VILLAGE OF WESTCHESTER

Cook County, Illinois

REQUEST FOR PROPOSAL

Managed Cybersecurity Detection, Response, and Monitoring Services

Issue Date:	6/3/26
Proposals Due:	7/31/26
Submit To:	kbrockman@westchester-il.gov
Contact:	Kevin Brockman, Senior Technology Officer kbrockman@westchester-il.gov

Village of Westchester
10300 Roosevelt Road, Westchester, Illinois 60154
www.westchester-il.gov

Table of Contents

Table of Contents 2
1. Introduction and Background 4
1.1 Purpose 4
1.2 About the Village 4
1.3 Current Technology Environment 4
1.4 Statement of Need 5
2. Scope of Services 6
2.1 Managed Endpoint Detection and Response (EDR) 6
2.2 Identity Threat Detection and Response (ITDR) 6
2.3 Security Information and Event Management (SIEM) 7
2.4 Real Time Threat Analysis and Twenty Four Hour Monitoring 7
2.5 Active Response and Incident Handling 8
2.6 Reporting and Visibility 8
2.7 Service Level Objectives 8
3. Mandatory Requirements 10
3.1 Compliance and Attestation 10
3.2 Insurance Requirements 10
3.3 References and Experience 10
4. Proposal Submission Requirements 11
4.1 Format and Delivery 11
4.2 Proposal Content and Order 11
4.3 Questions and Addenda 11
4.4 Pre Proposal Conference 11
5. Cost Proposal Format 13
6. Evaluation Criteria 14
7. Contract Terms 15
7.1 Term 15
7.2 Termination for Convenience 15
7.3 Termination for Cause 15
7.4 Data Ownership and Return 15
7.5 Confidentiality and Public Records 15
7.6 Indemnification 15
8. Required Certifications 16

8.1 Bid Rigging and Bid Rotating Certification 16
8.2 Drug Free Workplace Certification 16
8.3 Tax Compliance Certification 16
8.4 Non Collusion Certification 16
8.5 Equal Employment Opportunity Certification 16
9. General Conditions 17
9.1 Reservation of Rights 17
9.2 Proposal Becomes Property of Village 17
9.3 Costs of Preparation 17
9.4 Sub Contractors 17
9.5 Governing Law 17
9.6 No Contact Provision 17
Appendix A: Calendar of Events 18
Appendix B: Acknowledgment of Receipt 18

1. Introduction and Background

1.1 Purpose

The Village of Westchester, Illinois ("Village") is issuing this Request for Proposal ("RFP") to solicit proposals from qualified firms ("Proposer" or "Vendor") to provide a fully managed cybersecurity detection, response, and monitoring service. The selected Vendor shall deliver a unified solution that includes managed endpoint detection and response, identity threat detection and response, security information and event management, and continuous real time threat analysis with active human led incident response.

The intent of this procurement is to consolidate multiple point security tools into a single managed service relationship with a Vendor capable of serving as an extension of the Village's information technology function.

1.2 About the Village

The Village of Westchester is a municipal corporation located in Cook County, Illinois, serving a population of approximately 16,500 residents. The Village operates a full service local government including the following departments and functions:

- Office of the Village Manager and Administration
- Westchester Police Department
- Westchester Fire Department
- Department of Public Works
- Finance Department
- Community Development

1.3 Current Technology Environment

The Village operates a hybrid information technology environment. Proposers should design their response with the following environment in mind. The Village reserves the right to modify, add to, or remove any element of the environment described below at any time.

- Hybrid Microsoft Active Directory with on premises domain controllers and Microsoft Entra ID synchronization
- Microsoft 365 Government Community Cloud G3 tenant covering all Village staff
- Approximately 175 endpoints including Windows workstations, Windows servers, and macOS devices
- Approximately 60 mobile devices managed through Mosyle Mobile Device Management
- Multiple line of business applications hosted on premises and in cloud infrastructure

- Public safety systems supporting Police and Fire operations, subject to applicable Criminal Justice Information Services (CJIS) Security Policy requirements
- Edge security provided by Ubiquiti Enterprise Fortress Gateway and associated network infrastructure
- Cloud infrastructure including virtual machines hosted with Vultr and Cloudflare edge protection

1.4 Statement of Need

The Village requires a managed cybersecurity service that delivers continuous, twenty four hour, seven day per week monitoring of endpoints, identities, cloud workloads, and network telemetry. The service shall be staffed by a Security Operations Center (SOC) with live human analysts capable of investigating, escalating, and responding to threats in real time, including outside of normal business hours. Automated detection alone is not sufficient; the Village requires that a human analyst review, validate, and act upon alerts before they are escalated to Village staff.

2. Scope of Services

The selected Vendor shall provide all of the following services as a single integrated managed offering. Pricing shall be inclusive of software licensing, agent deployment, configuration, tuning, monitoring, alerting, investigation, and incident response unless otherwise specified.

2.1 Managed Endpoint Detection and Response (EDR)

The Vendor shall deploy and continuously manage an endpoint detection and response agent across all Village owned Windows, macOS, and applicable Linux systems. At minimum the EDR capability shall include:

- Behavioral and signatureless threat detection covering ransomware, persistent footholds, living off the land techniques, and lateral movement
- Continuous process, file, registry, and network telemetry collection with searchable retention of not less than ninety (90) days
- Automated and analyst initiated host isolation that can remove a compromised endpoint from the network without requiring local user intervention
- Managed agent lifecycle including deployment, version updates, health monitoring, and remediation of agent failures
- Tuning of detection rules and suppression of false positives without requiring Village staff involvement in routine operations
- Identification and remediation guidance for persistent footholds, unauthorized scheduled tasks, malicious services, and other dwelling threats

2.2 Identity Threat Detection and Response (ITDR)

The Vendor shall provide continuous monitoring of the Village's Microsoft 365 and Entra ID tenant for identity based threats. At minimum the ITDR capability shall include:

- Detection of credential theft, token theft, and session hijacking against Microsoft 365 accounts
- Monitoring for malicious mailbox rules, suspicious mail forwarding, and unauthorized delegation
- Detection of suspicious OAuth application consent grants and unauthorized enterprise application registrations
- Monitoring of multi factor authentication enrollment changes, including unauthorized MFA device additions
- Anomalous sign in detection across geography, device, and behavior baselines
- Business email compromise detection including invoice fraud, vendor impersonation, and executive impersonation indicators

- Technical capability and authorization workflow to revoke active sessions, disable accounts, and reverse malicious tenant configuration changes during an active incident
- Monitoring of privileged role assignments and changes to conditional access policies

2.3 Security Information and Event Management (SIEM)

The Vendor shall provide a fully managed SIEM capability that ingests, normalizes, and correlates security telemetry from across the Village environment. The Vendor shall be responsible for log source onboarding, parser maintenance, and correlation rule development. At minimum the SIEM capability shall ingest and analyze the following log sources:

- Microsoft 365 unified audit log, Entra ID sign in logs, and Microsoft Defender telemetry
- On premises Active Directory domain controller security events
- Firewall, edge gateway, and intrusion prevention system logs
- Network switch authentication, change, and anomaly logs where supported
- Wireless infrastructure authentication and association logs
- DNS query and response logs
- Server operating system security event logs for Windows and Linux hosts
- Application logs for Village hosted web applications and line of business systems
- Mobile device management telemetry from Mosyle
- Cloud infrastructure logs from Vultr and Cloudflare

Log retention shall be a minimum of three hundred sixty five (365) days of hot, searchable retention with an additional twenty four (24) months of cold or archive retention available on request. Proposers shall describe retention pricing and any per gigabyte or per event ingestion fees in the cost proposal.

2.4 Real Time Threat Analysis and Twenty Four Hour Monitoring

The Vendor shall operate a Security Operations Center (SOC) staffed twenty four hours per day, seven days per week, three hundred sixty five days per year, including all federal and state holidays. The SOC shall be staffed by employees of the Vendor or a clearly identified subcontractor; pure offshore call center triage models will not be considered. The Vendor shall:

- Validate, triage, and investigate every alert generated by the platform before escalation to Village staff
- Provide written investigation summaries for all escalated incidents, including timeline, indicators of compromise, scope of impact, and recommended containment actions
- Maintain a documented escalation matrix including primary and after hours contacts for the Village

- Meet defined service level objectives for time to detect, time to triage, and time to escalate (see Section 2.7)
- Provide direct telephone and secure messaging access to a live analyst at any hour

2.5 Active Response and Incident Handling

The Vendor shall be authorized and capable of taking active containment actions during a confirmed incident. The Vendor shall:

- Execute host isolation, account disablement, and session revocation on confirmed compromise
- Provide live incident response support during an active event, including coordination calls with Village staff and any third party incident response retainer holder
- Produce a written incident report within five (5) business days of incident closure, suitable for cyber insurance carrier and regulatory submission
- Cooperate with law enforcement, the Multi State Information Sharing and Analysis Center (MS ISAC), and the Cybersecurity and Infrastructure Security Agency (CISA) on Village request

2.6 Reporting and Visibility

The Vendor shall provide the Village with a single web based portal accessible to authorized Village staff that includes, at minimum:

- Real time dashboard of current detections, open investigations, and asset coverage
- Searchable access to all collected telemetry and historical alerts within the retention window
- Configurable user accounts with role based access control and multi factor authentication enforcement
- Monthly executive summary report including detection counts, investigation outcomes, top risks, and trend analysis
- Quarterly strategic review meeting with a named account contact

2.7 Service Level Objectives

The Vendor shall meet or exceed the following service level objectives. Proposers may propose stronger objectives but may not propose weaker ones. Failure to meet objectives shall trigger service credits as defined in the resulting contract.

Metric	Critical / High Severity	Medium / Low Severity
Time to Detect	≤ 15 minutes	≤ 60 minutes
Time to Triage	≤ 30 minutes	≤ 4 hours
Time to Escalate to Village	≤ 60 minutes	Next business day

Metric	Critical / High Severity	Medium / Low Severity
Platform Uptime	99.9% monthly	99.9% monthly
Analyst Availability	24/7/365	24/7/365

3. Mandatory Requirements

Proposals that fail to meet the mandatory requirements in this section will be deemed non responsive and will not be evaluated further. Proposers shall affirmatively respond to each requirement in writing.

3.1 Compliance and Attestation

- Vendor shall maintain a current SOC 2 Type II attestation; report shall be made available to the Village under non disclosure agreement upon request
- Vendor shall affirm in writing that all personnel with access to Village data are subject to background investigation
- Vendor shall affirm capability to support Criminal Justice Information Services (CJIS) Security Policy compliance for the Police Department environment, including signing of a CJIS Security Addendum if required
- Vendor shall identify the geographic location of all data storage, all SOC operations, and all analyst personnel; data storage outside the continental United States is not permitted
- Vendor shall affirm compliance with applicable provisions of the Illinois Personal Information Protection Act (815 ILCS 530)

3.2 Insurance Requirements

The selected Vendor shall maintain, at its own cost, the following minimum insurance coverages for the duration of the contract:

- Commercial General Liability: $2,000,000 per occurrence and $2,000,000 aggregate
- Cyber Liability and Technology Errors and Omissions: $5,000,000 per occurrence and $5,000,000 aggregate
- Workers Compensation as required by Illinois law
- Professional Liability: $2,000,000 per occurrence
- The Village of Westchester, its elected officials, officers, employees, and agents shall be named as additional insureds on all policies except Workers Compensation and Professional Liability

3.3 References and Experience

- Vendor shall demonstrate not less than five (5) years of continuous operation providing managed security services
- Vendor shall provide a minimum of three (3) references from current customers of similar size and scope, with at least one (1) reference from an Illinois municipal or public sector customer
- Vendor shall disclose any material security incidents affecting their own platform within the past three (3) years

4. Proposal Submission Requirements

4.1 Format and Delivery

Proposals shall be submitted electronically in Portable Document Format (PDF) to the email address listed on the cover page of this RFP. The subject line shall read: "RFP Submission: Managed Cybersecurity Services." Proposals received after the date and time stated on the cover page will not be accepted. The Village will not accept facsimile or paper submissions.

4.2 Proposal Content and Order

Proposals shall be organized in the following order. Failure to follow this order may result in deduction of evaluation points.

1. Cover letter signed by an authorized representative of the firm, including a statement that the proposal is a firm and irrevocable offer for one hundred twenty (120) days from the submission deadline
2. Executive summary, not to exceed two (2) pages
3. Company profile, ownership structure, and years in operation
4. Detailed response to Scope of Services in Section 2, addressing each subsection in order
5. Detailed response to Mandatory Requirements in Section 3
6. Proposed implementation plan and timeline
7. Sample reports and portal screenshots
8. Three (3) customer references including name, title, organization, telephone, and email
9. Cost proposal in the format prescribed in Section 5
10. Executed certifications required by Section 8
11. Proof of insurance or letter of insurability from the Vendor's broker
12. Any exceptions taken to this RFP, clearly identified by section number

4.3 Questions and Addenda

All questions regarding this RFP shall be submitted in writing via email to the contact listed on the cover page no later than ten (10) calendar days prior to the proposal due date. The Village will issue written responses to all questions in the form of addenda. Addenda will be posted on the Village website and emailed to all parties who have registered interest in this RFP. Verbal communications with Village staff or elected officials are not binding and shall not be relied upon. Proposers shall acknowledge receipt of all addenda in their cover letter.

4.4 Pre Proposal Conference

An optional pre proposal conference may be held at the discretion of the Village. If held, the date, time, and location will be posted on the Village website and communicated by addendum. Attendance is not mandatory but is strongly encouraged.

5. Cost Proposal Format

The cost proposal shall be provided in a separate, clearly labeled section of the response. All pricing shall be firm fixed for the initial contract term. Pricing shall be presented in the following format:

Component	Year 1	Annual Recurring
One time onboarding and deployment	$	N/A
Managed EDR (per endpoint)	$	$
Identity Threat Detection (per identity)	$	$
Managed SIEM (base + per GB)	$	$
24/7 SOC monitoring and response	$	$
Incident response (included hours)	$	$
TOTAL ANNUAL	**$**	**$**

Proposers shall also provide pricing for optional renewal years two and three, with any annual escalation clearly stated as a fixed percentage not to exceed five percent (5%) per year.

6. Evaluation Criteria

Proposals will be evaluated by the IT Department in coordination with the Village Manager. The Village intends to award based on best value, not lowest price. Evaluation will be conducted using the following weighted criteria:

Criterion	Maximum Points
Technical capability and completeness of solution (EDR, ITDR, SIEM, SOC)	**30**
Quality and depth of 24/7 SOC operations and active response	**20**
Cost proposal and total cost of ownership	**20**
Vendor experience, references, and financial stability	**15**
Compliance with CJIS, SOC 2, and data residency requirements	**10**
Implementation approach and transition plan	**5**
TOTAL	**100**

The Village may, at its sole discretion, conduct interviews, request demonstrations, request best and final offers, or negotiate with one or more finalists prior to award. A demonstration to the village board may be required.

7. Contract Terms

7.1 Term

The initial contract term shall be three (3) years from the effective date, with two (2) optional one (1) year renewals at the sole discretion of the Village. Renewals shall be exercised in writing not less than sixty (60) days prior to the end of the then current term.

7.2 Termination for Convenience

The Village reserves the right to terminate the resulting contract for convenience upon ninety (90) days written notice. The Vendor shall be entitled to payment for services performed through the date of termination but shall not be entitled to lost profits or consequential damages.

7.3 Termination for Cause

The Village may terminate the contract for cause upon thirty (30) days written notice in the event of material breach by the Vendor that remains uncured at the end of the notice period. Failure to meet service level objectives for three (3) consecutive months shall be deemed material breach.

7.4 Data Ownership and Return

All Village data ingested, processed, or stored by the Vendor shall remain the sole property of the Village. Upon termination of the contract for any reason, the Vendor shall return all Village data in a commonly readable format within thirty (30) days, and shall certify destruction of all copies within sixty (60) days thereafter.

7.5 Confidentiality and Public Records

The Vendor shall hold all Village information in strict confidence. The Vendor acknowledges that the Village is subject to the Illinois Freedom of Information Act (5 ILCS 140) and that information provided to the Village may be subject to public disclosure. Proposers who wish to designate portions of their proposal as exempt from disclosure shall clearly mark such portions and cite the specific statutory exemption claimed; the final determination of disclosure rests with the Village.

7.6 Indemnification

The Vendor shall defend, indemnify, and hold harmless the Village, its elected officials, officers, employees, and agents from and against any and all claims, damages, losses, and expenses arising from the negligent acts or omissions of the Vendor in the performance of the contract.

8. Required Certifications

The Proposer shall execute and submit each of the following certifications with the proposal. Failure to submit executed certifications shall render the proposal non responsive.

8.1 Bid Rigging and Bid Rotating Certification

The Proposer certifies that the Proposer, its officers, employees, and agents are not barred from submitting a response to this RFP as a result of a violation of the Bid Rigging or Bid Rotating provisions of the Public Contracts Section of the Illinois Criminal Code of 2012 (720 ILCS 5/33E 3, 33E 4), or as a result of a violation of any other law, rule, ordinance, or regulation.

8.2 Drug Free Workplace Certification

The Proposer certifies that it will provide a drug free workplace as required by the Illinois Drug Free Workplace Act, 30 ILCS 580/1 et seq.

8.3 Tax Compliance Certification

The Proposer certifies that it is not delinquent in the payment of any tax administered by the Illinois Department of Revenue, or has entered into an agreement with the Department to pay such tax and is in compliance with that agreement.

8.4 Non Collusion Certification

The Proposer certifies that the proposal has been arrived at independently and submitted without collusion with any other Proposer or any officer or employee of the Village.

8.5 Equal Employment Opportunity Certification

The Proposer certifies compliance with the Illinois Human Rights Act (775 ILCS 5), the Equal Employment Opportunity clause required by the Illinois Department of Human Rights, and all applicable federal equal employment opportunity laws.

9. General Conditions

9.1 Reservation of Rights

The Village reserves the right to accept or reject any or all proposals, in whole or in part; to waive any informality or irregularity in any proposal; to request additional information or clarification from any Proposer; to negotiate with any Proposer; to award by individual component or in the aggregate; and to cancel this RFP at any time prior to execution of a contract. The issuance of this RFP does not obligate the Village to award a contract.

9.2 Proposal Becomes Property of Village

All proposals submitted in response to this RFP shall become the property of the Village upon receipt and will not be returned.

9.3 Costs of Preparation

All costs incurred by the Proposer in the preparation and submission of a proposal, including any subsequent presentations or interviews, shall be borne solely by the Proposer.

9.4 Sub Contractors

If the Proposer intends to subcontract any portion of the work, the proposal shall clearly identify each proposed subcontractor, the scope of work to be performed, and the percentage of total work to be subcontracted. Any change in subcontractors after award shall require prior written approval of the Village.

9.5 Governing Law

This RFP and any resulting contract shall be governed by and construed in accordance with the laws of the State of Illinois. Venue for any dispute shall lie in the Circuit Court of Cook County, Illinois.

9.6 No Contact Provision

From the date of issuance of this RFP through the date of contract award, Proposers and their representatives shall not contact any member of the Village Board of Trustees, the Village Manager, or any Village employee other than the designated contact regarding this RFP. Violation of this provision may result in disqualification.

Appendix A: Calendar of Events

The Village anticipates the following schedule. The Village reserves the right to modify any date in this schedule by addendum.

Event	Date
RFP Issued	
Optional Pre Proposal Conference	
Written Questions Due	
Village Responses Issued	
Proposals Due	
Evaluation and Interviews	
Notice of Intent to Award	
Contract Execution Target	
Service Commencement	

Appendix B: Acknowledgment of Receipt

Proposers are requested to complete and return this form to indicate their intent to respond to this RFP. This form is for the convenience of the Village and is not mandatory.

Firm Name	
Contact Name	
Title	
Email	
Telephone	
Intent to Propose (Y/N)	

— END OF REQUEST FOR PROPOSAL —