SOLANA NETWORKS Visible Intelligence™

GET PLUGGED IN

SCADA Security Vulnerability Assessment

The Client: Public Safety Canada

Objective: Public Safety CCIRC is charged with protection of national critical infrastructure against cyber incidents including SCADA security attacks. The client wanted to conduct security vulnerability assessment studies on SCADA network infrastructure and protocols.

Background: SCADA (Supervisory Control and Data Acquisition Systems) are IT-based systems used to control industrial processes in a variety of critical infrastructure including power, nuclear, water, and oil & gas. When the security of such systems is compromised, malicious attackers can gain control over Canadian critical infrastructure or cause destruction/damage to the equipment and its surroundings.

.

Outcome: Working with Byres Security, Solana Networks developed a SCADA cyber security test bed for the client. The test bed modeled industrial processes in the oil & gas as well as power industries and included wired and wireless infrastructure representative of real-world SCADA systems. Vulnerability assessment and cyber security testing was carried out on a range of network devices including PLCs, SCADA protocols, SCADA routers, 3G wireless routers, industrial firewalls. The testing uncovered a number of previously unreported vulnerabilities. Working with partners Bell Canada and Exida, Solana also delivered a Best Practices Guide and Red-Blue Training Exercises for securing SCADA networks.