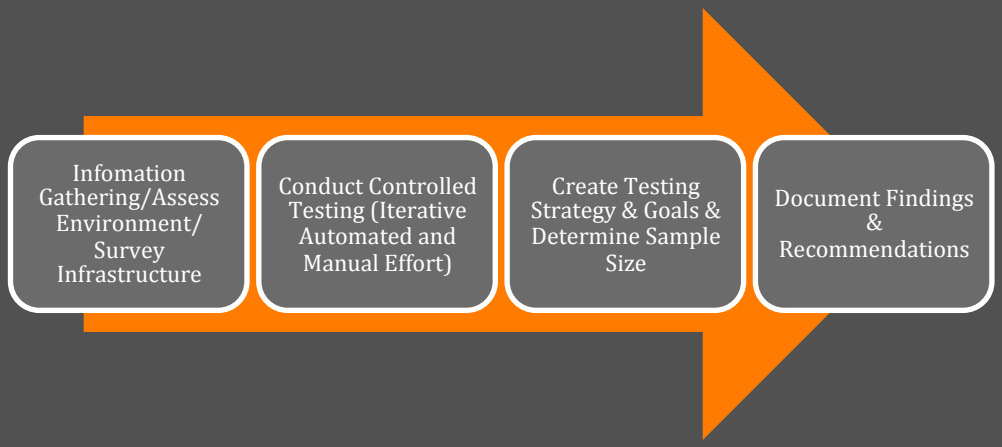
Securing Your Critical Infrastructure

SCADA NETWORK PENETRATION TEST & VULNERABILITY ASSESSMENT

- PINPOINT NETWORK AND SYSTEM SECURITY FLAWS
  Determine whether the networks and systems are resilient to unauthorized access or malicious attacks and afford adequate protection.
- ASSESS NETWORK SECURITY ARCHITECTURE
  Determine whether the network architecture is adequately configured to mitigate probable attack vectors, as well as afford client's sufficient knowledge and notice to adequately respond to any attack.
- ASSESS EXISTING PROCESSES AND PROCEDURES
  Analyze whether existing processes/procedures are adequate to prevent a reoccurrence of vulnerabilities.
- ANALYZE AND DOCUMENT FINDINGS
  Analysis and documentation, including findings and recommendations at both a technical and procedural level.

relay SECURITY GROUP

Service Offering



Details

Relay Security Group, LLC (Relay) was founded in 2007 by information security professionals with over twenty years of cumulative IT security experience in a wide range of markets. Our mission is to provide our clients—through actual validation of vulnerabilities and with minimal impact on their often-sensitive operations—with the most accurate information about security threats to their environments and their readiness to meet current industry standards and regulations. Relay's validation methodology, processes, and recommendations take into account the complexities of these environments, which translate to recommendations that are both reasonable and actionable.

In addition to a strong general understanding of IT security, Relay consultants have over nine years of experience performing evaluations within SCADA environments and of SCADA products and applying/interpreting the NERC CIP standard. The Relay team has significant expertise within the power and energy industry.

Relay's Supervisory Control and Data Acquisition (SCADA) Penetration Test and Vulnerability Assessment services are based on proven penetration testing and vulnerability assessment methodology, which incorporates the Open Source Security Testing Methodology Manual (OSSTMM) v3.0 in combination with Relay's proprietary techniques that, not only takes into account industry specific requirements, but also provides a detailed review of the client's systems and networks.

Relay's main focus during the testing is to mitigate any disruption to the operational infrastructure while obtaining a thorough understanding of the information security posture. To achieve this Relay uses the following process:

- Conduct interviews and review documentation (including specific pertinent industry standards) to gain a better understanding of the infrastructure as it pertains to the perimeter and SCADA infrastructure;
- Create a testing strategy that includes different goal-based scenarios, which will be reviewed and approved by pertinent client staff;
- Determine a valid sample size that may incorporate trust relationships between systems, as well as development, secondary, or backup systems (e.g. HMI, Application servers, Historians, & PI servers);
- Conduct controlled port and/or vulnerability scans and controlled validation testing to ascertain how these vulnerabilities may indirectly or directly impact the operational environment; and
- Assess the security configuration and management of the SCADA network/systems/application with respect to access control, user and group management, application/system/network security configuration, and the authentication processes.

3750 Brodie Way Dublin California 94568 ☎ 800.613.0431 ✉ sales@relaysecurity.com WWW.RELAYSECURITY.COM