COUNTY OF ROCKLAND
Department of General Services
Purchasing Division

Contract Award Notification

Title:	**Cyber security Monitoring & Detection SaaS**
Contract Period:	January 1, 2026 through December 31, 2026 w/3-1-year options
Original Date of Issue:	January 6, 2026
Date of Revision:	
BID No:	**RCO-RC-2025-016**
Ordering Method:	**Special Request**
Authorized Users:	County Agencies, United States Agencies, Other States & Political Subdivisions Therein, Local Governments, School Districts & Non-Profit Agencies

Address Inquiries to:

Name: Sabrina Samuels
Title: Assistant Director of Purchasing
Phone: (845) 364-3807
Fax: (845) 364-3809
E-mail: samuelss@co.rockland.ny.us

Description

This contract is to provide Cyber Security Monitoring & Detection SaaS.

Contract #	Vendor Number	Contractor & Address	Telephone No.
RCO-RC-2025-016	0000026567	Vandis Inc. 1 Albertson Ave Suite 1 Albertson, NY 11507 Contact: Melonie Kolega mkolega@vandis.com	516-281-2205

COUNTY OF ROCKLAND
DGS – PURCHASING DEPARTMENT
BLDG. A, 6TH FLOOR, 50 SANATORIUM ROAD
POMONA, NY 10970
TELEPHONE NO.: 845-364-3820

VENDOR: Vandis

LINE NO.	DESCRIPTION	ITEM NUMBER	EST. QTY.	UNIT	UNIT PRICE
1	Adlumin Complete licenses Cybersecurity Monitoring and Detection NAB-MDR-MDRC-Y or approved Equal	20889	300	each	**$171.91**
2	1 YEAR Log Rentention per license Adlumin NAB-MDR-MDRLOG-Y or approved equal	20889	300	Each	**$12.05**
3	Incident Response Adlumin NAB-MDR-IR-Y or approved equal	20889	300	Each	**$10.81**

Upon receipt of all required approvals a Contract shall be deemed executed and created with the successful Bidder(s) upon the Commissioner's mailing or electronic communication to the address on the bid of: (i) a Letter of Acceptance; or (ii) a fully executed contract; or (iii) a Purchase Order authorized by the Commissioner

COUNTY OF ROCKLAND - DGS-PURCHASING
BLDG. A., 6TH FLOOR, 50 SANATORIUM RD, POMONA, NY 10970
TELEPHONE: 845-364-3820 / TELEFAX: 845-364-3809

TITLE: Cybersecurity Monitoring and Detection	**RCO-RC-2025-016**

PURCHASES BY UNITED STATES AGENCIES, OTHER STATES AND POLITICAL SUBDIVSIONS THEREIN, LOCAL GOVERNMENTS, SCHOOL DISTRICTS, AND NON-PROFIT AGENCIES

As per the New York State General Municipal Law, § 103(3) all political subdivisions of New York State are allowed to make purchases through the resulting contract(s). As per Rockland County Procurement Policy § 140-13, the United States of America or any agency thereof, any state, or any other political subdivision or district therein and certain Non-Profit Agencies approved to participate in New York State's Contract Extension Program are authorized to make purchases through the resulting contract(s).

1. The County of Rockland shall make all contract award information available to other political subdivisions and non-profit agencies through the **Empire Procure Connect Marketplace**.
2. Any other political subdivision or Rockland County non-profit agency will issue purchase orders directly to vendors within the specified contract period referencing the County's contract and shall be liable for any payments due on such purchase orders; and shall accept sole responsibility for any payment due.
3. All purchases shall be subject to audit and inspection by the other political subdivisions and Rockland County non-profit agencies for which the purchase was made.
4. No officer, board or agency of a county, town, village, or school district shall make any purchase through the County when bids have been received for such purchase by such officer, board or agency, unless such purchase may be made upon the same terms, conditions and specifications at a lower price through the County.
5. All Bidders shall be on notice that as a condition of the award of a County contract, the successful bidder shall accept the award of a similar contract with any other political subdivision in New York State and Rockland County non-profit agencies authorized to use New York State's contracts, if called upon to do so. A listing of approved Rockland County non-profit agencies is available on the Purchasing Division's website at www.rcpurchasing.com. The County, however, will not be responsible for any debts incurred by the participants pursuant to this or any other agreement.
6. Necessary deviations from the County's specifications in the award of a participant contract, whether such deviations relate to quantities or delivery points shall be resolved between the successful bidder and the other political subdivisions and Rockland County non-profit agencies.

COUNTY OF ROCKLAND - DGS-PURCHASING
BLDG. A., 6TH FLOOR, 50 SANATORIUM RD, POMONA, NY 10970
TELEPHONE: 845-364-3820 / TELEFAX: 845-364-3809

TITLE: Cybersecurity Monitoring and Detection	**RCO-RC-2025-016**

SCOPE OF WORK AND SPECIFICATIONS

1. Purpose

1.1. The purpose of this Best Value Bid Specification is to solicit proposals from qualified cybersecurity service providers capable of delivering comprehensive Adlumin Managed Detection and Response (MDR) services or approved equal. The selected vendor will provide 24x7x365 threat monitoring, analysis, escalation, and response capabilities aligned to the service expectations, roles, deliverables, and limitations.

2. Scope of Work

2.1. Vendors shall provide MDR services that deliver full-spectrum cybersecurity monitoring, detection, analysis, and incident containment support. The MDR service must integrate seamlessly with the organization's IT infrastructure and provide enterprise-grade visibility, threat intelligence, user behavior analytics, and reporting capabilities.

The awarded vendor must deliver services consistent with or exceeding the following:

2.2. Continuous Monitoring & Threat Detection

2.2.1. 24/7/365 monitoring and threat detection operations using dedicated MDR security analysts

2.2.2. Multi-layered detection leveraging threat research, data science, and custom detection engineering teams.

2.2.3. Real-time alerting with automated and analyst-driven triage workflows.

2.3. Threat Hunting

2.3.1. Continuous proactive threat hunting to identify risks, weaknesses, and emerging threats across the customer environment before they escalate.

2.4. Incident Investigation & Response

2.4.1. Detailed investigation notes, including timeline, analyst actions, and remediation recommendations.

2.4.2. Containment response actions using automated and analyst-initiated Security Orchestration, Automation and Response (SOAR) capabilities for clients opting into FULL Mode

2.4.3. Support for customer war rooms, including senior analyst engagement for up to three hours per incident where applicable.

2.5. Client Collaboration & Communication

2.5.1. Support through Jira ticketing, Microsoft Teams, Cisco Webex, and Security Operations Center (SOC) email channels

2.5.2. Clear escalation logic for emergency and non-emergency incidents.

2.5.3. Optional scheduled engagements with senior MDR analysts for security posture review and recommendations.

COUNTY OF ROCKLAND - DGS-PURCHASING
BLDG. A., 6TH FLOOR, 50 SANATORIUM RD, POMONA, NY 10970
TELEPHONE: 845-364-3820 / TELEFAX: 845-364-3809

TITLE: Cybersecurity Monitoring and Detection	**RCO-RC-2025-016**

3. Deliverables

The vendor shall provide the following deliverables at minimum:

3.1. Security Operations

3.1.1. 24/7/365 SOC monitoring by qualified MDR analysts.
3.1.2. Actionable alerts with detailed analyst investigation summaries and recommendations.
3.1.3. Continuous tuning and refinement of detection logic by dedicated detection engineers

3.2. Automation & Response

3.2.1. Automated alert acknowledgement, triage, containment, and escalation workflows.
3.2.2. Optional automated SOAR playbook execution based on FULL or WATCH Mode engagement models

3.3. Reporting & Review

3.3.1. Post-incident investigation summaries within the ticketing system.
3.3.2. Detailed incident timeline and activity analysis.
3.3.3. Optional strategic MDR analyst meetings for incident review and environment posture assessment.

3.4. Alert Noise Reduction

3.4.1. Collaborative filtering of low-value or risk-accepted detections to reduce operational noise

4. Service Level Objectives (SLOs)

4.1. Vendors must meet or exceed the following SLOs:
4.2. 24/7/365 availability of MDR services
4.3. Timely response according to severity, with immediate contact for threats impacting business operations.
4.4. Adherence to escalation protocols (ticketing + telephone contact based on urgency).

5. Client Requirements

5.1. Vendor proposals must support the following environmental requirements:
5.2. Deployment of required agents, syslog collectors, and API integrations for EDR, IAM, and other critical data sources
5.3. Customers retain responsibility for configuration of devices and log ingestion.
5.4. MDR team must **not** directly modify customer systems such as EDR, firewall, VPN, IAM, IDS/IPS, DNS, or others

6. Rules of Engagement

The vendor shall support two engagement models:

6.1. FULL Mode

6.1.1. Vendor may execute automated and analyst-initiated SOAR actions (e.g., host isolation, account disablement) .
6.1.2. Clients may set exclusions for SOAR actions (user or detection-based suppression).

6.2. WATCH Mode

6.2.1. No automated or analyst-initiated SOAR actions performed.
6.2.2. Vendor provides monitoring, triage, and notification only.

COUNTY OF ROCKLAND - DGS-PURCHASING
BLDG. A., 6TH FLOOR, 50 SANATORIUM RD, POMONA, NY 10970
TELEPHONE: 845-364-3820 / TELEFAX: 845-364-3809

TITLE: Cybersecurity Monitoring and Detection	**RCO-RC-2025-016**

6.2.3. Clients may execute SOAR playbooks independently, outside MDR visibility.

7. Required Team Capabilities

7.1. Vendor must demonstrate MDR team structure that includes competencies substantially similar to the following roles:

7.1.1. **Blue Team**: Alert triage and containment actions
7.1.2. **Orange Team**: Customer response and communication
7.1.3. **Yellow Team**: Detection engineering for tuning and new detection development
7.1.4. **Black Team**: Senior analyst support for critical incidents (limited engagement hours)
7.1.5. **Green Team**: Quality assurance and training
7.1.6. **Grey Team**: Threat hunting, automated containment, and IOA/IOC validation

8. NIST Cybersecurity Framework Alignment

8.1. Vendor MDR service must align with NIST CSF 2.0 functional areas (Identify, Protect, Detect, Respond, Recover) consistent with the Adlumin MDR mapping or approved equal.

9. Retention

9.1. One year of log retention.

10. Award

10.1. Award will be made to the vendor whose proposal offers the **best overall value**, considering price, performance, capability, and conformance to the MDR specifications outlined above.

Price Adjustments: A Price Adjustment request must be made in writing and include the reason for the request, documentation supporting the request (i.e., commodity increases), the current pricing, and the requested revised pricing.

The County will review the Price Adjustment request. If the Price Adjustment is deemed reasonable the Price Adjustment request will be accepted by written acknowledgement. If the request is not accepted the County may entirely reject the request or may counter with revised pricing. In either case the County will provide a written explanation in support of the decision.

The Director of Purchasing may use available indexes (e.g., CPI or PPI) to determine if the requested Price Adjustment is reasonable. Typically, a Price Adjustment that exceeds 5% will not be approved unless very unusual and significant changes have occurred in the industry.

In the event industry costs decline, the County shall have the right to receive, from the Contractor, a reasonable reduction in prices/pricing that reflect such cost changes in the industry. The County will make a written request to the Contractor for a Price Adjustment in writing with supporting documentation.

COUNTY OF ROCKLAND - DGS-PURCHASING
BLDG. A., 6TH FLOOR, 50 SANATORIUM RD, POMONA, NY 10970
TELEPHONE: 845-364-3820 / TELEFAX: 845-364-3809

TITLE: Cybersecurity Monitoring and Detection	**RCO-RC-2025-016**

Discounts: The discounts offered are considered minimum discounts that must be offered under the resulting contract. Authorized Users/Participating Entities may negotiate additional discounts on a per order basis.

Volume Discounts: Volume discounts may be negotiated by the Authorized User/Participating Entity and applied per Purchase Order. Volume discounts shall be defined and applied as follows:

A. Purchase Order volume discounts shall be additional discounts applied to individual Purchase Orders over a specified dollar amount.

B. Cumulative agency volume discounts shall be additional discounts applied to all future orders made by an individual ordering entity once an established volume has been met by that entity.

RESELLER UTILIZATION: A Manufacturer may respond to this solicitation directly or allow authorized resellers to respond to the solicitation by region. A Manufacturer that responds directly may utilize Resellers to sell Equipment, and, if applicable, provide Services. A listing of the authorized Resellers must be submitted with the bid response and Resellers must be eligible to quote regionally or statewide, independently and lower than Manufacturer (Contract) pricing for procurements under resulting Contracts. Resellers must also be able to accept orders, invoice and receive payment.

USE OF FEDERAL FUNDS: Purchases made under this contract may be funded in whole or in part with federal funds. Therefore, the following provisions will apply as required by the Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards, also known as the Uniform Guidance (2 CFR Part 200). The contractor must comply with all federal laws, regulations, and the specific terms and conditions related to the use of federal funds. This includes but is not limited to the following:

1. Equal Employment Opportunity: The contractor must comply with Executive Order 11246, as amended by Executive Order 11375, and all regulations issued by the Secretary of Labor (41 CFR Part 60), prohibiting employment discrimination.
2. Davis-Bacon Act: For contracts subject to the Davis-Bacon Act, the contractor agrees to pay prevailing wages to laborers and mechanics as determined by the U.S. Department of Labor.

3. Contract Work Hours and Safety Standards Act: The contractor must comply with this Act, which governs the hours and safety standards for labor on federally funded contracts over $100,000.

4. Rights to Inventions Made Under a Contract or Agreement: If the contract involves experimental, developmental, or research work funded by federal dollars, the contractor must comply with the provisions of 37 CFR Part 401.

COUNTY OF ROCKLAND - DGS-PURCHASING
BLDG. A., 6TH FLOOR, 50 SANATORIUM RD, POMONA, NY 10970
TELEPHONE: 845-364-3820 / TELEFAX: 845-364-3809

TITLE: Cybersecurity Monitoring and Detection	**RCO-RC-2025-016**

5. Clean Air Act and Federal Water Pollution Control Act: For contracts exceeding $150,000, the contractor must comply with all applicable standards, orders, or regulations issued under these Acts.

6. Debarment and Suspension: Contractors are prohibited from awarding contracts to any party listed on the General Services Administration's (GSA) System for Award Management (SAM) as debarred, suspended, or otherwise excluded from participation in federal programs.

7. Byrd Anti-Lobbying Amendment: Contractors who apply or bid for an award exceeding $100,000 must file the required certification that they will not use federal funds to influence or attempt to influence any government official or employee in connection with obtaining any federal contract or award.

8. Procurement of Recovered Materials: The contractor must comply with Section 6002 of the Solid Waste Disposal Act, as amended by the Resource Conservation and Recovery Act, which requires that items designated by the Environmental Protection Agency (EPA) be made from recovered materials.

The contractor is responsible for completing and submitting the **Federal Contract Clauses** included in this solicitation with their Offer and ensuring that these and any other applicable federal contract clauses are included in any subcontracts and are adhered to throughout the performance of the contract. Failure to comply with these federal requirements may result in termination of the contract and other penalties as prescribed by law.

Rockland County
Ed Day, Rockland County Executive

DEPARTMENT OF GENERAL SERVICES, PURCHASING DIVISION
Dr. Robert L. Yeager Health Center
50 Sanatorium Rd, Building A
Pomona, New York 10970
Phone: (845) 364-3820 Fax: (845) 364-3809
Email: purchasing@co.rockland.ny.us

Paul Brennan, FNIGP, NIGP-CPP, CPPO
Director of Purchasing

ADDENDUM # 1

RCO-RC-2025-016

The information in this addendum supersedes any contradictory information set forth in the contract documents. Acknowledge receipt of this addendum in the space provided on the signature page of the bid proposal. Failure to do so, may subject the bidder to disqualification. This addendum forms a part of the contract documents.

Question # 1: These directly affect Sentinel/SIEM ingestion volume, retention tiers, and MDR pricing. Please provide the estimated daily log volume (GB/day) across all sources (firewalls, servers, endpoints, network appliances, SaaS systems).
Response #1: This information cannot be provided for security reasons.

Question #2: How many total endpoints, servers, and network devices are in scope for continuous MDR monitoring?
Response #2: 300 endpoints, servers

Question #3: Which specific log sources are required, and which are optional? (e.g., firewall, EDR, identity logs, SaaS logs, OT logs).
Response #3: All are required.

Question #4: Is full-log ingestion required, or is the County open to a security-value prioritized ingestion strategy?
Response #4: Yes, full-log ingestion is required.

Question #5: Are third-party EDR tools already deployed (CrowdStrike, SentinelOne, Cisco Secure Endpoint), and must the MDR vendor integrate with them?
Response #5: Yes, ThreatDown Ultimate

Question #6: Please confirm the full list of technologies requiring monitoring, including: Firewalls, EDR, Email security, IAM systems, Cloud/SaaS sources, OT/SCADA (if applicable). Are custom log connectors required?
Response #6: Yes, all noted are required, we also required switches.

Questions #7: Is vulnerability scanning required as part of MDR? If yes, internal scanning only, external attack surface monitoring?

Response #7: Yes, both internal and external scanning.

Question #8: Please confirm the security technologies and data sources in scope for MDR monitoring and API integration, including (as applicable) a) endpoint / EDR b) identity & IAM (e.g., active directory, Entra ID / Azure AD) c) network security (firewalls, VPN, IDS/IPS) d) email security e) cloud platforms (e.g., M365, Azure, AWS, GCP).

Response#8: Yes, all are noted in the scope, please refer to the bid.

Question #9: Which telemetry sources are mandatory at service commencement versus eligible for phased onboarding?

Response #9: Deployment of required agents, syslog collectors, and API integrations for EDR and Microsoft Email Tenant.

Question #10: Should bidders assume enterprise-wide MDR coverage, or will the County designate in-scope and out-of-scope environments post-award?

Response #10: Bidders should assume enterprise-grade visibility, threat intelligence, user behavior analytics, and reporting capabilities MDR coverage.

Question #11: Does the County have baseline estimates for a) number of monitored endpoints, users, servers, and network devices and b) approximate daily log ingestion volume (GB/day or EPS)

Response #11: Approximately 300 monitored endpoints, we are unwilling to provide daily log ingestion volume for security purposes.

Question #12: Does the County have predefined severity tiers (Critical / High / Medium / Low), or should bidders propose severity classifications?-

Response #12: Bidder must define their tiers. Please refer to the referenced tiers in the bid as an example.

Question #13: Are there defined SLOs for time-to-acknowledge, time-to-escalate, and time-to- contain per severity level?

Response #13: Please refer to the bid

Question #14: For business-impacting threats, please define a) required contact channel(s) (phone, SMS, Teams/Webex) or b) target response time in minutes.

Response #14: Please refer to the bid

Question #15: Please confirm the County's desired default mode a) FULL mode (SOAR enabled b) WATCH mode (monitoring and notification only) or c) Hybrid model (by asset group, severity, or incident type).

Response #15:Full mode is desired but the solution must support both Full mode and Watch mode.

Question #16:If FULL mode is enabled, please provide the list of pre-approved automated and analyst-initiated containment actions (e.g., host isolation, account disablement).

Response #16:The vendor may execute automated and analyst-initiated SOAR actions (e.g. host isolation, account disablement).

Question #17:In FULL mode, will containment actions be a) pre-authorized via approved playbooks, or b) approved on an incident-by-incident basis?

Response #17:The vendor may execute automated and analyst-initiated SOAR actions (e.g. host isolation, account disablement).

Question #18:Who retains final authority during active incidents a) county IT/Security b) county leadership or c) MDR provider within approved playbooks

Response #18:County IT

Question #19:Given the restriction on direct system modification, what mechanism (API, orchestration tool, ticket-based execution) will be used to trigger containment actions in FULL mode?

Response #19:Deployment of required agents, syslog collectors and API Integrations.

Question #20:Will the MDR provider be permitted to a) provide guidance only or b) actively assist with agent, collector, and API integration under County supervision

Response #20:Actively assist with agent, collector, and API integration under County supervision.

Question #21:Will required API access be available at contract start, or should phased onboarding be assumed?

Response #21:This should be phased onboarding.

Question #22:Does the County have historical or expected metrics for a) average alert volume and b) High and Critical incident frequency.

Response #22:No this information is not available.

Question #23:Please confirm how the included three (3) hours of senior analyst support applies a) per Critical incident only or b) per High and Critical incidents. Also, is this allocation capped annually?

Response #23:Please include per high and Critical incidents, and not capped annually.

Question #24:Are there defined fair-use limits or commercial terms for a) incident surges b) senior analyst hours beyond included entitlements?

Response #24:No this is not something the County has.

Question #25:Which platform will serve as the authoritative incident ticketing system a) county-provided Jira or b) MDR provider platform integrated with County workflows.

Response #25:MDR provider platform integrated with County workflows.

Question #26:Please confirm the preferred primary communication channel for Critical incidents (Teams, Webex, or email).

Response #26:Email

Question #27:Which regulatory or compliance frameworks must MDR reporting support (e.g., CJIS, HIPAA, NY State mandates)?

Response #27:All noted above.

Question #28:Are post-incident deliverables expected to meet a) operational SOC reporting standards or b) formal audit / legal / evidentiary standards?

Response #28:Formal audit/legal/ evidentiary standards.

Question #29:Are senior-analyst posture or program review meetings expected to occur a) monthly b) quarterly or c) on-demand only

Response #29:On- demand.

Question #30:Please confirm what a single MDR license represents a) endpoint/device b) user/identity c) server/workload or d) blended unit

Question #30:All noted above.

Question #31:Does each MDR license include a) endpoint + identity + log ingestion for a single asset or b) broader telemetry coverage tied to a logical entity?

Response #31:Endpoint + identity + log ingestion for a single asset

Question #32:Does the 1-year log retention license apply to a) all ingested telemetry or b) alerts and incident-relevant logs only?

Response #32:All ingested telemetry

Question # 33:Is the Incident Response license intended to cover a) MDR-led investigation and containment only or b) extended IR services (forensics, recovery guidance, RCA)?

Response #33:Extended IR services(forensics, recovery guidance, RCA)

Question # 34: If monitored assets exceed the initial 300 licenses, should bidders assume proportional license true-ups or separate procurement?-

Response #34:Proportional license true-ups

Question #35:Should proactive threat hunting be assumed as a) continuous and platform-driven or b) periodic analyst-led engagements?

Response #35:A continuous and platform driven proactive threat hunting.

Question #36:Are detection tuning and new detection development expected to be a) continuous as part of standard MDR or b) customer-initiated / scheduled?

Response #36:Continuous as part of standard MDR.

Question #37:Are formal MDR quality assurance reviews expected to be a) continuous or b) milestone-based?

Response #37:Based upon continuous quality assurance reviews.

Question #38:Please confirm that offensive security / Red Team testing is out of scope unless separately authorized.

Response #38:Red Team Testing should be included as part of the service.

Question #39:Detailed count of devices, laptops, desktops, servers tablets?

Response #39:300 devices

Question #40:Are networking devices included in the monitoring, routers, switches, firewalls.

Response #40:Yes all devices are included.

Question #41:Can work be done remotely?

Question #41:The County will require On-site work.

SIGNED:

Paul J. Brennan

PAUL J. BRENNAN, FNIGP, NIGP-CPP, CPPO
DIRECTOR OF PURCHASING

ADDENDUM

12/9/25