

VULNERABILITY MANAGEMENT PROGRAM (VMP)

Identify your weak spots and slash your cyber risk.

In the modern threat landscape, you need actionable threat intelligence for all your network assets across each attack surface, including traditional, cloud, mobile, and DevOps environments. By integrating the Atomic Data Vulnerability Management Program (VMP) into your security plan, you'll address hidden security flaws before they wreak havoc on your network.

Custom-tailored vulnerability management how and when you want.



With leading vulnerability detection tools and 24x7x365 NSOC incident response, we provide comprehensive vulnerability management that delivers more value and less risk than a standalone scanning solution. We'll tailor a VMP to your governance objectives, security standards, and compliance requirements.

- ✓ Network & Asset Scanning
- ✓ Active Directory Reports
- ✓ Compliance Standards
- ✓ Unlimited Device Coverage
- ✓ Custom Scan Frequency
- ✓ Azure Active Directory Reports
- ✓ Custom Remediation (including immediate)
- ✓ External Scanning



2022 TOP EXPLOITED VULNERABILITIES

| | | |
|------------|------------|------------|
| Log4Shell | ProxyShell | PetitPotam |
| ProxyLogon | ZeroLogon | Follina |



One-time assessment followed by an ongoing management program.

INITIAL ASSESSMENT

- Assessment agent deployed
- Network scanned
- Program run for up to one week
- Report presented to client



ONGOING PROGRAM

- Probe deployed
- Agent deployed on each device
- Network scanned
- Customized scanning schedules
- Security-based reports
- Client access to program portal