

Your internet-facing systems are always visible, often targeted first. Our service simulates a real-world attack from an outsider's perspective, identifying how external assets could be exploited before malicious actors do.

## See What Attackers See. Fix What Matters First.



With a methodology grounded in industry best practices and real-world tactics, we deliver clarity on your exposure, and the steps needed to close it:

**Public IPs & Network Services:**

Assess open ports, outdated services, and exposed infrastructure.

**Remote Access Points:**

Test the security of VPNs, RDP, and other remote connectivity mechanisms.

**Web Applications & APIs:**

Identify vulnerabilities in login portals, forms, and exposed APIs.

**Authentication & Session Handling:**

Attempt to bypass or exploit login mechanisms and access controls.

**Third-Party & Vendor Exposure:**

Evaluate risk from connected external platforms or partner integrations.

## WHY CHOOSE US?

**Real-World Attacker Perspective:**

We replicate post-compromise behavior, not just scan for surface flaws.

**Manual Testing Where It Matters:**

Our security engineers go beyond tools—validating, escalating, and analyzing manually.

**Risk-Aligned Reporting:**

Our findings are prioritized by exploitability and business impact, not just severity score.

**Trusted by Regulated Organizations:**

DigitalEra supports clients across finance, healthcare, government, and other high-compliance sectors.

## OUTCOMES YOU CAN EXPECT

- A prioritized list of vulnerabilities and exposures
- Realistic view of your external attack surface
- Actionable remediation steps for high-risk issues
- Executive and technical reporting deliverables
- Enhanced preparedness for audits and compliance reviews

## EMPOWERING YOUR **SECURITY** OPERATIONS

- ✓ Full Technical Report with Findings & Risk Ratings
- ✓ Executive Summary for Non-Technical Audiences
- ✓ Detailed Remediation Plan with Prioritized Actions
- ✓ Debrief Session with Security Experts
- ✓ Optional Re-Test Assessment and Report