CANARYTRAP

Catching Vulnerabilities and Trapping Exploits

Canary Trap's elite team of security experts come armed with the tools, experience and credentials to help improve your organization's security resiliency and cyber risk posture.

SOCIAL ENGINEERING VULNERABILITY ASSESSMENT

Assess, educate and inform end user security awareness and resiliency.

SERVICE OVERVIEW

Social engineering is the tactic of manipulating, influencing, or deceiving a victim to gain control over a computer system, or to steal personal, financial and otherwise sensitive information. It uses psychological manipulation to trick users into making mistakes or giving away sensitive information.

Scams based on social engineering are built around how people think and act. As such, social engineering attacks are designed to manipulate a user's behaviour. Once the adversary understands what motivates a user's actions, they can deceive and manipulate the user effectively and efficiently.

Generally, social engineering attackers have one of two (2) goals:

1) Sabotage
2) Theft

Canary Trap will employ the following methods, tactics and types of simulated social engineering attacks during a Social Engineering Vulnerability Assessment (SEVA):

- ✓ Pre-engagement Research
- ✓ Phishing Emails
- ✓ Spear Phishing
- ✓ Vishing (Voice Phishing)
- ✓ Reporting and Recommendations

Canary Trap combines human expertise with sophisticated tools, proven methodologies and, where appropriate, threat intelligence to ensure a thorough, in-depth approach to security testing, advisory and assessments.

Engage Canary Trap

Complete our Scoping Questionnaire at www.canarytrap.com or Contact Us directly by telephone or email.

Findings Report

Canary Trap will deliver a Findings Report highlighting any identified vulnerabilities for remediation.

The Canary Trap Approach

- ✓ **Step 1:** Define
- ✓ **Step 2:** Assess
- ✓ **Step 3:** Report
- ✓ **Step 4:** Remediate
- ✓ **Step 5:** Retest

inquiries@canarytrap.com (844) 750-2018 www.canarytrap.com