SecurityGen

Telecom Security. Transcending Generations.

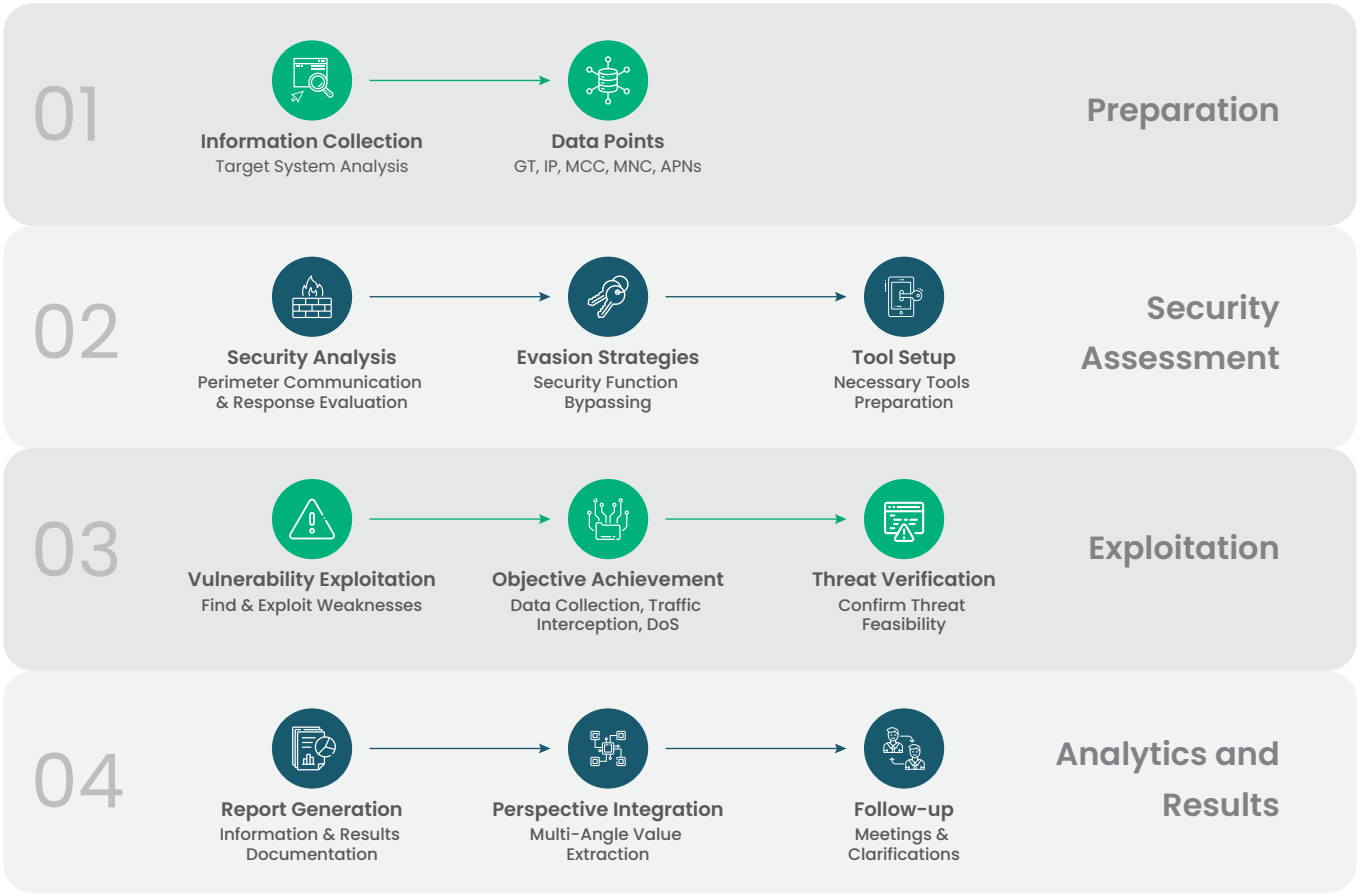
Why Telecom Security Assessmnets (TSA) is crucial?

Telecom Security Assessments (TSA) are crucial for safeguarding networks amid rapid technological advancements and evolving cyber threats. By proactively identifying vulnerabilities and providing actual data for risk management strategies, TSA ensures robust defense systems beyond mere compliance, allowing organizations to adapt dynamically and enhance overall security posture.

SecurityGen offers comprehensive TSA programs, providing visibility through signaling protection and leveraging extensive experience to safeguard global telecom networks, reinforcing the necessity of proactive security measures in modern communication infrastructure.

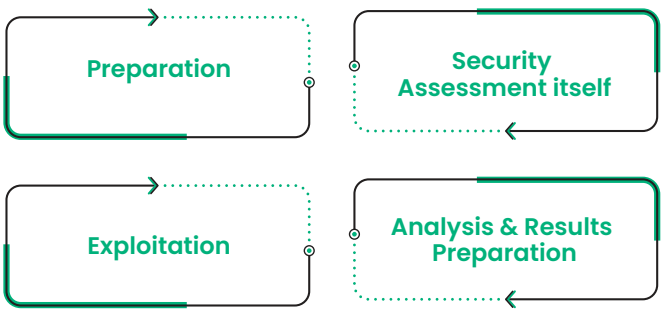
SecurityGen TSA Program covers testing across the telecom network ecosystem - signalling network (SS7, Diameter, GTP), SIP deployments, RAN, SIM, and VoLTE. These detailed assessments meticulously highlight potential attack vectors across entire telecom infrastructure and other associated risks.

SecurityGen TSA methodology



Telecom security assessments are uniquely designed to analyse the security posture of various domains within the mobile network and the ecosystem of services built around it. Our TSA program has been developed by our team – who have decades of experience and expertise in leading global telecom projects and deploying telecom security solutions.

While the methodology employed is not unique and shares similarities with penetration testing in enterprise systems it is focused on telecom infrastructure, the entire project can be divided into four stages:



SecurityGen

Telecom Security. Transcending Generations.

First Stage: Preparation

During this phase, we gather pertinent information about the target system for analysis, encompassing elements such as the **5G core network, RAN, IMS, NFVi, OSS/BSS,** among others. For instance, in core network analysis, we may collect data on **Global Title (GT) ranges, IP ranges, MCC, MNC, and APNs** in use, essential details that could be exploited by adversaries for staging an attack.

Second Stage: Security Assessment Itself

Our auditors, adopting the role of attackers, evaluate network reachability, conduct communication tests with perimeter devices, analyze responses, and verify the presence of security measures **(such as Home-Routing, Signaling Firewalls, IP-based filtering, etc.).** Subsequently, we seek methods to circumvent these security measures and infiltrate the target network, necessitating the deployment of requisite tools and formulation of corresponding bypass techniques.

Third Stage: Exploitation

After breaching the perimeter successfully, we advance to the exploitation stage. Tailored to the audit's objectives, we endeavour to discover and exploit vulnerabilities to attain our aims, whether it **involves gathering sensitive data, intercepting traffic, or inducing denial of service.** This phase, though brief, is the most exciting part of the audit, where we validate and demonstrate the plausibility of these threats.

Fourth Stage: Analysis and Results Preparation

In the final stage, translating collected data and results into a comprehensive report is paramount, providing actionable insights for management and detailed recommendations for engineers to address vulnerabilities. Effective communication with business executives, the network department, and the cybersecurity team is essential, tailoring insights to their perspectives for maximum value.
This process is followed by meetings and clarification calls to support departments in addressing issues, planning adjustments/fine-tunning, implementing security roadmaps and enhancing the cyber-resilience of the mobile network infrastructure, the services and the subscribers.

It's vital to recognize that security is an ongoing process. These activities are inherently recurring in nature to ensure continuous measurement of security posture, timely identification, and remediation of vulnerabilities and weaknesses. While repetitive security assessments are common, automation through various tools for vulnerability management, breach, and attack simulation is increasingly feasible and effective.