Stockholm, Sweden
03 March 2025 08:00:00 CET

stc Achieves 100% Compliance to GSMA Signaling Protection Guidelines, Demonstrates Commitment to Protect Subscribers and Critical Infrastructure

stc Reports Flawless Results using Enea Adaptive Signaling Firewall

Saudi Arabia’s largest mobile network operator stc has become one of the few telecom operators worldwide to achieve 100% compliance with the signalling security controls recommended by the GSMA. This milestone reflects stc’s unwavering commitment to securing its network and subscribers against the ever-evolving threats in the telecommunications landscape. Powered by the Enea Adaptive Signaling Firewall, stc’s signaling network demonstrated exceptional resilience across all signaling protocols, including SS7, Diameter, and GTP-C.

STC achieved this milestone by designing and implementing robust security controls, and validating their effectiveness through extensive penetration testing. This was accomplished not only by adhering to GSMA security guidelines as the telecom industry benchmark for signaling security but also by incorporating additional measures to ensure comprehensive protection. These threats range from personal data leaks and unauthorized location tracking to the interception of sensitive communications through voice calls, messaging, and data. As a key enabler of Saudi Arabia's Vision 2030, stc recognizes the critical importance of providing secure and reliable communications to its consumer and business subscribers. This achievement positions stc as a global leader in providing safe and secure communication services, exceeding industry benchmarks and setting a new standard for subscriber and infrastructure protection.

The longstanding alliance between stc and Enea has been pivotal in achieving this milestone. By combining stc’s proactive approach to security with Enea’s cutting-edge signaling firewall technology and threat intelligence, the partnership has developed robust defenses against even the most sophisticated cross-protocol attacks. The two companies have worked closely together through a continuous cycle of rigorous testing, in-depth threat analysis, targeted use case development, and enhanced signaling firewall deployment. While GSMA recommendations are a valuable foundation, stc is committed to pushing the boundaries of signaling security to deliver the highest level of protection for its network and subscribers.

Meticulously designed to identify vulnerabilities and validate the robustness of stc’s signaling protection against real-world attacks, the comprehensive testing complies with and far exceeds industry standards such as GSMA’s guidelines for signaling firewalls. For example, the testing included complex cross-protocol attacks, requiring advanced cross-protocol analysis by the signaling firewall to be detected. By adopting a threat actor's perspective and leveraging the combined expertise of stc and Enea, all attempts to bypass the firewall's security controls failed. The fact that no attempts succeeded underscores the success of stc and Enea's dedicated work in implementing the most robust signaling security possible.

Stockholm, Sweden
03 March 2025 08:00:00 CET

Abdulaziz Alaqil, Cybersecurity & Data Governance Excellence GM at stc, stated "Achieving a 100% compliance rate to GSMA guidelines is about much more than passing tests; it's a testament to stc's comprehensive security strategy and our relentless pursuit of excellence in protecting our subscribers. We proactively design and implement security controls above and beyond standards, continuously validating their effectiveness through rigorous penetration testing. As one of the few operators globally to reach this level of compliance, stc is proud to lead the industry in setting new benchmarks for telecom security. Enea's expertise and technology have been instrumental in reaching this 100% signaling security milestone, and the accomplishment is a direct result of our strong partnership".

John Huges, SVP and Head of the Network Security Business Group at Enea, commented: "This achievement reinforces our position as a leader in telecom security and underscores the importance of constant improvements founded on intelligence insights. Working closely with stc's cybersecurity team, regarded as one of the most skillful in the industry, helps us stay on our toes and show what is possible. We are very proud of achieving this milestone together with stc."
stc and Enea remain steadfast in their commitment to pushing the boundaries of signaling security, ensuring stc's subscribers can communicate with confidence and peace of mind in an ever-evolving threat landscape. This achievement represents a significant step forward in securing the future of telecommunications.

Contact Enea

Claire Murphy, Head of Marketing
Claire.murphy@enea.com

Contact stc

Ryain Rajihi, Cybersecurity Design Director
rrajihi@stc.com.sa

About Enea

We are a world-leading specialist in advanced telecom and cybersecurity software with a vision to make the world's communications safer and more efficient. Our solutions connect, optimize, and protect communications between companies, people, devices, and things worldwide. We are present in over 90 markets and billions of people rely on our technology every day when they connect to mobile networks or use the Internet. Enea is headquartered in Stockholm, Sweden and is listed on NASDAQ Stockholm. Visit us at **enea.com**

About stc
We are a forward-focused digital champion always been focused on innovation and evolution. Our purpose is to create and bring greater dimension and richness to people's personal and professional lives. With stc, You will always be empowered to focus on delivering what's next through collaborative and agile ways of working, and a culture that is open to fresh ideas. Transforming the future through impactful digital solutions and mega-projects while fostering our commitment to sustainability.

Stockholm, Sweden
03 March 2025 08:00:00 CET

###

Attachments

---

stc Achieves 100% Compliance to GSMA Signaling Protection Guidelines, Demonstrates Commitment to Protect Subscribers and Critical Infrastructure