SOC 2 Penetration Testing Services

Steps to Schedule Your SOC 2 Penetration Test:

>> Schedule a 30-minute Discovery Session

>> We determine IF and HOW we can help

>> We provide a Tailored Proposal

>> Together, we review the Proposal

Developed by the AICPA, SOC 2 is specifically designed for technology service providers that store client data in the cloud. SOC 2 applies to nearly every SaaS (Software-as-a-Service) company, as well as any company that uses the cloud to store client information. To become SOC 2 compliant, companies must conduct a cybersecurity audit. This audit analyzes five controls, known as the Trust Service Principles (TSP): security, availability, processing integrity, confidentiality, and privacy. Auditors assure that these five controls are relevant to the industry.

We recommend penetration testing once a quarter as part of SOC 2 compliance.

There are two types of SOC 2 Audits – Type I and Type II. A SOC 2 Type I audit is more of a documentation review, whereas a SOC 2 Type II audit is a review of operations – control implementation effectiveness.

Penetration testing is primarily used to test control effectiveness in SOC 2 Type II audits.

METHODOLOGY

We follow a seven phase methodology designed to maximize our efficiency, minimize risk, and provide complete and accurate results. The overarching seven phases of the methodology are:

- Planning and Preparation
- Reconnaissance / Discovery
- Vulnerability Enumeration / Analysis
- Initial Exploitation
- Expanding Foothold / Deeper Penetration
- Cleanup
- Report Generation

BENEFITS / RETURN ON INVESTMENT

We think it is better to have an ethical hacker find the holes into your enterprise than an adversary. Our SOC 2 Penetration Testing provides details on exploitable vulnerabilities in a prioritized, tangible manner. Our report allows you to better understand what your environment looks like from an attacker perspective. This helps you prioritize efforts to mitigate risk to reduce breach likelihood or damage.

Not only do our SOC 2 Penetration Testing Services show you what your attack surface looks like to an adversary attacker, but they can be used as a safe way to test your organization's Incident Response (IR) and digital forensics capabilities. Our Penetration Testing services can be used to tune and test your security controls, such as your IDS, Firewall, Endpoint Security, Router ACLs, etc.

DELIVERABLE

The **SOC 2 Penetration Test Report** includes IP addresses, URLs, mobile apps, and APIs tested, vulnerabilities discovered, steps taken during the assessment, exploitable areas discovered, and prioritized recommendations. For any systems we are able to exploit, an "Attack Narrative" section is used to discuss step-by-step the process we used to gain access, escalate privileges, etc.