ASSESSMENT SERVICE OFFERINGS

Proactively evaluate your organization's ability to effectively prevent, detect, and respond to cyber threats before they disrupt your business and impact your bottom line. Receive tactical and actionable recommendations to improve processes, technologies, and overall security posture.

Defensible Assessment Service	Service Description
Penetration Testing	Defensible's Penetration Testing Service is aimed at testing both your external internet-facing and internal network controls, this service evaluates how your defenses stand against the latest threats, aiding in the development of a security strategy that highlights and prioritizes risks. Key penetration testing methods are focused on: • Internal Penetration Tests: Investigate the security of your internal networks to uncover vulnerabilities and potential avenues for insider threats or lateral movements. • External Penetration Tests: Assess the security of your external, internet-facing assets to identify weaknesses that could be exploited by external attackers. • Web Penetration Testing: Concentrate on discovering security flaws in your web applications and services, ensuring they are robust against cyber-attacks. These tailored services are designed to match the specific environment and needs of your organization, offering a targeted approach to enhancing your security posture.
Compromise Assessment	Defensible's Compromise Assessment service detects cyber threats—past and present—in your IT environment. Our team uses advanced tools to analyze digital evidence, identify compromise indicators, uncover unauthorized actions, and fix vulnerabilities to halt threat progression. • Business Email Compromise • Ransomware Readiness • Phishing
Comprehensive Risk Assessment	Evaluate cybersecurity risk comprehensively, ensuring it aligns with your business goals. Defensible approaches security risk assessment from both external and internal viewpoints, combining security technology with business stakeholder interviews to pinpoint weaknesses in your cybersecurity risk management strategy. This methodical evaluation not only reveals risks but also assists in prioritizing them, maximizing the effectiveness and return on your cybersecurity investments.
Compliance or Cyber Insurance Readiness Assessment	Strengthen and document your information security strategy to fulfill the demands of compliance frameworks and cyber insurance requirements. Focus on establishing explicit policies, controls, processes, and procedures for a comprehensive assessment to pinpoint and rectify compliance gaps. • SOC2 • ISO27001 • HIPAA • PCI DSS • CMMC • NIST Cybersecurity Framework • CIS Controls