PROXIT, INC.
PROPOSAL FOR SERVICES

July 31, 2025

OVERVIEW

Proxit, Inc. is pleased to submit this proposal for services to support the Village of Thornton. The purpose of this proposal is to assist the Village with Cybersecurity evaluation and analysis of the existing networking infrastructure. Our approach to this process is three tiers.

Tier One is tactical. This involves vulnerability scanning and reporting of network attached systems. Devices are scanned and their current state is compared to the current list of published Common Vulnerabilities and Exposures (CVEs). The reporting from this process provides a road map for elimination for know attack vectors that could be used by malicious actors from inside or outside the network perimeter.

Tier Two is strategic. This process evaluates operational policies and compliance with those policies such as; password protections, multifactor authentication compliance, implementation of defense, in depth processes for backup and recovery and other best practices.

Tier Three is proactive management processes. This includes: Business continuity, Disaster recovery, Incident response, and standards compliance.

This is a Tier One Proposal.

The Objective

Identify devices that require updates, patches or replacement in order to protect those devices from being exploited. In the current environment, malicious actors find a way to take control over an internal device. This is not always a personal computer. It can be any device running software and connected to the network such as a camera, a sensor, or even a Ring doorbell. Once that happens they explore your network looking for devices with known vulnerabilities to exploit. Vulnerability scans performed at least annually meets the requirements of Cybersecurity insurance policies and reduces the probability of a successful attack.

OUR PROPOSAL

Vulnerability assessment has a three-step process:

Step 1. The scope of the vulnerability assessment is determined by identifying the sensitive data storage areas, the systems running on a network, internet-facing assets, and devices.

Step 2. An automated vulnerability scanner is engaged to root out all the potential vulnerabilities in the systems within the scope of the assessment.

Step 3. A security vulnerability assessment report is prepared with analytical information on the vulnerabilities found, segregate the false positives from genuine issues, rank the severity and risk score of the vulnerabilities, provide the possible ways to remove those issues, etc.

The Village will be able to use this information to address the issues identified and strengthen the security of devices and the overall infrastructure.

Technical/Project Approach

Pretest Planning

An initial meeting is required to collect information required for a proper scan. For an internal scan this includes: IP address range, credentials to login to devices and execute data collection, physical logistics and timing of the scan.

The Village agrees to provide administrator or full access logins to all devices, including Microsoft Domain, firewall, switches, servers not part of the domain and other devices identified during the discovery process.

Scanning Process

This is an unobtrusive process. Each device will need to be powered on and available during the scanning window. The automated scan will take a significant amount of time (up to a full day) depending on the number of devices and may be schooled to run more than once.

Reporting and Analysis

Once completed, a group of reports will be produce along with a summary report of recommended actions

Resources

The tool used in this process is NESSUS PROFESSIONAL.

NESSUS IS #1 IN VULNERABILITY ASSESSMENT

#1 in Accuracy Nessus has the industry's lowest false positive rate with sixsigma accuracy (measured at .32 defects per 1 million scans).

#1 in Coverage Nessus has the deepest and broadest coverage with more than 62,000 CVE and over 100 new plugins released weekly within 24 hours of vulnerability disclosure.

#1 in Adoption Nessus is trusted by more than 30,000 organizations globally. 50% of the Fortune 500 and more than 30% of the Global 2000 rely on Nessus technology

Project Deliverables

Following is a complete list of all project deliverables:

Deliverable	Description
Reporting.	HTML report with drill down links
Raw Data	Comma delimited file for further analysis
Summary Review	Report and presentation of results and opportunity to discuss action items

This meets the requirements generally referred to in Cyber insurance policies and as request by others such as the Illinois secretary of state, and state of Illinois DOIT support of LEADS 3.0

Timeline for Execution

Description	Start Date	End Date	Duration
Initial Meeting and setup			2-4 hours
Subnet Scan			One per day
Analysis			Off Site 2-5 days
Review Meeting			

Generally this process takes three to four weeks from initial meeting to review meeting.

PRICING

The cost of this project is $5,000 with 50% billed on the date of the initial meeting. Payment due within 45 days.

The remainder will be billed the final review meeting. A credit for the second installed will be issued should the Village contract with Proxit for recurring services within 60 days of the final report.

A Purchase Order in the amount of the $5,000.00 is requested. W-9 Attached

Please contact me with any questions or to discuss this proposal.

Bradley Gordon

Proxit, Inc.

708 860 4725