VONAHI SECURITY

CAIT Internal w/ VulScan

EXECUTIVE SUMMARY

CAITDMZ

February 03, 2026

Copyright

© Vonahi Security. All Rights Reserved. This is unpublished material and contains trade secrets and other confidential information and is subject to a confidentiality agreement. The unauthorized possession, use, reproduction, distribution, display, or disclosure of this material or the information contained herein is prohibited.

The methodology used to audit the computer systems is considered proprietary intellectual information of Vonahi Security and may not be disclosed without written permission from Vonahi Security. Vonahi Security gives permission to copy this report for the purpose of disseminating information within your organization, or any regulatory agency.

Confidentiality

This document contains organization confidential information of a proprietary and sensitive nature. As such, this document should be afforded the security and handling precautions that a confidential document warrants. This document should have a controlled distribution to relevant parties only and should not be copied without written permission. Vonahi Security treats the contents of a security audit as organization confidential material and will not disclose the contents of this document to anyone without written permission.

Assessment Project Team

Below is a list of contacts that were involved in this engagement. Should you have any questions pertaining to the content of this document or any project and non-project-related items, please feel free to reach out to the necessary project contacts.

Primary Point of Contact	
Name:	Alton Johnson
Title:	Principal Security Consultant
Office:	(844) 866-2732
Email:	support@vpentest.io

Executive Summary

CAITDMZ has requested the assistance of Vonahi Security to perform a comprehensive security assessment to assist with evaluating the cyber risks presented within the tested environment(s). The objective of this engagement was to determine if any identified threats could be used to mount an attack against the organization that could lead to the disclosure of sensitive information or access to critical information systems.

Included in this Executive Summary report is a high-level overview of the results that were observed during this assessment. A copy of more specific information pertaining to technical findings and remediation details are documented within the Technical Report.

Engagement Scope of Work

Prior to beginning the assessment, Vonahi Security and CAITDMZ agreed to a scope of work to define the specific assessment phases. The table below outlines the engagement scope of work and details entailed within each assessment phase that was conducted as part of this engagement.

Assessment Component	Assessment Phases
Internal Network Penetration Test	This assessment attempted to identify security threats that are exposed on the internal network environment. Threats identified within the internal environment are usually less severe than those of the external environment due to the limited exposure. → **Internal Network Penetration Test** - A penetration test was conducted to identify the potential impact of exploiting any identified vulnerabilities. Only exploits that are deemed safe were executed during this phase.

Engagement Statistics

The information below displays overall statistics that were recorded as part of this engagement. Following the statistics, Vonahi Security has summarized all of the threats identified.

Internal Network Penetration Test

The information below provides a high-level overview of the assessment results recorded as part of this engagement. Following this section is a summary of all the threats identified and their potential risk to your organization.

Overall Severity Ranking



ASSESSMENT SCHEDULE

Tue, February 03, 2026
12:08 AM ET

Immediate remediation or mitigation is required. Exploitation of identified vulnerabilities require minimal effort from an attacker and pose a significant threat. A successful attack could result in unauthorized access to systems and/or valuable data.

Engagement Results Charts

To help CAITDMZ understand the severity of the threats identified during testing, Vonahi Security has included an over-all summary chart below that displays a comparison of the report findings as well as the vulnerabilities that were discovered.

Internal Network Penetration Test Results



PenTest Findings

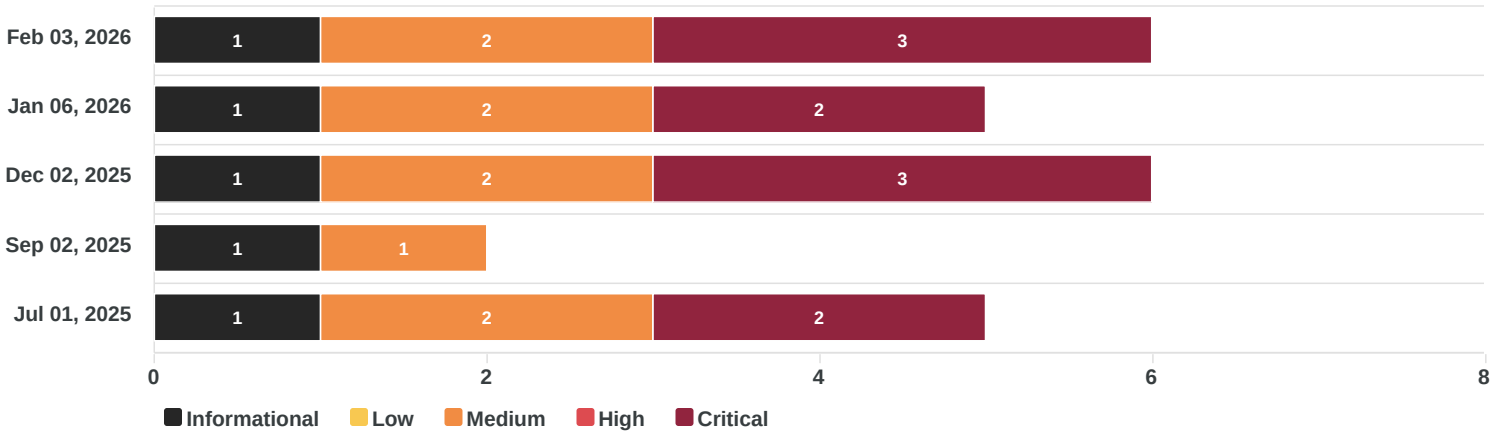
The following chart displays the overall severity of the report findings that were documented as part of the penetration testing efforts.

C	3	CRITICAL	H	0	HIGH
M	2	MEDIUM	L	0	LOW
I	1	INFO			

Comparison Charts

To help CAITDMZ understand the trend of the PenTest Findings and vulnerabilities discovered in the past as part of this on-going engagement, Vonahi Security has provided trend data in this section of the report.

History of PenTest Findings



Engagement Results Summary

To summarize the results, Vonahi Security has grouped all of the findings from the penetration test into rollup findings. These rollup findings can be used to quickly determine the root cause of the issues identified in the technical report. By implementing a remediation strategy for the findings based on the rollup issues identified below, CAITDMZ's security posture would be greatly improved.

Internal Network Penetration Test

Category	Summary
Configuration Deficiencies	Configuration weaknesses were identified that could potentially lead to a successful compromise of systems and/or data within the tested environment. Although some of the configuration weaknesses may be exploitable in limited circumstances, the potential impact of a successful attack could be relatively high.
Egress Filtering Deficiencies	Testing identified that excessive services are accessible on the public Internet from the internal network environment. This could allow for an attacker to circumvent security controls by using alternative communication channels. Furthermore, a compromised system may be able to use such alternative communication channels to exfiltrate sensitive information.

Remediation Roadmap

For each assessment conducted, Vonahi Security provided a remediation roadmap to help CAITDMZ understand the issues within the respective environment and the overall remediation strategies that should be implemented to resolve the issues identified during the penetration test. It should be noted that the remediation strategies below apply to multiple issues identified within the technical report and can greatly reduce the overall attack surface once successfully implemented.

Internal Network Penetration Test

Issue	Remediation Strategy
Configuration Deficiencies	Implement or improve a security configuration baseline that adheres to security best practices and industry standards such as National Institute of Standards and Technology (NIST). This security configuration baseline should ensure that no services and/or systems are deployed within the environment until a thorough configuration review has been performed.
Egress Filtering Deficiencies	Ensure that the organization's network firewalls restrict outbound access to the public Internet to services that are required for business operations. For services that are required for business operations, the organization should document these in a policy and procedure so that business justifications are communicated and understood within the organization. Any adjustments to these configurations should be documented in a change management program to establish an audit trail.