PENETRATION TEST SUMMARY

CONFIDENTIAL - REDACTED VERSION

Aftershock Cyber Solutions

⚠️ **This is a redacted version for public trust center display. Full report available under NDA.**

Executive Summary

Aftershock Cyber Solutions engaged [redacted] to conduct an external penetration test of our Azure cloud infrastructure and web applications. The assessment was performed to identify security vulnerabilities and validate our security controls.

The testing team successfully identified and validated several security findings, all of which have been addressed or are in active remediation. No critical vulnerabilities were exploited during testing.

Test Details

Test Period:	October 1-5, 2025
Testing Firm:	[redacted]
Lead Tester:	[redacted]
Test Type:	External Black Box Penetration Test
Scope:	Azure Cloud Infrastructure, Web Applications, APIs
Methodology:	OWASP Testing Guide, PTES, NIST SP 800-115

Findings Summary

Severity	Count	Status
Critical	0	N/A
High	2	Remediated
Medium	4	In Progress (Target: Nov 15, 2025)
Low	7	Accepted Risk / Scheduled
Informational	3	Noted

Key Findings (Redacted)

High Severity - Remediated

H-01: [redacted]

Impact: Potential unauthorized access to [redacted]
Remediation: Implemented MFA and conditional access policies. Verified October 8, 2025.

H-02: [redacted]

Impact: Information disclosure risk
Remediation: Updated security headers and API configurations. Verified October 10, 2025.

Medium Severity - In Progress

M-01: Missing security headers on [redacted] endpoints

Target Date: November 1, 2025

M-02: [redacted]

Target Date: November 15, 2025

M-03 & M-04: Additional findings under remediation

Positive Findings

- ✅ Strong network segmentation and firewall rules
- ✅ Properly configured Azure Security Center with active monitoring
- ✅ No SQL injection vulnerabilities identified
- ✅ No cross-site scripting (XSS) vulnerabilities in tested applications
- ✅ Secure authentication mechanisms with MFA enforcement
- ✅ Proper encryption in transit (TLS 1.2+)
- ✅ Regular patching and update procedures in place
- ✅ Incident response procedures documented and tested

Recommendations

1. Continue prioritizing remediation of medium-severity findings
2. Implement automated security scanning in CI/CD pipeline
3. Conduct quarterly vulnerability assessments
4. Enhance security awareness training for development teams
5. Consider bug bounty program for continuous security validation

Conclusion

The penetration test demonstrated that Aftershock Cyber Solutions maintains a strong security posture with no critical vulnerabilities identified. The organization has shown commitment to security through rapid remediation of high-severity findings and ongoing efforts to address medium and low-severity issues.

We recommend annual penetration testing with quarterly vulnerability assessments to maintain this security posture as the infrastructure evolves.

Document Classification: Confidential - Redacted for Public Display

Report Date: October 15, 2025

Next Test Scheduled: October 2026