SecurityGen
Telecom Security. Transcending Generations.

SecurityGen's IDS deployment helps a leading MNO significantly enhance the security posture

The Customer

A leading integrated operator offering a wide range of telecommunications and digital services focused on the best customer experience.

The Business Scenario and Challenge

This MNO deployed an IPS with filter and blocking rules on border elements and traditional rules. However, even after a year of deployment, not all the IPS rules were efficient enough. How to boost the existing security plan - With the evolving threat landscape, continuous network monitoring through a signalling IDS was critical to ensure protection against the call, message interception, and subscriber data breaches. As a leader and a firm believer in secure and resilient telco transformations, the MNO team was keen on establishing security as an enabler to support and ensure their business transition. The critical elements of their 5G security framework:

- Security readiness for 5G
- Steady improvement in the security posture of critical assets, the interval between security assessments to be secured by monitoring
- Adoption of automation and analytics, integration to SOC
- Development of security framework and benchmarking
- Adherence to increased compliance

The Solution

Given the digital environment's rapidly changing ecosystem, the MNO chose **SecurityGen IDS (Intrusion Detection System)** to monitor the perimeter constantly and thus help improve and align security posture at this fast pace. IDS deployment helped the MNO strengthen their security posture with comprehensive security monitoring, anomalous activity detection, and reporting across the signalling network perimeter. SecurityGen IDS deployment enabled the SOC team:

- Continual monitoring, a repository of compliance reports from any given period, evidence of actions and security level, and protection against advanced attacks.
- Monitor threats, prioritize actions and immediately verify results and impacts.
- Using actionable data collected from the IDS, the SOC team can correct STP/DEA configuration or update Firewall rules to address and thwart threats emerging from new techniques or changes on the signalling service chain.

Key metrics

- From thousands of messaging billing evasion fraud events per month reduced to **Zero**.
- Overall attempts of high severity attacks volume reduced to **50%**.