PARSONS

ICS/SCADA CYBERSECURITY

CRITICAL INFRASTRUCTURE PROTECTION SOLUTIONS

COMPANY OVERVIEW

Founded in 1944, Parsons is an engineering, construction, technical, and professional services firm with revenues of $3.1 billion in 2014.

Parsons is a leader in many diversified markets with a focus on defense/security, industrial, and infrastructure. Parsons delivers design/design-build, program/construction management, and other professional services packaged in innovative alternative delivery methods to federal, regional, and local government agencies, as well as to private industrial customers worldwide.

We conquer the toughest logistical and technical challenges and deliver landmark projects worldwide. Today, more than 15,000 Parsons employees are engaged in executing nearly 5,000 projects in all 50 states, and in 29 countries across the globe. For more information about Parsons, please visit www.parsons.com.

WORKING BEHIND THE SCENES

Parsons' defensive security services monitor and protect operational technologies and Industrial Control Systems and Supervisory Control and Data Acquisition (ICS/SCADA) infrastructure against breaches, fraud, theft, and sabotage. Our proactive countermeasures identify methods used by our nation's most sophisticated cyberenemies. We deliver proven cybersecurity solutions and are ready to support you.

THE CHALLENGE

The U.S. Department of Homeland Security has identified 16 critical infrastructures, including power generation and distribution; water and wastewater; transportation; manufacturing; and commercial facilities, such as building automation systems. ICS are used to manage almost every aspect of those critical infrastructures. ICS networks were originally physically isolated from business networks, and no data transfer occurred between the two. A truly air-gapped industrial control system is no longer the reality for most facilities. The introduction of Microsoft operating system-based controllers; IT network protocols, such as transmission control protocol/internet protocol (TCP/IP); and connection to the Internet allowed for improved operational efficiencies and cost savings. Businesses often rely on ICS production data reporting systems to manage their operations. Vendors and plant engineering staff may require remote access to support industrial control systems. Support staff may cross the air gap when they patch or update their systems – thus exposing ICS. The insecure state of ICS continues to make headlines as news of vulnerabilities and incidents are published. Viewed as a decade or more behind traditional IT security, these systems are attractive targets for external and internal attackers.

Are you equipped with the expertise to adequately defend your control network against threats?

CRITICAL INFRASTRUCTURE CYBERSECURITY SERVICES – PARSecure™

When it comes to cybersecurity, Parsons recognizes that our customers are driven by the growing cyberthreat and need to navigate the critical infrastructure regulatory compliance maze. PARSecure™ encapsulates our cyberservices portfolio and includes systems engineering, vulnerability assessments, penetration testing, and compliance capabilities and methodologies targeted to meet your needs.

Systems Architecture Engineering and Integration.

Parsons leverages our deep expertise in ICS and cybersecurity in conjunction with our engineering, technical, construction, and management services for critical infrastructures to provide unique services for asset owners and operators. We can assist customers in developing new procurement language for cybersecure ICS architectures.

NEW WAYS TO VIEW THE PROBLEM

Parsons builds and maintains mobile ICS/SCADA demo, testing, and training platforms with live real-world components.

Vulnerability Assessments.

Vulnerability assessments are the key to an impartial review of our customer's ICS cyberposture. We have conducted active and passive vulnerability/penetration testing for SCADA systems and designed solutions that immediately rectify the most critical vulnerabilities and provide a path for remediating the rest. Reviewing your people, process, and technology areas allows Parsons to determine any gaps between your security posture and industry best practices.

Penetration Testing.

Penetration testing (PENTESTING) is a form of vulnerability assessment that involves discovering weaknesses and then attempting to exploit those weaknesses at a customer's request. PENTESTING validates the existence of those weaknesses and illustrates the feasibility of a cyberattack. PENTESTs are usually unannounced to your security team, to simulate what an actual attacker may accomplish. We deploy custom-developed tools in the execution of PENTESTING services.

Compliance Services.

Compliance is an important aspect of your ICS/SCADA security program; however, a growing number of threats, regulations, and technology solutions make for a complex, convoluted security and compliance landscape. Parsons' knowledge, expertise, and methodologies enable us to assist with compliance program creation and review, analyze existing program gaps, and perform program audits.

Training Services.

We know that knowledge is power. Parsons has built and refined Control Systems Security Essentials courses and curricula that can be tailored to executives and engineers focused on understanding ICS/SCADA architectures, vulnerabilities, threats, drivers, and security strategies.

NEW WAYS OF ATTACKING THE PROBLEM

Parsons recognizes the sensitive, complex nature of ICS/SCADA systems and has developed innovative technologies to visualize, model, and simulate operational technologies. In our state-of-the-art Cyber Solutions Center, we can work with you to replicate your operational environment for risk modeling, attack simulation, incident response training, architecture analysis, and more. Parsons offers security appliance configuration services, including deep packet inspection of industrial control protocols such as Modbus TCP or DNP3, to secure communications between endpoints.

YOUR TRUSTED ADVISER

Parsons has been a respected partner in the federal, state, and municipal critical infrastructure community for decades. We look forward to extending our relationship and becoming your trusted cybersecurity adviser as well.

OUR CUSTOMERS

- Numerous federal agencies and intelligence community
- U.S. Department of Defense
- Major municipal utilities
- Metropolitan transit authorities
- Higher education universities
- Other confidential government and commercial industry customers

OTHER SECURITY SERVICES

- Security assessments
- Operational and IT security engineering
- NOC/SOC security engineering and operations
- SCADA/ICS security design and engineering
- Advanced protocols and secure routing deployment

CONTACTS

Liz Fields
VP, Sector Manager,
Information Systems & Security
(626) 808-8871
elizabeth.fields@parsons.com

Jay Williams
ICS/SCADA Cybersecurity
Business Development Director
(315) 706-7154
jay.williams@parsons.com

design.build.protect.℠

www.parsons.com