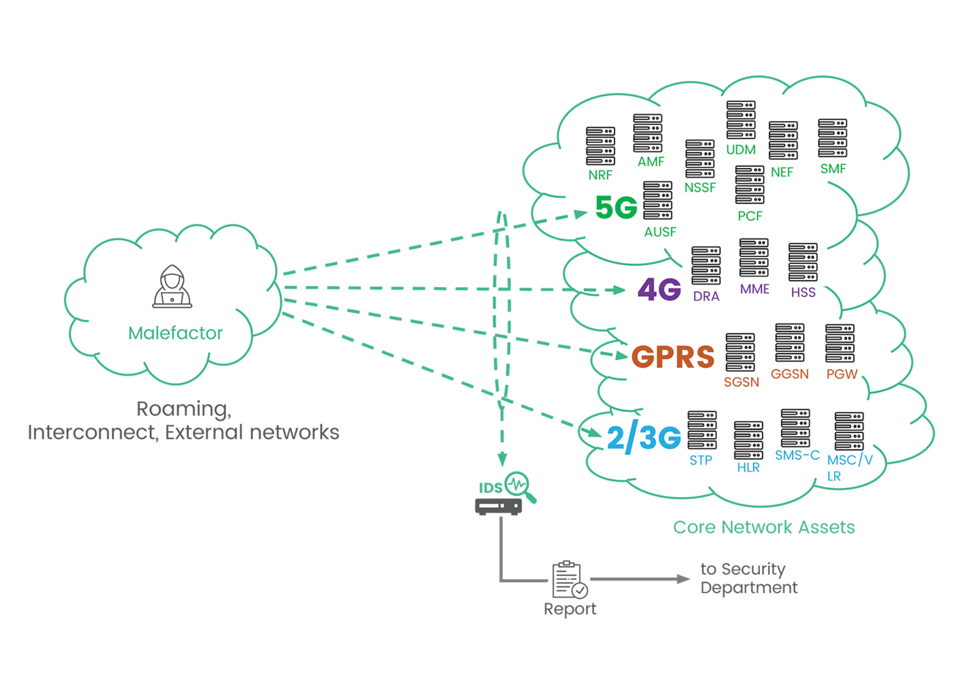
SecurityGen
Telecom Security. Transcending Generations.

IDS: INTRUSION DETECTION SYSTEM PLATFORM

SecurityGen's Intrusion Detection System (IDS) enables telecom operators to promptly address emerging threats by providing comprehensive coverage. It encompasses a wide range of security monitoring features and real-time detection of unusual activities, safeguarding the integrity of signaling networks across various protocols such as HTTP/2, Diameter, GTP-C, and SS7. With its advanced analytics and reporting functionalities, the IDS platform ensures proactive security measures, thwarting hacker attacks and fortifying the core network's protection. Furthermore, it enhances the operators' reputation among subscribers, establishing a sense of trust and goodwill.

How It Works?

- Enhanced visibility for early threat detection
- Advanced analytics for rapid incident response
- Supported by a robust Knowledge Base of over 2000 signatures for all mobile network generation from 2/3G to 5G



SecurityGen IDS Edge

- **Element Profiling**
  SecurityGen IDS collects detailed statistics across each node on the type of messages used and the number of times used during a specified period. This information enables looking for any node and identifying what kind of messages the node was executed during that period. Further, TSG checks the reliability of each traffic source with every message. Each node in the roaming network has its role. SecurityGen IDS platform provides a comprehensive analysis of the traffic - based on what is allowed for a specific role and what is not. And in the event of any inconsistency, places that specific node into an unreliable list. Thus, while observing the possible attacks/events in the IDS interface, the MNO team can analyse the suspicious marks on the source – which helps them validate the decision for blacklisting/creating a new FW rule.

- **Correlation-Based Mechanism**
  SecurityGen IDS solution works on the principle of correlation mechanism whereby it does not just process unitary messages one by one (the way firewall usually does) but addresses the signalling flow in entirety – across transactions, correlating different events. This broader security perspective helps highlights the attacks that already took place and can be prevented in further activity.

- **Cross-Protocol Attack Detection**
  SecurityGen IDS stores and correlates different subscriber information; keeping and detecting the location data (Country, Operator, Node) is part of the functionality. This data is successfully used to check if specific messages (GSMA Cat.3) are coming from plausible locations or if it is technically possible for the subscriber to move from one country to another.

  This technique helps detect cross-protocol attack/s even with the location data missing for a few protocols.

  Our IDS UI allows observing all the attack data on the same subscribers spread over all protocols on one screen, thus making the malefactor's behaviour analysis much easier in a cross-protocol approach.

Get Ahead Of Cyberattacks

SecurityGen IDS ensures identification of all forms of malicious activity, including:

Network Equipment Denial of Service	Denial of 5G services	Denial of service Subscriber/IoT/ Industrial IoT	Fake network function implementation
Subscriber data interception: SMS, data, voice calls	Fraud cases: grey routes, billing bypass, USSD manipulation, SIM card vulnerabilities, etc.	Network and Subscriber information disclosure	Subscriber location tracking

Talk to us to know more on SecurityGen IDS: contact@secgen.com