SecurityGen

Telecom Security Transcending Generations.

IDS: INTRUSION DETECTION SYSTEM PLATFORM

Solution Overview Datasheet

www.secgen.com

In a digital world driven by critical infrastructure and sensitive data, telcos run the clear and present risk of being caught in the crosshairs of cyberattacks.

Extensive research carried out by our teams has revealed that all legacy networks --2G, 3G, 4G-LTE – and even 5G are easily exploitable, given that flaws in signaling protocols—SS7 and Diameter — can allow an attacker to compromise subscriber privacy, intercept calls, track subscriber locations, carry out fraud, and cause a denial of service. More shocking still is the fact that such tools are no longer preserve of just nation-state intelligence services, but available to even low-skilled hackers.

The stakes have never been higher, and MNOs' basic rule-based firewalls can't claim to be a deterrent to advanced and sophisticated threats. Watertight security now calls for constant vigil and visibility, and a proactive approach to checking for, and attending to, alerts.

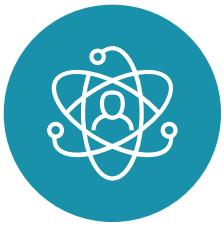
Reinforce Cybersecurity Posture

With the combined power of a best-in-class signaling intrusion detection system and business intelligence (BI) module, SecurityGen IDS offers a comprehensive yet easy approach for security monitoring and signaling traffic analysis. It offers end-to-end coverage - from security monitoring and up-to-the-minute anomalous-activity detection, to protecting signaling network perimeter across HTTP/2, Diameter, GTP-C and SS7 signaling protocols. Coupled with rich analytics and reporting capabilities, SecurityGen IDS platform empowers telecom operators to respond to threats as they occur. SecurityGen IDS keeps you ahead, prevents hacker attacks, and protects your core network while enhancing your goodwill among subscribers.

Key Features

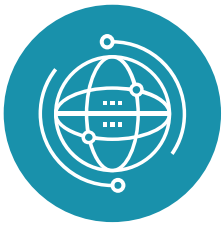
Enhanced Visibility For Early Threat Detection

The IDS platform provides complete visibility of the core telecom network and enables real-time threat detection. While traditional SOC could control only the core IT infrastructure, IDS allows the monitoring of a telco's core network. Capable of integrating natively with SIEM and SOAR systems, IDS empowers SOC with real-time data alerts on threats and events. This proactive monitoring helps SCO stay ahead of adversaries and fortify their cybersecurity posture.



Advanced Analytics For Rapid Incident Response

SecurityGen IDS's rich analytics and reporting capabilities allow for real-time threat responses. It displays aggregated data on comprehensive dashboards and generates actionable attack-related reports, which help mitigate attack consequences. Moreover, it also performs real-time or retrospective incident investigations.



Intuitive Navigation & Advanced Forensic Capabilities

The rise in the number of attacks detected is an unmissable signal to enhance filtering mechanisms capable of fast and intuitive navigation. IDS provides filtering, grouping and sorting capabilities for instant search across the attack by specific criteria. It offers flexibility to customize views by adding or removing attributes to display on the attack list. Besides attack time, source, and target, the IDS platform also helps enrich data with GSMA threat category, attack type, severity, and potential impact.

Maximized Efficiency Of Other Security Measures

The platform comes with the capability of evaluating the performance of other security countermeasures, and provides valuable information to improve their performance. For example, it simplifies the management of filtering rules, and provides insights on how to fine-tune signaling firewall settings to block specific attacks more efficiently.

Seamless Operation

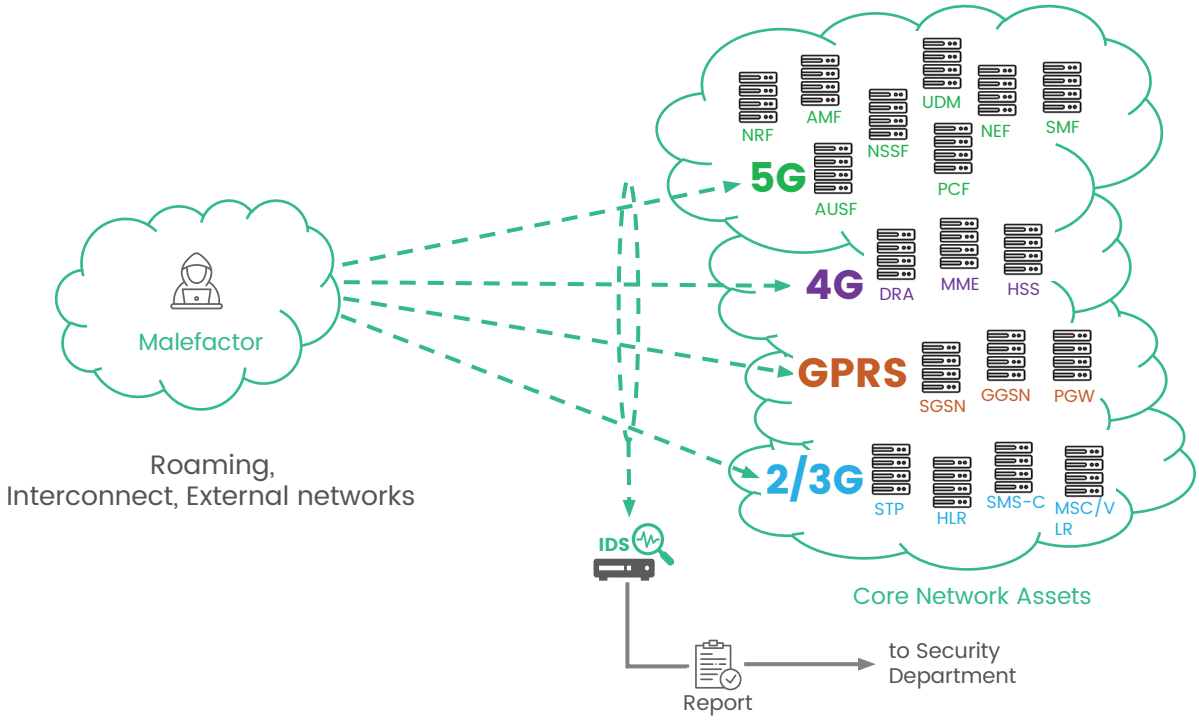
A copy of signaling traffic is all that the platform needs to detect attacks against a telecom operator. By performing thorough analyses in the background, the platform captures both incoming and outgoing traffic flows, with zero impact on core infrastructure, network services or critical operations and processes.

Machine Learning & Element Profiling

Taking into account vulnerabilities and the rapid obsoletion of signatures, our IDS platform comes integrated with Machine Learning (ML) and Element Profiling technologies which, based on the statistical analysis of signaling traffic, help detect suspicious signaling nodes (pertaining to odd number of messages - ML or in case they unexpectedly change roles -Element Profiling). Embedded ML technologies, advanced analytics, unique threat detection rules, and retrospective analysis allow our IDS platform to decrease attack surface, detect attacks outside signature database, and reduce cases such as Zero-day instead of waiting for exploits by malefactors.

How The Platform Works

Detect - IDS



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

BUSINESS BENEFITS

SecurityGen IDS ensures a host of advantages, including but not limited to:

Enhanced awareness to manage security risks

Automated security operations to keep costs down

Faster incident investigation and response to minimize damage

Benefits from investing in a cost-effective solution

Being a step ahead of the threats in signalling network element Profiling by ML

Receiving expert support directly from acknowledged vendors

Protecting your brand and reputation

About SecurityGen

Founded in 2022, SecurityGen is a global start-up focused on telecom security. We deliver a solid security foundation for driving secure Telco digital transformations and ensuring next-gen enterprise intelligent connectivity.

Connect With Us

Email: **contact@secgen.com**
Website: **www.secgen.com**

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