**“Assume Breach”**

General concept is we provide a low(er) touch SAAS for the initial offering and then use results of that to sell physical devices on network and low touch SASS.

Initial Offering:

1. External Attack Surface Scan
   1. Open Source Reconnaissance
2. Phishing Test
   1. <https://getgophish.com/>
   2. <https://www.trustedsec.com/social-engineer-toolkit-set/>
3. Browsing Assessment
4. Initial Foothold Executables
   1. Test
      1. Execution
      2. Escalation
      3. Lateral Movement
      4. Egress
5. Optional:
   1. Ship organization a PwnPro Clone (<https://store.pwnieexpress.com/product/pwn-pro/> )
   2. Automated Network Attacks
   3. Automated Wireless Attacks

Secondary Offering:

1. On Premise
   1. Network honeypot canaries on cheap hardware
   2. Wireless honeypot canaries
   3. Custom CanaryTokens ([https://canarytokens.org/generate](https://l.messenger.com/l.php?u=https%3A%2F%2Fcanarytokens.org%2Fgenerate&h=ATPp1MF7NgSJ5yGAxUuc8E63a1c99rrPluiti5douuUzRXg7HMPB0fojGj_hGv42q0PowKxmzsUFjxAgGtirO77QfX-iKuoUizsaaMD_))
   4. Attack Box
2. Executable Zoo
   1. \_n\_ pieces of unique malware a month testing various things
   2. Execute, Escalate, Lateral, Egress
   3. One zip file, one script to execute it all, and log everything
   4. Check callbacks server side
3. Continual Scanning
4. Continual Phishing Training