Banking on BroadShield

BROADSHIELD

Why This Case Study Is Relevant

It demonstrates the importance of installing anti-jam and anti-spoofing software.

Background

A major international financial services provider was experiencing issues in their lab environment with its GNSS-based timing systems. GNSS reception was being intermittently lost and the customer didn't know why. Rather than using a stronger, interference-resistant signal like STL from Orolia, the customer was using a competitor's traditional GPS-based antenna, which was experiencing trouble from an unknown source of RF interference.

Solution

Orolia installed BroadShield, our powerful anti-jam and anti-spoof software, into the customer's SecureSync time server. BroadShield immediately took mitigating action by identifying the potential GPS/GNSS signal interference.

The customer had been uncertain whether they would ever see BroadShield in action, but thought it was a prudent investment given the critical role of GPS based timing in the infrastructure they were rolling out. After all, accurate time is a major part of Financial regulations. This incident proved that BroadShield worked as described by protecting the fidelity of their network and ensuring ongoing compliance with regulations.

Result

The customer was so pleased that they mandated that all of their stratum 1 time servers, and even a few stratum 2 units, would include antijam antennas and BroadShield as their standard configuration.

30 November, 2018 – Banking on BroadShield (A)