COALFIRE FEDERAL

Technical security assessments

Coalfire delivers methodology-driven assessments across a diverse set of technologies, including penetration testing, red team operations, hunt operations, application security assessments, social engineering assessments, and training.

Most organizations are already compromised, but they lack the ability to recognize an adversary in their own environment. Mature organizations are beginning to accept the fact that it's not if they will be breached, but when. Reports indicate 70% of the high-severity vulnerabilities are detected NOT by automated security tools, but rather, by trained experts. Our team includes recognized experts who have experience with some of the most sophisticated technical problems and the capability to demonstrate the true risk organizations face. Our team provides a complete analysis of the real risks to organizational information systems, an immediate set of actionable items, and assistance in developing a long-term strategy for overall security program maturity. Our services include:

- **Penetration testing:** Our adaptive penetration testing methodology provides valuable insight into the real-world risks of system vulnerabilities and business impact of network intrusions to reduce organizational risk exposure.
- **Red team operations:** Our adaptive red teaming methodology provides a full-scope assessment of the effectiveness of security operations processes, personnel, and technology against highly sophisticated threats.
- **Application security assessments:** Our assessments build critical, secure application lifecycles to comprehensively identify weaknesses in applications – whether in-house or third-party developed – regardless of the operating platform.

Client partnerships

CERTIFIED TECHNICAL EXPERTS IN LEADING CLOUD, ENCRYPTION, VIRTUALIZATION, AND CONTINUOUS MONITORING SOLUTIONS

Carnegie Mellon University

Since 2010, Coalfire has partnered with Carnegie Mellon University (CMU) Software Engineering Institute (SEI) to provide support to the Department of Homeland Security (DHS), beginning with the development of the risk and vulnerability analysis (RVA) program. Since then, we have developed and refined additional technical disciplines for DHS including penetration testing, vulnerability assessments, cyber hygiene, testing methodologies, security services development and framework integration, assessment tool evaluation/prototyping evaluation, and run book development. In addition, we have worked with SEI for five years on their information security continuous monitoring (ISCM)/cybersecurity compliance validation (CCV)/continuous diagnostics and mitigation (CDM) program.

Social Security Administration

When the Social Security Administration (SSA) required assistance in achieving and maintaining compliance with the Federal Information Security Management Act (FISMA) of 2002 and Office of Management and Budget (OMB) requirements, they tasked our team with independent verification and validation (IV&V) services support. Specific tasks included the creation of a boundary scope memo (BSM), security control testing activities (assessment prep, actual assessment, and security assessment report), risk analysis, risk management framework (RMF) activities, penetration testing, and policies and procedures support. In later task orders, Coalfire provided additional penetration testing, FISMA and RMF assessment support, continuous monitoring, software assurance, vulnerability scanning, and other security assessment support services. Our efforts resulted in SSA achieving and maintaining compliance with FISMA and OMB requirements. We also supported the SSA with the tools, templates, systems, and processes necessary to continue to reduce and mitigate risks. Our recommendations improved their overall security program, and our team also uncovered various locations that contained SSA data but had not been previously assessed.

TRUSTED INSIGHT FOR NAVIGATING THIS COMPLEX CYBER WORLD

GSA Schedule 70

- 132-45A Pen Test
- 132-45C Cyber Hunt
- 132-45D Risk & Vulnerability Assessment (RVA)

Other contract vehicles

- CDM BPA Subcontractor
- SeaPort Enhanced prime contract

GSA IT Schedule 70 Contract Holder SeaPort-e

CMMI Services Maturity Level 3 | Accredited FedRAMP 3PAO, PCI QSA and HITRUST CSF Assessor | Certified ISO 9001 (2015), ISO 27001 (2013) CONUS/OCONUS Support Capability | System for Award Management Registered

CAGE Code: 36BY6 | **DUNS #:** 184456155 | **NAICS:** 541519, 541512, 541513, 541611, 541690, 541511

COALFIRE FEDERAL

Cybersecurity that fuels success | CoalfireFederal.com | 877.224.8077

Fed_CTechSecurityAssessment_111119