VAPT for IOT devices

Business Challenge

VAPT for IOT devices at a regular frequency

Requirement

Assess the vulnerability of IOT.
Unearth if there is any vulnerability but not to the below list

- Weak, Guessable, or Hardcoded Passwords.
- Insecure Network Services.
- Insecure Ecosystem Interfaces.
- Lack of Secure Update Mechanism.
- Use of Insecure or Outdated Components.
- Insufficient Privacy Protection.
- Insecure Data Transfer and Storage.
- Lack of Device Management.
- Insecure Default Settings.
- Lack of Physical Hardening.

Provide the Vulnerability Report

Technology & Tools

- **Need to update**
- Language – Python, TCL /TK, Shell Scripting
- IDE – PyCharm
- Framwork: OpenWRT,
- IPv4 / IPv6 Routing , Bridging/Switching & Wireless routing
- Deployment – JENKINS, CI/CD
- Tools- STC, IxChariot, UCI, FAPI, Clish, Linux commands, pExpect, Paramiko

Value add by Mirafra

1. Implement the VAPT process
2. Furnishing VAPT report
3. Ensuring vulnerabilities are fixed
4. Retest the fixed build.