[redacted]

2026 Supplemental Documentation & Letter of Attestation

2026 / Version 1

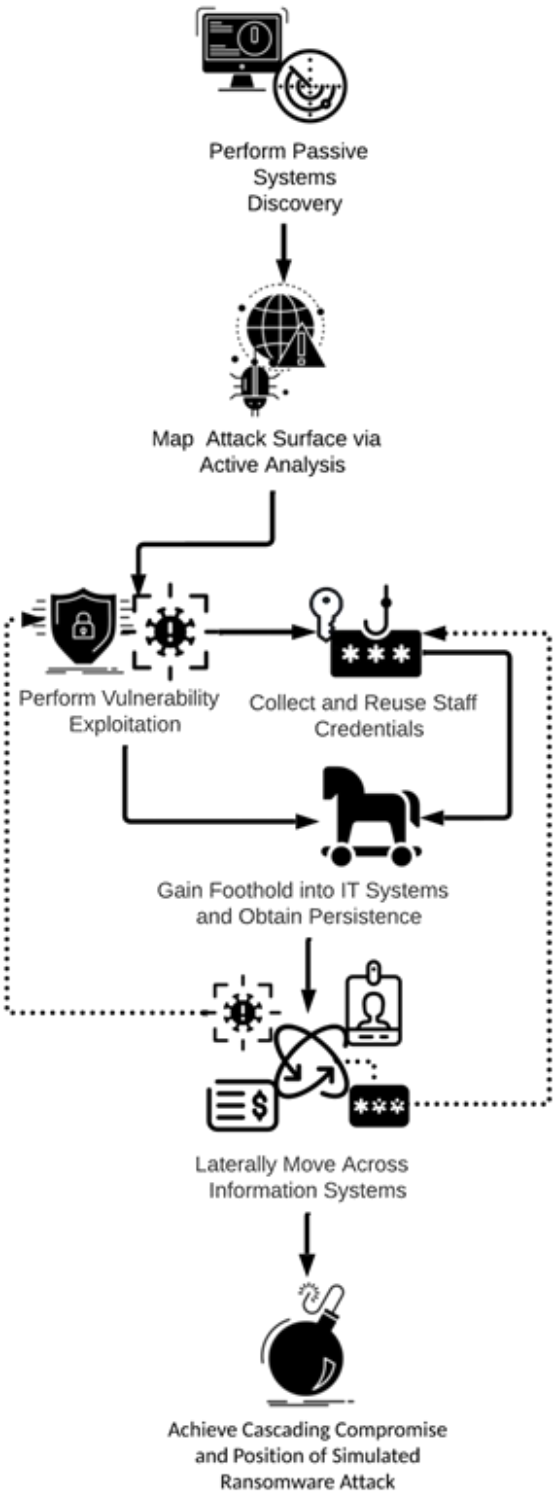
Security Testing Scope:

[redacted] contracted Abacus to perform an Artificial Intelligence (AI) enabled penetration test on internal infrastructure between the dates of April 1st, 2026, and April 17th, 2026, on [redacted]

Objectives of this Engagement:

- Leverage AI-enabled penetration testing to identify high-risk security gaps in [redacted] internal information systems and technical security controls.
- Replicate the vantage point and attack vectors of a malicious actor who has breached [redacted] externally facing perimeter and is trying to laterally move across [redacted] internal information systems.
- Bring attention to the weakest areas of the [redacted] security posture by leveraging AI-driven exploitation of the highest risk security gaps and attack vectors present across the [redacted] internal network.
- Deliver comprehensive due diligence documentation to [redacted] encompassing detailed vulnerability insights, risk mitigation strategies, reconnaissance methodologies, exploitation techniques, system metrics, compromised credentials, acquired configuration files, kill-chain and network diagrams, and more. This information is presented through a combination of AI-driven penetration testing reports and supplemental documentation, enriched with expert analysis and interpretation by Abacus security engineers.

Security Testing Methodology

Pentesting Phases	MITRE ATT&CK Tactics	Abacus Group's Standard Kill Chain
Conduct Organizational Reconnaissance	Reconnaissance TA0043	
Conduct Intelligence Gathering	Resource Development TA0042	
Analyze the Attack Surface		
Conduct Initial Exploitation	Initial Access TA0001	
Establish a Foothold	Execution TA0002	
	Persistence TA0003	
	Defense Evasion TA005	
Conduct Lateral Movement	Lateral Movement TA0008	
Privilege Escalation	Privilege Escalation TA0004	
	Discovery TA0007	
	Collection TA0009	
Establish Command and Control	Command and Control TA0011	
Demonstrate the Practical Impact	Impact TA0040	

Abacus Observations and Supplemental Information

Based on the results from the AI-enabled penetration test, Abacus has included additional information for further explanation and interpretation. This information is meant to supplement what was identified as a result of the penetration test. [redacted] should bear the additional information in mind when considering risk mitigations.

External Network Penetration Test Finding One: Scoring Adjustment:

- Finding: **SMB Signing Not Required**
- Overall Severity Rating: **High**
  - Additional Justification: The identified weakness does pose a high impact for [redacted] While this finding is normally regarded as a moderate vulnerability, due to the number of devices affected, it has been changed to a High. An attacker could exploit this misconfiguration by performing man-in-the-middle attacks, where they intercept, alter, and relay Server Message Block (SMB) messages between the client and server without detection.

Internal Network Penetration Test Finding One: Scoring Adjustment:

- Finding: **Expired SSL/TLS Certificate**
- Overall Severity Rating: **Informational**
  - Deconfliction Reasoning: The identified weakness does not pose a significant impact for [redacted] While this does not pose a significant impact since this only affects internal applications, an attacker can take advantage of this by launching man-in-the-middle attacks using a fraudulent certificate and trick users into divulging confidential information.

Enclosures:

1. action_logs.csv
2. activedir_passwords.csv
3. certificates.csv
4. credentials.csv
5. data_stores.csv
6. database_repos.csv
7. docker_registries.csv
8. exec-summary-report.pdf
9. external_domains.csv
10. file_shares.csv
11. fix-actions-report.pdf
12. git-repos.csv
13. hosts.csv
14. iam_roles_aws.csv
15. iam_roles_azure.csv
16. impacts.csv
17. pentest-report.pdf
18. s3-buckets.csv
19. segmentation-report.pdf
20. services.csv
21. users.csv
22. weaknesses.csv
23. websites.csv

Security Testing Results

While Abacus makes a best effort to rank the severity of vulnerabilities, it is not possible for any assessment to guarantee that low-risk issues cannot be chained together and significantly impact [redacted] systems. All risk ratings in this report are a combination of industry-standard ratings and considerations for unique business risk as identified by Abacus. Special consideration should also be given to the fact that multiple low-risk issues may compound into higher-risk threats.

As a result of the engagement, the following was discovered:

- 2 High Risks
- 1 Moderate Risks
- 2 Low Risks
- 1 Informational Risks

Abacus Group completed the internal network penetration testing activities, identifying two high-risk findings, one moderate-risk finding, and two low-risk findings. From an internal perspective, [redacted] attack surface presented two avenues for practical exploitation. The identification and exploitation of IPMI 2.0 exploits RAKP authentication that allows an attacker to obtain password hashes and conduct offline password guessing attacks by obtaining the HMAC from a RAKP message. Ultimately, once these password hashes are cracked, the attacker can gain control of the management interface of the affected systems.

Abacus performed testing in accordance with NIST SP800-115 (Technical Guide to Information Security Testing and Assessment), PTES (Penetration Testing Execution Standard), Open Web Application Security Project (OWASP) guidelines, and the MITRE ATT&CK framework. The findings in this report are not necessarily exhaustive; they are limited to IT system targets within the signed Rules of Engagement (RoE) scope or directly approved by [redacted] point of contact during the engagement. Furthermore, resource restrictions and the need to avoid disrupting business operations limit the testing that may be performed.

This report reflects [redacted] security posture, as seen during the dates in which the security testing was conducted. Future changes to any applications or infrastructure will alter the security position of the environment from its current state. Additionally, as time passes, new types of attacks may arise which were previously unknown to the security industry. Considering this, Abacus always recommends that all information systems undergo recurring security testing within a reasonable timeframe.

Date of Attestation Letter: April 17th, 2026

Dane Piazza

Director, Security Testing & Vulnerability Management
Abacustechnology.com | 212-696-0500
655 Third Avenue, 8th Floor, New York, NY 10017

About the Security Testers:

Founded in 2008, Abacus is an innovative, award-winning IT and Cybersecurity managed service provider offering an enterprise integrated platform specifically designed for the unique needs of the financial services industry. Abacus's Red Team has deep industry expertise that provides high-quality security testing and continuous monitoring which is tailored to meet the unique needs of financial & healthcare services firms against evolving threats and compliance demands.