SCADA Services

Oil and gas, alternative energy, manufacturing and utility companies increase demand for proper tool implementations to allow remote access to controlling and regulating SCADA and other industrial control systems. The advancements in technology allow organizations to connect seamlessly to their environments, though there are noticeable risks emerging which exposes the environment to the public.
Stakeholders who require such seamless remote connectivity are:

- *Accountants*
- *Maintenance*
- *Purchasing Departments*
- *Other SCADA platforms communicate over the internet*

The remote access necessary to perform organization duties with ease come with inherent risk as the level of exposure increases resulting in a rise in potential malicious attacks. Cybercrime is one of the greatest threats facing the world, the level of impact on a global scale is unmeasurable.
There are many reports of devastating incidents of organizations resulting in a breach, generating severe losses and physical damages to the corporate infrastructure.

Testing Your SCADA Network

With inevitable cyber-attacks continuing, security professionals in critical infrastructure face enduring pressures, which affect organizational priorities. They require improved flow of information and innovative strategies in risk management.

No organizations are completely resistant to cyber-attacks, though a proactive, all-encompassing strategy can eliminate a majority of threats. At a time when one small exposure can devalue an organization's brand, getting security right is imperative.

Why CyberArq SCADA Services?

CyberArqs industry security experts can assist asset owners protect SCADA and other critical infrastructure from emerging cyber threats. SCADA systems should be analyzed for threats and vulnerabilities.

Our team of security experts can assist you with:

- *SCADA Vulnerability Testing*
- *Risk Management*
- *Social Engineering*
- *Educate Officers, Managing Directors and Board Members on cyber risks*
- *Application & Database Vulnerability Testing*
- *Employee Security Awareness Training*
- *Educate employees to improve their knowledge and competency regarding cyber-security*

SCADA Targets

- One third of industrial sites are connected to the Internet.
- 60% of industrial sites have passwords traversing over networks in plain text.
- 50% are not running anti-virus protection software on their endpoints.
- IT security implementation. Most organizations have not fully deployed their IT security programs.
- About 20,000 different malware samples were found in ICS belonging to over 2,000 different malware families in 2016.
- Incomplete knowledge about network-connected devices. Legacy systems paired with newer technology may result in sacrificing mission-critical security.
- Casual patching practices. Consistent firmware and software updates, including patching bundled vendor packages is imperative.
- Incomplete monitoring. Many organizations are not getting actionable real-time threat alerts about security exploits.
- Discontinuity in system and user authentication can allow unauthorized users access to the system.
- Disparate policies and procedures. A unified security policy protects both information technology (IT) and operational technology (OT).