SecurityGen

Telecom Security. Transcending Generations.

5G

protection use cases

As an established player in the telecom security domain with over 300+ telecom security assessments undertaken by our core team, we have partnered with leading MNO teams in their 5G transformation journeys, from the blueprint to design to rollout. Below we have explained some of the use cases which are an outcome of 5G cyber-security projects where we accompanied our MNO customers.

www.secgen.com

5G Design and Planning

Use case #1

Customer: LGU + **Mobile users:** 20M

Digital services: Telecommunication services, high-speed internet, VoIP, IPTV, 5G and IoT

The customer was building the 5G network and planned to have clarity of the security posture while building the network and not afterwards, to prevent higher investments in case the architecture proves itself insecure later.

SecurityGen team first conducted an offensive security assessment of the 5G SA network, outlining technical vulnerabilities, protocol deficiencies and architectural obstacles, considering that the network did not include all required nodes by that time.

The customer already had the vulnerability management process established in the organization, having a general NIST-like security approach consisting of 5 significant steps: assess, detect, protect, respond and, remediate. The customer specialists understood that the security process and vulnerability verification in 5G SA infrastructure should be continuous. SecurityGen ACE Breach and Attack Simulation solution already covered the LTE network - ACE for SS7, Diameter and GTP. Thus, to further protect the 5G SA the client upgraded the existing ACE module with a new instance.

This security monitoring of 5G SBA now allows both SOC specialists and the network planning department to automatically inspect their 5G core at any stage of the deployment, understand the security posture of the 5G network and use the recommendations to improve the situation. It was an initial step of embedding 5G security into the company-wide vulnerability management cycle. Closer to the 5G network going live, the security cycle will be complemented by detection and protection parts.

1. **Solution used:** ACE Breach and Attack Simulation Platform
2. **Service used:** 5G Telecom Security Assessment

Use case #2

Customer: A leading MNO **Mobile users:** 25M

Digital services: Telecommunication services, high-speed internet, connected cars, cloud storage, 5G and IoT.

The 5G network is in the later stage of readiness. Hence, the customer requested an assessment of the 5G core - to identify whether any specific threats could be verified and proved – as absent or available.

The SecurityGen team noticed that the customer was keen and aware of SS7 and Diameter security, and there were nodes of signalling firewalls in place. For some reason, GTP-C protection was largely missing. Often GTP-C security is underestimated, but this can be perilous as the GTP-C protocol is required for roaming interworking on the N26 interface within 5G.

So as a first step SecurityGen team implemented SecurityGen TSG (Telecom Security Guard) IDS GTP module in the network for the visibility of GTP traffic. As the SOC was actively providing monitoring of different systems and networks, signalling was not an exception, so the following step was a quick and easy integration with the SIEM system on the SOC side. This step initiated security assessments of the GTP and 5G networks. Search and partial exploitation of vulnerabilities in both protocols were highlighted by TSG IDS in place, simultaneously providing visibility of GTP attacks on SIEM dashboards with different responses according to procedures that were developed.

1. **Solution used:** TSG IDS
2. **Service used:** GTP Telecom Security Assessment

During these engagements and several other sessions with the MNO network and security personnel while helping them plan and secure their 5G rollouts , we faced the following questions:

"We have implemented signalling firewalls and traffic filtering for all legacy generations. We are undertaking continuous or at least one-off security analysis for 4G and 5G NSA networks; What should be our next step for better 5G security posture?"

The answer may sound logical if you look at the basic security cycle paradigm:

- Know your crown jewels
- Verify your threats
- Implement sufficient protection
- Continuously monitor security and prepare a remediation plan in the worst case.

Stay tuned to learn more about vulnerabilities, threats and protection of the 5G network.

Below you can browse through our 5G focused offerings

SecurityGen 5G solutions

1. ACE – The inspection module

Our award-winning Artificial Cybersecurity Expert, our industry-first AI-enabled Signalling Breach and Attack Simulation platform (BAS) is the Inspection module purpose-built for securing mobile networks. ACE conducts continuous security assessments to monitor the entire network and expose any flaws or vulnerabilities. Thus, ACE helps validate the strength of your security systems in an automated manner.

- Continuous validation of security systems
- Automated loop to identify, prioritize & remediate threats
- Proactive security posture across legacy protocols (GTP, Diameter and SS7) and 5G.

2. TSG - Telecom Security Guard (Detection and Protection Modules)

- TSG IDS

Our intrusion detection IDS platform provides MNOs with complete, end-to-end visibility of the telecom network in real time.

- TSG NGFW

Our next-generation signalling firewall: the NGFW platform combines comprehensive visibility with intelligence and high-powered analytics to safeguard the network and the extended 5G ecosystem.

3. 5G Telecom Security Assessment

Our 5G Security Program is specially designed to help MNOs reinforce their security strategy and offers comprehensive guidelines for maintaining reliability and resiliency of 5G SA/NSA network and services.

Here is what you get:

- Business impact evaluation of threats
- Clear, actionable recommendations for ongoing 5G security strategy based on comprehensive assessments
- Guidance for immediate remediation of critical weaknesses and vulnerabilities
- Security assurance for a range of service offerings, including wholesale and private networks
- Verification of compliance with industry recommendations and known vulnerabilities where applicable.

About SecurityGen

SecurityGen is a global company focused on cybersecurity for 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 | Egypt
India | South Korea | Japan | Malaysia | UAE