May 22, 2023

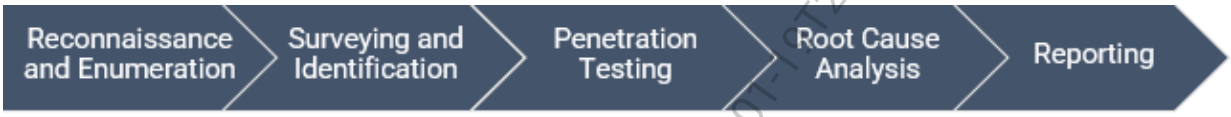
To whom it may concern:

Rapid7 Consulting conducted a thick client penetration test for Automox between April 24 and May 5, 2023. This test was designed to provide Automox with an independent, point-in-time assessment of thick client vulnerabilities from the perspective of a malicious actor in accordance with Center for Internet Security (CIS) Controls and National Institute of Standards and Technology (NIST) guidelines.

The thick client application penetration test objectives include:

- Document and demonstrate attack vectors.
- Quantify the impact of successful attacks through active exploitation.
- Identify specific threats that Automox can remediate.

Rapid7 uses a modular methodology that applies testing resources to essential areas in progressing phases:



During the analysis phase, Rapid7 evaluated Automox's security posture in the areas of:

- **Network Security:** Rapid7 evaluated the network's security controls by testing Service Management, Encryption and Privacy, Admission Control, Authorization Control, and Patch Management.
- **Susceptibility to Brute-Force Attack:** Rapid7 evaluated if login portals can be brute-forced by testing User Accounts, User Passwords, Service Enumeration, and Service Passwords.
- **Internal Prevention and Monitoring:** Rapid7 evaluated how internal networks prevent and monitor intrusions by testing the Logging, Auditing, Intrusion Detection, and Threat Response.
- **Open-Source Intelligence Gathering:** Rapid7 evaluated how much Open-Source Intelligence (OSINT) is available by assessing User Accounts, Metadata, Social Networks, and Search Engines.

Regular security assessments demonstrate Automox's commitment to their security program and helps to identify ways that technical risk can translate into business risk.