PARSONS

Vulnerability Assessment Services

COMPANY OVERVIEW

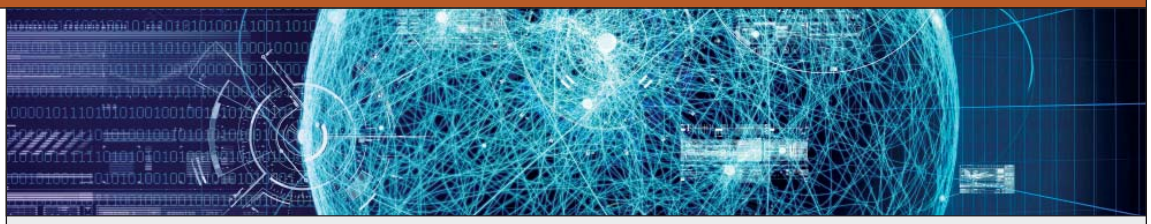
- Founded in 1944
- $3 billion revenue
- 162 offices worldwide
- 15,000 employees
- 1,500 cyber-professionals
  - CISSPs
  - CEHs
  - PMPs
  - CISMs
  - and many more

OUR CUSTOMERS

- Numerous federal agency 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 information technology security engineering
- NOC/SOC security engineering and operations
- SCADA/ICS security design and engineering
- Advanced protocols and secure routing deployment



We believe that Vulnerability Assessments (VAs) are the keys to impartial reviews of our customers cyberposture. We have conducted active and passive vulnerability/penetration testing for our customers and built remediation solutions that rectify the immediate vulnerabilities as well as address future issues. Reviewing our customers protocols, procedures, and response techniques gives Parsons the ability to present any gaps or findings that exist between security fitness and industry best practices.

OUR APPROACH – APPLICATION VAs

We conduct application VAs on static source code—meaning we work from flat files of precompiled programming code versus live production systems. In addition, we base our application VAs on industry guidelines from the National Institute of Standards and Technology (NIST), the Open Web Application Security Project (OWASP), and the Open Source Security Testing Methodology manual. The risk to customer production systems for this effort is negligible, as we safeguard securely transferred files to conduct our scan. We then analyze the identified results, eliminate false positive readings, prioritize findings, and produce our report. Normally, our presence is not required on premises because we can work remotely from Parsons' secure facilities.

OUR APPROACH – INFRASTRUCTURE/NETWORK VAs

Parsons can perform a vulnerability scan on our customer's compliance standards from the Department of Homeland Security, NIST, and ISO 27002; and we can search for vulnerabilities against the most recent attack vectors and critical device misconfigurations. The sole focus of the scan are the IP addresses identified to Parsons by our customer. Prior to any testing, both teams will thoroughly discuss test objectives, coordination, logistics, safeguards, and progress calls. For the external scan, our presence is not needed on the customer's premises as we can work remotely from Parsons' secure facilities. The risk to customer systems is minimal, and we take nothing for granted, working closely with our customer's technical staff to ensure proper mitigation steps are planned. We prefer to scan non-production environments such as backup data centers and fail-over/development networks. In addition, we prefer to conduct tests on Friday and Saturday during the late evening hours.

BUILDING TRUST AND WORKING BEHIND THE SCENES

Parsons has quietly worked behind the scenes, delivering cybersecurity services that protect our nation's most sensitive information and critical infrastructure for 30 years. Parsons' defensive security services monitor and protect against breaches, fraud, theft, and sabotage. Our proactive countermeasures identify threats and methods used by our nation's most sophisticated cyberenemies. We deliver proven solutions and are ready to support you.