LIFARS
your digital world, **secured**

LIFARS REMOTE WORKER CYBER RESILIENCE SERVICES

Gap Analysis testing as well as remediation guidance for your remote work cyber infrastructure

*Each service includes a Summary Report of current posture along with remediation guidelines

1. **Daily T.R.U.T.H.**
    a. Daily Threat Hunt of client infrastructure
    b. Detection of known threats and suspicious behavior
    c. Monthly Depending on size employee population

2. **Quick Remote Access Penetration Test**
    a. External Testing of Remote Access Infrastructure
    b. 2 Days

3. **Remote Worker Device Assumed Breach Test**
    a. Internal Testing what a threat actor can do if access to remote worker device is compromised
    b. security posture validation. Verification if one compromised remote worker means compromised infrastructure
    c. 2-3 Days

4. **Remote Vulnerability Access Audit**
    a. Audit overall remote infrastructure configuration of remote access infrastructure
    b. 2 Days

5. **Remote Worker Endpoint Protection**
    a. Deploy Fidelis or Carbon Black to Remote Endpoints for 30 Days for Free
    b. Employ Daily monitoring for ENDPOINT ONLY
    c. Monthly Depending on size employee population

6. **Remote Worker Workstation Hardening Guidelines**
    a. Review config of remote Workstation to understand current cyber strength
    b. Prepare guidelines for hardening of those devices
    c. One Day
    d. LIFARS could perform the hardening on demand