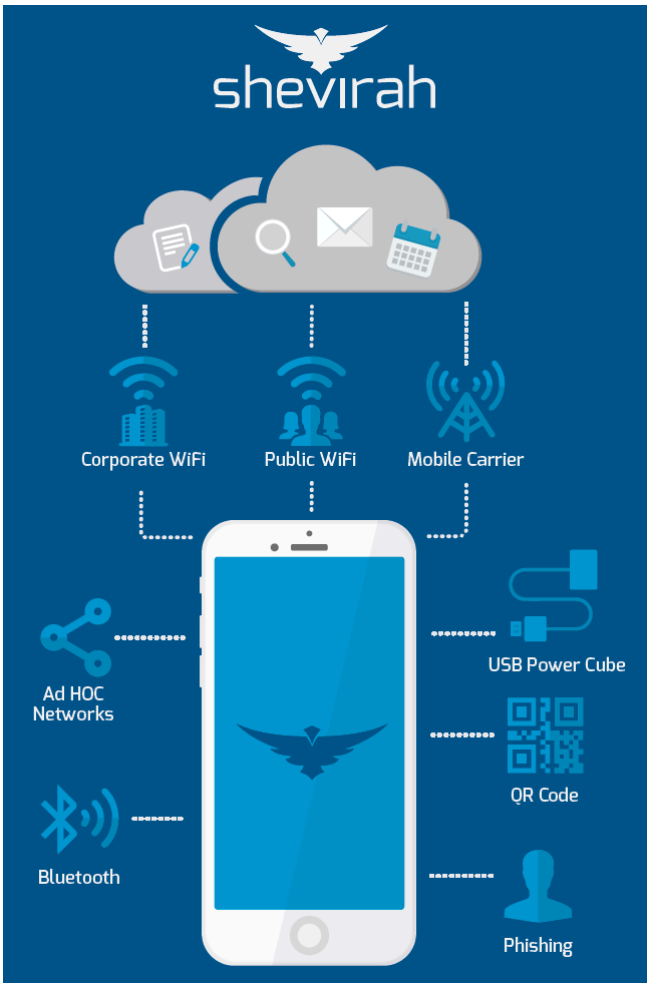
Dagah™ mobility and IoT cybersecurity testing tools

Automated mobile and IoT device vulnerability assessment, penetration testing, and mobile security awareness training



> ***"Dagah tool is truly cutting edge"***
> **Admiral Blair**
> Ex Director National Intelligence
>
> ***"The network is not the vulnerability, your people are"***
> **Mary Chaney**
> JD, CISSP, VP ICMCP

Dagah tools automate **mobile** and **IoT** vulnerability assessment (VA), pen testing, reporting and compliance for a large playbook of simulated cyberattacks including:

- **Email / text / IM phishing attack**
- **Bluetooth/NFC attack**
- **QR code attack**
- **Malicious apps**
- **Data loss**
- **Remote control attack**
- **Rogue cell or Wi-Fi attack**
- **Rogue ad hoc networks**
- **Rogue hardware**
- **Rogue charger/USB device attack**

Dagah can also be used for awareness and training programs, for example, around simulated mobile phishing attacks [1]. Mobile users are up to three times more vulnerable to phishing attacks [2]. Target devices can be smartphones, tablets, or Internet of Thing (IoT) systems including vehicles, drones, CPE (Customer Premise Equipment), PoS (Point of Sale), wearables or medical devices.

Why is it needed?

Automated testing tools have been available for a long time, covering data centers, PCs and laptops. Legacy tools have not kept up with the rapid enterprise adoption of the cloud, smartphones, tablets and connectivity for once air-gapped IoT systems. Newer app-based cybersecurity tools, Mobile Threat Defense (**MTD**), Enterprise Mobility Management (**EMM**) and Mobile Device Management platforms (**MDM**) cover some but by no means all mobile attack vectors. Even that coverage may be absent where agents are not pre-installed, for example, in Bring Your Own Device (**BYOD**) programs.

Dagah™ mobility and IoT cybersecurity testing tools

Gaps in coverage leave organizations with potentially undetected vulnerabilities, or having to carry out manual testing. Manual testing brings its own challenges of costs, delays and access to resources with the appropriate expertise to test effectively rather than simply ticking boxes. Dagah automates effective mobile device VA, pen testing and training processes, with no agent installation or pre-preparation required, for rapid ROI.

Getting started

- **Apple iOS or Google Android**
- **Easy-to-use GUI or command line**
- **Easy-to-operationalize**
- **SaaS or on premise**
- **Contact us for more information, a demo, or trial**

Compliance with cybersecurity standards and best practices including	
• **CIS Controls**	**- Critical Security Controls**
• **EO 13800**	**- Strengthening the Cybersecurity of Critical Infrastructure**
• **GDPR**	**- General Data Protection Regulation**
• **FTC**	**- IoT: Privacy and Security in a Connected World**
• **NIST 800-53 r4**	**- Security and Privacy Controls for Federal IT**
• **NIST CsF**	**- Cybersecurity Framework**
• **NYDFS**	**- Cybersecurity Regulation (23 NYCRR 500)**

About Shevirah

Shevirah is a U.S. company founded in 2015 by cybersecurity expert Georgia Weidman. We specialize in products for automated mobile and IoT device vulnerability assessment, penetration testing, and mobile security awareness training. Our capabilities compliment traditional Mobile Threat Defense (MTD), Enterprise Mobility Management (EMM), Mobile Device Management (MDM), or mobile app inspection tools. Shevirah's name comes from the Hebrew word for "shattering or breaking of vessels", reflecting the goals of cybersecurity assessment and testing. Shevirah's platform includes the patent pending Dagah software. We are headquartered in the greater Washington, D.C. area. Learn more, or request a free trial, at Shevirah.com.

Selected recognition & awards for Shevirah and its founder	
• **Published**	**- Penetration Testing - A Hands-On Introduction to Hacking**
• **Graduated**	**- MACH37 Cyber Accelerator, VA**
• **Awarded**	**- DARPA funds**
• **Awarded**	**- Commonwealth Research Commercialization Funds, VA**
• **Awarded**	**- "Women's Society of CyberJutsu Pentest Ninja", VA**
• **Named**	**- "20 Hottest East Coast Startups", MAVA TechBUZZ, D.C.**
• **Named**	**- "30 Most Promising Startups", Virginia Velocity Tour, VA**
• **Named**	**- "40 Cyber Innovators", DCA Live, D.C**
• **Finalist**	**- "Startup Arlington", VA**

1 "Cisco sends its employees fake phishing emails to train them not to click on malicious links" businessinsider.com/cisco-chief-information-security-officer-strategy-for-fighting-cyber-attacks-2017-9/#kill-your-click-throughs-1
2 "Mobile users three times more vulnerable to phishing attacks" securityintelligence.com/mobile-users-3-times-more-vulnerable-to-phishing-attacks/