Advanced Persistent Threat Assessment

DATA SHEET

A Single Assessment for Better Accuracy and Increased Threat Landscape Awareness

Traditional penetration tests and assessments focus on particular areas of discipline, such as technical controls, physical security, policy compliance, or social engineering. Because attackers do not limit their attacks to a single discipline, neither does TraceSecurity's Advanced Persistent Threat Assessment (APTA). The APTA is a comprehensive assessment that tests the ability to exploit multiple attack actions of an actual attacker and identifies any resulting weaknesses that could result in the unauthorized disclosure, misuse, alteration, or destruction of confidential information, including Non-Public Personal Information (NPPI).

The Compliance Overview

IT security and compliance regulations and guidelines, such as GLBA, FFIEC, HIPAA, NCUA, FDIC, etc., require organizations to conduct independent tests of their information security and compliance programs. In addition to regular security assessments, best practices recommend that organizations perform penetration tests to ensure the security of their information systems and critical data.

The APTA provides a realistic assessment and fulfills several testing objectives simultaneously - all while reducing cost and delivery time compared to identical, individual services.

TraceSecurity's Advanced Persistent Threat Assessment Overview

Attackers employ a variety of techniques to create a synergistic attack, and it only takes one successful exploit to enable futher attacks. TraceSecurity's APTA examines and tests your organization's controls at multiple layers: technical controls, personnel and procedural controls, and physical controls. Tests are designed to identify any weaknesses that could be used by external attackers to disrupt the confidentiality, availability, or integrity of the organization's data and information systems. Once identified, you are able to address each weakness.

TraceSecurity's Security Testing Methodology:

- Authentication and access controls
- Network security
- Host security
- User equipment security (e.g. workstation, laptop, handheld)
- Personnel security
- Physical security
- Application security
- Software development and acquisition
- Business continuity – security
- Service provider oversight – security
- Encryption
- Data security
- Security monitoring

Results are provided in an extensive report containing:

- Introduction
- Executive summary
- Remediation action plan
- Detailed audit results
- Control descriptions and verification procedures
- Script injection attacks
- Supporting documentation