is to evaluate the end customer's network resistance to passive listening, cloning of mobile phones, cloning subscribers, fake BSs and subscriber DOS conditions.



4) SIM Card Security Assessment

SIM card security assessments cover a set of services that help detect potential vulnerabilities related to the installed SIM card. This assessment helps detect whether the customer's signalling network transmits illegitimate signalling messages that allow hackers to deliver a binary SIM. It also helps evaluate if the customer's SIM cards contain potentially dangerous applications which can compromise data integrity and security.

Our remote testing has 3 standard stages:

Offline SIM card testing: The physical SIM cards are tested in the SecurityGen Lab in order to check if it is possible to compromise software and files on the SIM card file system.

MT STK SMS: Mobile Terminated SIM Toolkit messages are transported from a service centre to an MS. These may be input to the service centre by other mobile users (via a mobile originated short message) or by various other sources, such as speech, telex, or facsimile.

MO STK SMS: Mobile Originated SIM Toolkit messages are transported from an MS to a service centre. These may be destined for other mobile users or subscribers on a fixed network.

5) eSIM Security Assessment

There are two main eSIM deployment schemes – a consumer eSIM solution and a M2M eSIM solution. In the case of an eSIM security assessment for consumer eSIMs, the customer provides the web link or QR-code of an eSIM registration. Our experts then try to execute attacks aimed at eSIM confidentiality, integrity, and availability. Interaction with the Customer employees is not required.

During the eSIM Security Assessment, we test vulnerabilities of:

Cryptographic channel

eSIM infrastructure

SIM tool kit

The eSIM Security Assessment empowers MNOs with detailed information on:

- Strength and resistance of the cryptographic channel
- Identification of MNO restrictions on user equipment
- Possibility of remote exploitation of the eSIM STK
- Possibility of illegitimate control of the eSIM platform

About SecurityGen

Founded in 2022, SecurityGen is a global company focused on telecom security. We deliver a solid security foundation to drive secure telecom digital transformations and ensure safe and robust network operations. Our extensive product and service portfolio provides complete protection against existing and advanced telecom security threats.

Connect With Us

✉ Email: **contact@secgen.com**

🌐 Website: **www.secgen.com**

UK | Italy | Czech Republic | Brazil | India | South Korea | Japan | Malaysia | UAE | Egypt | Lebanon