EXHIBIT A

Statement of Work #003

Prepared for

Village of Orland Park, Illinois

Managed Detection and Response Services

Date Submitted: August 13, 2025

Submitted by Computer Aid, Inc.

CAI Headquarters
1390 Ridgeview Drive
Suite 300
Allentown PA 18104-9065

Table of Contents

CAI Headquarters
1390 Ridgeview Drive
Suite 300
Allentown PA 18104-9065

1. Executive Overview

Computer Aid, Inc. ("CAI") is pleased to provide this Statement of Work ("SOW") to Village of Orland Park ("Village" or "Client") for Information Technology services. This SOW is subject to the terms and conditions of the Master Services Agreement ("Agreement") between CAI and Village, effective Month Day, Year. No terms in this SOW take precedence over the Master Services Agreement unless explicitly noted. The terms and conditions and pricing set forth in this SOW are valid until December 31, 2025.

2. Term

This is an extension of the services outlined in SOW001 executed on January 24, 2025. The estimated Duration to complete this SOW is three (3) years with two optional renewal years.

The term of this Statement of Work is defined by the Duration and can be revised by a change request mutually agreed upon by both parties following the **APPENDIX B | CHANGE CONTROL** process.

3. Scope of Services

3.1. Description

CAI will provide cybersecurity advisory services in support of strategic initiatives by providing Managed Detection and Response (MDR) Services

3.1.1. Business Objectives

The following are the primary business objectives of providing MDR solutions:

- Protect Village, employee, and customer data.
- Identify areas where threat actors are actively identifying vulnerabilities
- Improve security operations through 24x7x365 monitoring for advance threat, detection, and response.

3.1.2. Requirements and Success Indicators

The requirements and primary success indicators include:

- Ability to provide 24x7x365 security monitoring
- Real-time responsiveness to threats or anomalies within an agreed upon timeframe to minimize impact
- Tracking and reporting of network security activity
- On-going upgrading and patches of the SOC monitoring solution against latest threats and vulnerabilities

3.2. Scope

3.2.1. Requested Services

CAI shall provide the LMNTRIX Adaptive Threat Response (ATR) security services listed below and detailed by this SOW:

Detect Sensor

- Provide the ATR Continuous Detection which is comprised of service elements: (1) LMNTRIX Detect, (2) LMNTRIX Intelligence

CAI Headquarters
1390 Ridgeview Drive
Suite 300
Allentown PA 18104-9065

- Provide one (1) or more instances of on-premises Multi-Threat Detection Sensor(s) (virtual system) or physical appliance with support for up to 24 cores.
- Provide hourly ingest of predictive intelligence exchange (PIE) feed into the Detect platform.
- Maintain and update information for ATR Portal

Response Agents

- Provide ATR Continuous Response comprised of service elements: (1) LMNTRIX Detect, (2) LMNTRIX Intelligence, (3) LMNTRIX Respond.
- Deploy Advanced Endpoint Threat Detection & Response (EDR) agents on up to 415 endpoints.
- Provide hourly ingest of predictive intelligence exchange (PIE) feed into the Detect and Respond platforms.
- Provide Breach Validation & Containment as required.
- Provide Proactive Threat Hunting (endpoint) as required.
- Maintain and update information for ATR Portal

ThinkGrid

- Provide one (1) or more Security Data Aggregators (SDA's) on Village's premises to capture logs, net flow, metadata, or truncated flows and forward them to the ThinkGrid platform hosted on the LMNTRIX Cloud.
- SIEM replacement providing open-source search and analytics engine enabling scalability and reliance.

3.2.2. Optional Services

Additional MDR services may be requested. If the Village desires these optional services, they will be quoted through a change order or new SOW.

Please see **APPENDIX B | CHANGE CONTROL** for change request form.

3.3. Approach

Please see **APPENDIX A | APPROACH** for detailed approach as well as monitoring and service delivery.

3.4. Timeline

The project start date will be 01/24/2026. The services will extend for one (3) calendar years and will be subject to annual renewal for up to five (5) years.

3.5. Roles

3.5.1. CAI / LMNTRIX Team Roles

Role	Key Activities / Responsibilities
CAI Service Delivery Manager	CAI will provide resources required to perform the following: • Financial management of the services • Village relationship management

CAI Headquarters
1390 Ridgeview Drive
Suite 300
Allentown PA 18104-9065

	• Consult on issue and risk escalation • Other duties as required
CAI Cybersecurity Lead	CAI will provide resources required to perform the following: • Quality Assurance • Liaison as needed with LMTNRIX • Coordination with Village Leadership • Oversee the CAI Service Team • Provide subject matter expertise • Other duties as required
Project Manager	CAI will provide resources required to perform the following: • Participate as a PM with the CAI Support Team • Adaptive Threat Response (ATR) security services as described above • Provide a single point of contact ("Project Manager" or “PM”) for all issues relating to the ATR Services delivered within the scope of this Service. Such person shall be identified and shall be available during Standard Business Hours. • Designate a backup contact when the Project Manager is not available. • Define the communication flow with Village’s project sponsor and key stakeholders. • Participate in regularly scheduled meetings with Village to discuss the status of the service, identify and document dependencies, risks and issues associated with the successful delivery of the service. • Act as the focal point for change management procedures.
Incident Manager	CAI will provide resources required to perform the following: • Participate as the Incident Manager within the CAI Service Team • Support the Adaptive Threat Response (ATR) security services as described above • Primary point of contact in the event of a security incident detected by the ATR solution • Participate in regularly scheduled meetings with Village to discuss the status of the service, identify and document dependencies, risks and issues associated with the successful delivery of the service.
Security Analyst	CAI will provide resources required to perform the following: • Participate as Security Analyst with the CAI Service Team • Perform functions in the Cyber Defense Center (CDC) to include • Support the Adaptive Threat Response (ATR) security services as described above. • Participate in regularly scheduled meetings with Village to discuss the status of the service, identify and document dependencies, risks and issues associated with the successful delivery of the service.

CAI Headquarters
1390 Ridgeview Drive
Suite 300
Allentown PA 18104-9065

Figure 1: CAI/LMNTRIX Roles

3.5.2. Village Team Roles

Role	Commitment	Key Activities / Responsibilities
Project Sponsor – Director of Information Technology	Participation as needed	Village will provide resources required to perform the following: • Serve as the primary source of sponsorship and business vision • Responsible for project communication and organizational mobilization • Responsible for escalated issue resolution • Updated regularly regarding status and critical decisions over the course of the engagement • Help evaluate options and resolve escalated business issues • Assist with communications and be a visible champion for the project • Designate a single point of contact to whom all The CAI Service Team communications may be addressed and who has authority to act on all aspects of the ATR services. • Designate a backup, or secondary, contact that has the authority to act on all aspects of the Services in the absence of the primary contact. • Identify a project sponsor and key stakeholders and define their roles in supporting this project.
Security Point of Contact	Participation as needed	Village will provide resources required to perform the following: • Participate in regularly scheduled project review meetings or conference calls. • Review the project schedule, objectives, services, and roles and responsibilities with the CAI Service Team. • Work with the CAI Cybersecurity Lead and CAI Service Team PM to ensure Village's project sponsor, key stakeholders and all project team members receive project communications and are included in regularly scheduled communications sessions.

CAI Headquarters
1390 Ridgeview Drive
Suite 300
Allentown PA 18104-9065

		• Work with the CAI Cybersecurity Lead and CAI Service Team PM to schedule the kick-off meeting and communicate the meeting schedule to the Village- identified stakeholders. • Provide information and documentation required by the CAI Service Team within a timely manner to maintain project schedules. • Notify the CAI Service Team of any Hardware and/or Software upgrades that relate to the delivery of the Services or any other change within Village's current network that relate to the delivery of the Services at least ten (10) business days prior to such upgrade. • Notify the CAI Service Team of any scheduled implementation activities within ten (10) business days of the scheduled activity. • Notify the CAI Service Team of any installation scheduling change at least seventy-two (72) hours prior to the originally scheduled installation date. • Notify the CAI Service Team of any scheduling changes related to this Term at least ten (10) business days of the scheduled activity. • Schedule the necessary facilities and access for on-site meetings (such as: badge or visitor access, conference rooms, projectors and conference bridges).
Network Team	Participation as Needed	• Assist in the implementation of ATR devices for the solution on the Village network • Assist with any onsite activities (e.g. hardware resets, device installation, replacement) • Provide support as required

Figure 2: Client Roles

4. Pricing

CAI will invoice Village monthly for the services presented in this SOW. See tables below for details:

4.1. Service Fees

As part of the agreement with LMTRIX, Village will be provided the first 30 days of service at no charge. Allowing for a trial of the ATR services and proof of concept. After the trial period of 30 days, the project will be delivered at the service fees listed in the table below.

CAI Headquarters
1390 Ridgeview Drive
Suite 300
Allentown PA 18104-9065

Service Options		Annual Cost	Monthly Cost	Selection
Current Environment	LMNTRIX Detect600 Network Sensor	$211,298.58	$17,608.21	☐
	LMNTRIX Intelligence			
	LMNTRIX Respond Endpoints (415)			
	ThinkGrid SIEM 10GB (Cloud-Based)			
20GB Daily Ingestion	LMNTRIX Detect600 Network Sensor	$235,911.85	$19,659.32	☐
	LMNTRIX Intelligence			
	LMNTRIX Respond Endpoints (415)			
	ThinkGrid SIEM 20GB (Cloud-Based)			
50 GB Daily Ingestion	LMNTRIX Detect600 Network Sensor	$301,445.19	$25,120.43	☐
	LMNTRIX Intelligence			
	LMNTRIX Respond Endpoints (415)			
	ThinkGrid SIEM 50GB (Cloud-Based)			

Figure 3: MDR Pricing Options

4.2. Expenses

CAI anticipates no additional travel or expenses in the delivery of this SOW. In the event of required travel, CAI required travel and other expenses shall be in accordance with Village expense and travel policy. CAI will use commercially reasonable efforts to limit the need for travel and minimize expenses. All instances of travel or expenses must be pre-approved in writing by the Village.

5. Change Control

Any changes in Scope of Services or Assumptions in connection with this SOW will be documented in a change order, see **APPENDIX B | CHANGE CONTROL**, signed by CAI and Village prior to the start of any such services.

CAI Headquarters
1390 Ridgeview Drive
Suite 300
Allentown PA 18104-9065

6. Notice to Proceed

This Statement of Work, effective date January 25, 2026, for CAI to provide Village with services as described above Statement of Work and Pricing sections, is hereby submitted for approval.

The parties acknowledge that they have read this document, understand it, and agree in principle to be bound by its terms and conditions. Further, the parties agree that this document, and the terms and conditions contained in the Master Agreement represent the final binding agreement between CAI and Village. In addition, the parties agree that, if a conflict should arise between the MSA and this SOW, the order of precedence for resolving issues shall be the MSA followed by this SOW unless clearly stated in the SOW.

This Notice to Proceed will serve as acceptance of this SOW, as set forth in this document, and will represent the definitive terms and conditions of the agreement between the parties.

The content and terms outlined in this SOW are valid through 01/24/26. If not executed by both parties on or prior to this date, this SOW is deemed to be invalid, and CAI may reevaluate the content and terms before providing a new SOW for consideration.

Village of Orland Park	Computer Aid, Inc.
By	**By**
Name	**Name** Abe Hunter
Title	**Title** President and Chief Revenue Officer
Date	**Date**

CAI Headquarters
1390 Ridgeview Drive
Suite 300
Allentown PA 18104-9065

Appendix A | Approach

The CAI Service Team is currently providing the ATR services to the Village. In the event of a SIEM upgrade from the current 10 GB daily ingestion, the CAI Services Team will coordinate with the appropriate personnel to provide the upgrade. Monitoring and Service Delivery will continue as described below.

Monitoring and Service Delivery

The CAI Service Team CDC will proactively monitor for key Security Incidents and thresholds in Village's network infrastructure. Monitoring will begin following Transition Out brief; Telemetry Tuning may be provided at any point during Service Delivery.

In the case of undetected Security Incidents, Village may declare a Security Incident by contacting the CDC, communicating via telephone any high priority Incidents (system down, degraded performance, etc.). Low priority incidents should be reported to the CDC via the ATR Portal (described in Section 1.4.3).

Upon automatic detection or manual submission of an Incident to the CDC, an Incident Ticket is created. The CDC is ultimately responsible for coordinating the management of the Incident, which includes communicating with Village throughout the Incident management process. This communication also includes notification to Village that the Incident has been resolved or remediated.

CAI Service Team Responsibilities:

- Create Incident Tickets on the ATR Portal.
- Classify each Security Incident into security category. Categories are based on a modified version of the US-CERT incident categories: http://www.us-cert.gov/government-users/reporting-requirements
- Prioritize all Incidents into High, Medium, and Low priority based on several criteria such as the type of infection, confirmation of the incident, identification of a human adversary on the network, or the number of assets associated with the Incident. Priorities are defined as:
    - **High**: Critical business impact or data loss to Village.
    - **Medium**: Adverse effect to Village, potential data loss, potential loss of service.
    - **Low**: Minimal adverse impact to Village. No financial loss. No data loss.
- Electronically notify designated Village contacts for new incidents via ATR Portal
- Provide mitigation recommendations as available for associated Security Incident

Village Responsibilities:

- Review Incident Tickets on the ATR Portal and provide details for ticket closure.
- Implement recommended mitigation techniques, if available.

Time to Begin Analysis.

The CAI Service Team will begin analysis of an Alert within the times set forth in the table below, calculated from the time the Alert was generated by the Service Element (as applicable).

Alerts Investigated.

CAI Headquarters
1390 Ridgeview Drive
Suite 300
Allentown PA 18104-9065

The CAI Service Team will investigate and report on the Alerts using the alert classification and corresponding timeline below. CAI Service Team has no obligation to investigate and report on Alerts that fall outside the purchased Subscription level.

Initial Investigation.

CAI Service Team analysts will perform an initial analysis of Village's Covered Systems to determine if the Alert is a true or false positive, benign, or suspicious activity.

Monitoring and Incident Records

The CAI Service Team is responsible for monitoring the Village environment, systems and data as defined in the information gathering exercises of the activation phase.

Activities primarily include monitoring and analyzing network, endpoint, deceptions-based data as well as threat intelligence feeds to identify potential malicious Security Incidents.

If the CAI Service Team's investigation determines that the Alert indicates a true compromise, the team will create an ATR Incident Ticket to the ATR Portal within one (1) hour of the time the team makes that determination. Regardless of whether the CAI Service Team's investigation determines that an Alert indicates a true compromise, CAI will create a ATR Incident Ticket on the Alert to the ATR Portal within the times set forth in the table below, based on the classification of the Alert (High Priority Alert, Medium Priority Alert, Low Priority Alert). Village acknowledges that in some cases, when the CAI Service Team's investigation is not complete, an ATR Incident Ticket may provide only an update of current status of the Alert investigation.

ATR Alert Classification	Time to Begin Investigation (from time Service Element generates Alert)	Time to Create ATR Incident Ticket (from time the CAI Service Team validates actual compromise)	Time to Create ATR Incident Ticket (when no validation of actual compromise; from time Service Element generates Alert)
High Priority Alert	1 hour	1 hour	24 hours
Medium Priority Alert	7 hours	1 hour	24 hours
Low Priority Alert	24 hours	1 hour	48 hours

The service levels noted in the table above will become effective thirty (30) days following the Order Effective Date, to allow time for Village to install on-premises virtual systems and/or physical appliances and for the CAI Service Team to determine the level of staffing needed to respond to Alerts in Village's environment.

Extended Investigations; Multiple Related Alerts

When the CAI Service Team has identified a true positive or suspicious activity, CAI Team analysts may perform an extended investigation, and/or may aggregate and review multiple Alerts from related Covered Systems to determine the extent of activity related to the Alert. CAI Team analysts may append results from the extended investigation or subsequent Alert investigations to the initial ATR Incident Ticket if the CAI Service Team determines that additional or subsequent Alerts are related, and in such cases, the CAI Service Team will not be required to issue a separate ATR Incident Ticket for each such related Alert.

Non-Remediable Alerts

CAI Headquarters
1390 Ridgeview Drive
Suite 300
Allentown PA 18104-9065

The CAI Service Team has no obligation to notify Village or generate a new ATR Incident Ticket on new Alerts that are directly related to previous investigations where an ATR Incident Ticket has been published and the CAI Team has provided recommended remediation steps, when Village has acknowledged the ATR Incident Ticket but chooses not to or cannot remediate the cause of these Alerts.

Alert Priority

The CAI Service Team may re-prioritize Alerts, regardless of their severity classification, to provide focus to Alerts that the CAI Service Team determines may have the largest impact to Village's environment.

Continuity of Monitoring

All monitoring, investigation and reporting activities described in this section will be provided on a 24/7/365 basis.

System Health Monitoring and Notification.

LMNTRIX does not provide system health monitoring or notification for any of the Service Elements deployed at Village Premise. To be clear, it is Village's responsibility to monitor the availability of the virtual systems and/or physical appliances for network connectivity or hardware faults.

Containment.

As Village has purchased the Continuous Response or Continuous Hunting subscription levels, these both include the Respond Service Element, for which the CAI Service Team at Village's discretion will deliver automatic exploit prevention, or when appropriate, recommend containment of the target Covered System from Village's network. Containment must be approved by Village leadership.

LMNTRIX Hunt: Telemetry Tuning

Village may also send additional Telemetry, as mutually agreed by both Village and the CAI Service Team, into the Hunting Platform to offer greater network visibility and context to active incident investigations.

The amount of additional Telemetry is limited by the original Hunting Platform telemetry thresholds as described in the Core Service Offerings overview. As the amount of data ingested by the Hunting Platform reaches the indicated storage thresholds, telemetry is rolled over with the oldest telemetry being purged to open storage for incoming telemetry. The Storage Expansion Add-On package, as described in Section Add-On Packages to Core Service Offerings", may be purchased if additional data retention is desired.

Telemetry from Village specific specialized devices or applications may require the purchase of a Development Request Add-On prior to being ingested by Hunting Platform.

CAI Service Team Responsibilities:

- Work with Village on network device discovery to understand network device roles and functions
- Prioritize Telemetry based on value to security incident monitoring
- Provide recommendations to Village on any changes required to enable the sending of Telemetry to the Hunting Platform
- Validate receipt of approved Telemetry into the Hunting Platform

Village Responsibilities:

CAI Headquarters
1390 Ridgeview Drive
Suite 300
Allentown PA 18104-9065

- Provide information required for network device discovery
- Work with the CAI Service Team to prioritize sources of telemetry
- Implement recommended changes to applicable network applications or devices in order to enable the sending of Telemetry into the Hunting Platform
- Work with the CAI Service Team to ensure Telemetry is received by the Hunting Platform

ATR Portal

The ATR Service includes a Client Portal ("ATR Portal") that will provide visibility into the delivery of the service.

During the initial setup phase, Village will receive accounts for authorized employees to access the ATR Portal. Instructions to access and navigate the ATR Portal will be provided as a part of the activation phase via video, WebEx, or onsite as determined by the CAI Service Team.

- Information available from the ATR Portal may include:
- Incident Ticket identification number – The tracking number assigned by the ATR CDC to each ticket.
- Incident Ticket opened date and time – The date the ticket was opened.
- Incident Ticket description – A brief description of the incident(s) detailed in the ticket.
- Incident Ticket status – The current status of the ticket as determined by the most recent note entered into the ticket.

CAI Service Team Responsibilities:

- Provide access to Village to dedicated ATR Portal.
- Provide accounts for authorized Village personnel to access the Portal.
- Provide instructions to access and navigate the ATR Portal. Instruction will be provided during the activation phase via video, WebEx, or onsite as determined by the CAI Service Team.

Village Responsibilities

- Determine and maintain list of authorized users with privilege to view ATR Portal.
- Review information presented in the ATR Portal

Designated Investigations Manager

A designated Investigations Manager with deep Incident analysis and investigation skills will be assigned.

This Investigations Manager will be responsible for:

- Responding to Village inquiries and assisting with Incident resolution as needed by Village
- Staying current with Village environment and relay any changes or updates to ATR CDC
- Research and observe trends at Village sites
- Follow through with Village to ensure swift resolution and closure of incidents
- Attend and lead the Monthly Technical Briefings (if applicable)
- Attend Quarterly Business Review Meetings (if applicable)

CAI Service Team Responsibilities:

CAI Headquarters
1390 Ridgeview Drive
Suite 300
Allentown PA 18104-9065

- Assign an Investigations Manager to assist Village throughout service delivery

Village Responsibilities:

- Provide the Investigations Manager with necessary information, documentation, and/or status as it relates to changes to the Village network environment monitored by the CAI Service Team

Proactive Threat Hunting (Continuous Response or Continuous Hunting)

The CAI Service Team will perform activities involving seeking out malicious activity not identified by traditional detection mechanisms. LMNTRIX Respond provides the option for endpoint hunting while LMNTRIX Hunt provides the option for network hunting.

CAI Service Team Responsibilities:

- Actively search for attacks by applying ongoing working knowledge of current threats and intelligence attributed to these threats.
- Document and update a living playbook that provides 'plays' for hunting threats specific to the Village environment
- Run plays according to frequency outlined by the CAI Service Team for each specific play. Create and prioritize an Incident Ticket if outcome of play displays evidence of a Security Incident as determined by the CAI Service Team.

Village Responsibilities:

- Review Incident Tickets created by the CAI Service Team because of a proactive play.
- Implement mitigation and/or remediation recommendations, if available.

CAI Headquarters
1390 Ridgeview Drive
Suite 300
Allentown PA 18104-9065

Appendix B | Change Control

Any changes to the scope defined in this SOW will be addressed through a Change Request ("CR"), which will be agreed to in writing by both parties. If an alteration to the Services provided in this SOW is identified by either Party; it shall be brought to the attention of the other Party's management by completing and submitting a Change Request Form. If any such change causes an increase or decrease in the cost or time required for performance of the work, the price and/or delivery schedule shall be equitably adjusted and identified within the Change Request Form. If both Parties mutually agree to implement the change in scope, the Change Request Form will be incorporated into the SOW as an addendum when signed by authorized representatives of both parties.

Change Request Form

This Change Request, when executed by both parties, will serve as an amendment to the Statement of Work entered into by the parties on the _____day of___, and shall be effective as of the date ("Date") last signed below the change authorization signatures.

<table>
<tr><th colspan="5">Change Order Form</th></tr>
<tr><td colspan="3">Submitted By:</td><td colspan="2">Change Order ID:</td></tr>
<tr><td colspan="3">Change Order Name:</td><td colspan="2">Priority (Indicate with an X)</td></tr>
<tr><td colspan="3" rowspan="2">Project Area:</td><td>High ☐</td><td>Medium ☐ Low ☐</td></tr>
<tr><td colspan="2"></td></tr>
<tr><td>Identified By:</td><td colspan="2">Assigned To:</td><td colspan="2">Date Submitted:</td></tr>
<tr><td colspan="5">Description of Proposed Change:</td></tr>
<tr><td colspan="5">Reason for Proposed Change (Benefits):</td></tr>
<tr><td colspan="5">Project Impact (Time, Cost, etc.):</td></tr>
<tr><td rowspan="2">Signoff</td><td colspan="4">Signatures</td></tr>
<tr><td colspan="4"><u>Village</u>
By: _____
Printed Name: _____
Title: _____
Date: _____

<u>Computer Aid, Inc.</u>
By: _____
Printed Name: _____
Title: _____
Date: _____</td></tr>
</table>