ASSERTION®
a voice security company

How a Leading ICT Provider Prevented Cyber Attacks on its SBCs with Assertion's SIP Remote Worker Security

The Challenge

Internet-exposed devices like Session Border Controllers (SBCs) that enable remote work are constantly threatened by cyber-attacks. SBCs act as security gatekeepers, verifying user credentials before allowing access to the network. However, attackers continually attempt to break in using stolen credentials or brute-force tactics to exploit vulnerabilities and break in.

Once inside as a legitimate user, they could make abusive, threatening, or harassing calls, call premium rate numbers to rack up huge bills (toll fraud), or eavesdrop on conversations Toll fraud alone costs enterprises over $12 billion per year globally. A successful breach results in significant revenue loss, system downtime, and compromised data confidentiality.

The ICT provider is a leading UCaaS / CCaaS provider for SMEs based on the Avaya voice platform and has 100s of customers in the country. Their SBCs would come under intense attack and it forced them to temporarily shut down the services, causing a lot of customer pain. They had a dedicated NOC team observing the SBC logs for indicators of attack and to take quick remedial action by blocking the attacker’s IP. This was not only expensive but ineffective as well – with many attacks still sneaking under the radar.

The Root Cause

While attack methods constantly evolve, a common vulnerability persists - the lack of robust, real-time monitoring systems to proactively detect and mitigate threats before they escalate.

Important Links

A single toll fraud incident can set you back by $20,000. Loss of confidential information, priceless!
Source - NoJitter.com

IRSF is one of the top frauds happening globally.
Source - CFCA.org

State of SBC Security Report 2021
Source - Assertion

Conventional Mitigation Approaches

Organizations have tried monitoring telecom bills for fraud indicators, tracking abnormal call spikes, call failures, CPU usage, and analyzing logs for suspicious activities. However, these reactive approaches require constant vigilance and deep expertise that most lack. By the time a monthly bill highlighting toll fraud arrives, the damage is already done.

The Solution

To safeguard its voice infrastructure, the ICT provider deployed Assertion® Secure Voice™. By applying AI to analyze every SIP registration message in near real-time, Secure Voice detects attack patterns accurately. Upon detection, it immediately alerts the NOC team and automatically blocks the attacker by provisioning rules on the SBC.

Leveraging a Vast Global Intelligence Network

Assertion® Secure Voice™ integration with its extensive AI network is a key advantage. This network consolidates global threat intelligence from various deployments, government sources, attack databases, premium rate number lists, and crowd-sourced attack information. This expansive repository ensures that the solution stays perpetually updated to counter emerging threats effectively.

Measurable Results

By implementing Assertion® Secure Voice™, the ICT provider achieved:

- Comprehensive visibility into active threats, unauthorized access attempts, and potential data breaches
- Automated real-time blocking of suspicious SBC registration attempts
- Significant cost savings by preventing toll fraud incidents and inflated telecom bills

A proactive, intelligent security solution is crucial in today's hostile cyber landscape. Assertion® Secure Voice™ is a robust sentry, guarding SBCs against multi-vector cyber-attacks.

About Assertion® Secure Voice™ for SIP Remote Workers

Assertion® Secure Voice™ is the world’s best solution for securing your SIP remote worker infrastructure. Among other capabilities, it

- Blocks Cyber Attacks on Your Remote Worker SBC
- Protects your SBC from enumeration, brute force, and time travel attacks.
- Blocks attacker IP automatically on SBC or Firewall within minutes.
- Allows registrations from specified countries only (geo-fencing)

Assertion® Secure Voice™ also screens your calls giving you complete traffic visibility and protects your business from Scam calls, Toll fraud, and TDoS attacks.

Watch the solution video and contact us Today for a trial