TRACE3

Security Solutions

Trace3's Security Solutions team leverages decades of combined experience in the field to address our client's most pressing security challenges. This expertise helps make Trace3 one of the most trusted partners in the emerging technology and security space.

Customer ("Client") would like Trace3 support in evaluating their security posture through comprehensive **External Network Penetration testing.**

SUMMARY OF SERVICE

Trace3 will perform an External Penetration Test for a set number of hosts on the client's publicly available perimeter, utilizing both automated and manual techniques. The goal is to provide a security assessment of the ports, services, and software running on an environment's external perimeter. Trace3's external network penetration test helps provide clients with an understanding of what risk is present on their perimeter as well as focused remediation efforts to help reduce their attack surface.

ASSESSMENT LEVELS

Trace3 offers two service levels – **Standard** and **Continuous** – each designed to meet varying security needs. At all levels, Trace3 testers will manually review findings and validate any potential vulnerabilities that are found. All testing is done based on frameworks such as OWASP, NIST, and MITRE.

- **Standard**: A one-time test focused on a point-in-time snapshot of findings and risks on the perimeter, as well as a one-time validation retest.
- **Continuous**: Ongoing automated review and testing of all assets on a regular cadence, with manual oversight and evaluation of findings to validate any potential false positives and highlight high-severity items.

ENGAGEMENT OVERVIEW

Trace3 will investigate, review, and evaluate all provided in-scope public IPs, URLs, and hosts for any known vulnerabilities. This includes an initial vulnerability scan and inventory assessment to establish a baseline. Trace3 testers will then manually review all active ports and services present and manually confirm any potential risks. Testers will focus on the ability to exploit security misconfigurations or abuse services for unexpected access or risk to the business. A report will be created with an Executive Summary, Technical Findings, and Assessment Narrative showing the steps taken.

APPLICATION RETEST

For the Standard level of service, Trace3 will conduct a one-time retest of the found vulnerabilities after the client implements fixes to verify the resolution of previously identified vulnerabilities. The retest may be performed within ninety (90) days of the completion of the previous assessment.