This document is a draft Scope of Services/Technical Specifications for a future competitive contract Miami-Dade County anticipates entering into. Scope of Services/Technical Specifications is subject to change without notice.
This is not an advertisement.

SCOPE OF SERVICES

Miami-Dade County, hereinafter referred to as the County, as represented by the Miami-Dade County Information Technology Department (herein after referred to as ITD), will be soliciting proposals for an Enterprise Cybersecurity Services Solution (herein after referred to as the 'Solution'), inclusive of software, products, and services to support and maintain the County cybersecurity environment. The solution and associated managed cybersecurity services will augment ITD staff within the Security Operations Center (SOC) and enhance the County's cyber resilience to be able to prepare, respond, and recover from cyber threats.

The selected Proposer shall provide the following:

Enterprise managed cybersecurity services via a Proposer-provided Security Operations Center (SOC), including information and event analysis, first line analysis of security alerts and potential threats as well as assistance in and/or performance of security audits by the selected Proposer to the County. These services shall include regular meetings with County staff at defined intervals and as needed. The County expects that the selected Proposer will provide artificial intelligence based upon County data and other external sources for preemptive detection of security events to generate alerts and initial review/assessment of security threats, 24 hours per day, seven days per week, 365 days per year. Data, reporting, and dashboards pertaining to Proposer-managed security services should be made available to the County via a cloud hosted web-based Security Information and Event Management (SIEM) portal. The selected Proposer shall be responsible for providing project management and implementation services and training for the Proposer-managed cybersecurity services delivered under the resultant contract.

The proposed Solution must be able to integrate with existing technology products such as Qualys, Microsoft Exchange, Office/Microsoft 365, Microsoft Entra ID, Active Directory, Fortinet firewalls, Mandiant, Trellix, various versions of *NIX operating systems, as well as industry standard network switches currently in production within the County network as further described in this Solicitation. The proposed solution must integrate and process events from Amazon Web Services (AWS), Microsoft Azure, Oracle Cloud, and Google Cloud.

The County anticipates awarding a contract for a five-year term with one, five-year Option to Renew. The County intends to complete payment for the Solution via a payment schedule that will be negotiated with the selected Proposer.

1. Background / Operating Environment

The County, as a large and modern public agency, relies on numerous forms of technology to serve millions of constituents. It is the County's mission to protect data and information it collects through centralized oversight of privacy and cybersecurity risk mitigation protocols, and governance over cybersecurity and privacy program functions. The Information Technology Department (ITD) is responsible for providing network services and technical support to all County Departments and external customers.

All County network traffic runs through the County's three datacenters:

1. County's Data Processing and Communication Center located at: 5680 SW 87th Avenue, Miami, FL

2. County's (CAT5) Integrated Command Facility Building located at: 11500 NW 25th St, Doral, FL
3. Network Access Point (NAP) of the Americas located at: 50 NE 9th St, Miami, FL

ITD also manages the SOC responsible for monitoring and supporting the County's enterprise security services. ITD serves just under 30 departments providing multiple services and functions that need to be coordinated for a complex and diverse network with multiple locations. The SOC performs oversight activities that govern all IT security initiatives ensuring all IT service areas are working towards a common goal of protecting County assets from cyberattacks.

The operating system environment within Miami-Dade County's current network includes approximately 3,200 Windows and Linux servers; 20,000 Windows and 500 MacOS workstations; 6,000 iOS and Android mobile devices without Endpoint Security. Proposals shall be based on 30,000 Endpoints and 30,000 Users.

The County currently has an SMTP gateway that integrates with Microsoft Office 365, with on premise hosts, virtual machines, and other cloud solutions. The County currently employs ProofPoint email security and Defender messaging security. The County currently has an EDR solution that protects current and legacy systems, DMZ\SAZ servers, and cloud-based servers. The current EDR keeps servers and endpoints protected while reducing the risk of breach disclosure by detecting and stopping unauthorized system changes with application control, behavioral monitoring, and fileless threat inspection. Additionally, the County has Microsoft F5 and G5 licenses for approximately half of its users with the intention of migrating all of its users to G5 which includes EDR, email security, identity, and application protection. The County also currently has a network sandboxing and monitoring solution against targeted attacks, advanced threats, and ransomware. It uses virtual images of endpoint configurations to analyze and detect targeted attacks by applying web filtering with URL reputation, local content correlated with comprehensive threat intelligence, and lateral movement detection.

The County currently utilizes generation "F" for the Fortinet Fortigate firewalls which provide intrusion prevention across multiple zones across the County's network. ITD is responsible for providing technical support to all County Departments. There are just under 30 departments providing multiple services and functions that need to be protected from cyber-attacks. The County currently adheres to specific governmental and industry standards and regulations such as PCI, CJIS, and HIPAA. The County currently utilizes FireEye Helix as its SIEM/SEIM platform with additional and complementary capabilities provided by Microsoft Sentinel. The selected Proposer will be responsible for importing 13 months of historical data, or provide access to a searchable archive, from the County's existing SIEM/SEIM platform over to the proposed Solution to ensure compliance with security standards.

2. Architecture and Infrastructure Specifications

The County is open to an architecture that is cloud-based, Proposer-hosted, on premise/County-hosted, or any combination thereof required to deliver the comprehensive Enterprise Managed Cybersecurity Services Solution. Accordingly, Proposers may propose any of these methodologies in their Proposals, thereby allowing the County flexibility in selecting a deployment strategy that best suits operational needs. The architecture should allow the selected Proposer to provide same capabilities for air-gapped or non-internet-facing systems (such as secure public safety or utility systems) as is provided for those connected to the internet.

Proposed Solution's compatibility with the current County computing environment is required. The architecture should optionally include controls for sensitive data usage for the following: Data Loss Prevention (DLP) for OneDrive, SharePoint Online, Dropbox, Box, and Google Drive use pre-built and customizable compliance templates to control sharing of controlled data. Further, the architecture should protect file sharing from malware: Scans files shared from remote workers, partners, and mobile devices to ensure threats don't migrate through file sharing.

Cloud or Proposer-Hosted Specifications

For cloud or Proposer-hosted Solutions, the selected Proposer shall maintain availability of 99.982% uptime, calculated annually, not including routine maintenance or administrative procedures to be scheduled during non-business hours with prior notification the County. Cloud or Proposer-hosted Solutions should be designed to effectively mitigate latency and data speed issues. The selected Proposer shall provide appropriate bandwidth required to ensure optimal performance for concurrent application access and data access for normal daily operational use. It is required that hosting be contained within the Continental United States and/or United States territories.

On Premises/Self-Hosted Specifications

For on premise/County-hosted Solutions, Proposers shall adhere to the Miami-Dade County Technology Model and Hosting requirements. For on premises/County-hosted deployment, Proposer must install the applicable Solution components at the County's facility as a component of the implementation services more fully described in Section 2.6.

For on premises/County-hosted implementations, the applicable Solution components will reside and be maintained at the following facilities:

- Miami-Dade County's Data Processing and Communication Center located at: 5680 SW 87th Avenue, Miami, FL.
- Miami-Dade County's (CATEGORY 5 Hurricane Rated) Integrated Command Facility Building located at: 11500 NW 25th St, Doral, FL.

For on premise, the County expects to operate a test and production environment. The test environment can be set up as a small environment as it provides the system administrator with an environment for testing upgrades/patches before applying them to production. Functionality to push updates and data across environments to facilitate migrations is required. The County is open to Solutions that operate in a virtualized environment and desires VMware virtualization, except for databases servers.

Enterprise Managed Cybersecurity Services

The County is seeking a qualified Proposer capable of providing enterprise managed cybersecurity services to monitor the County's security environment, investigate incidents and/or provide guidance for remediation when exploits evade protection controls. It is anticipated that the selected Proposer will provide managed alerting and monitoring services, alerting the County to suspicious activity with telephonic incident response advice as well as continuous threat hunting, or managed IOC/IOA searching, for detection of threats and provide direct incident response remotely.

These managed services shall also include a dedicated technical analyst, regular meetings (either virtual or in-person) with County staff at defined intervals (weekly or as recommended by the selected Proposer and agreed to by the County) and as needed. Such meetings may be targeted towards specific mission critical operations, such as elections or public safety, as well as the general security needs of the County. The dedicated technical analyst shall also be the primary point of contact for questions, addressing security alerts, or briefing County staff on new and emerging threats and Zero Day vulnerabilities.

The selected Proposer should enable County SOC personnel to provide services as a managed security service provider (MSSP) to the County, as well as for potential expansion to other governmental entities. The Solution should be scalable such that all components can be expanded to allow the County to extend MSSP services to other local government entities serviced by ITD.

The County expects that the selected Proposer will employ Artificial Intelligence based upon County data and other external sources for preemptive detection of security events to generate alerts and initial review/assessment of security threats, 24 hours per day, seven days per week, 365 days per year. Data, reporting, and dashboards pertaining to Proposer-managed security services should be made available to the County via a Security Information and Event Management (SIEM) portal.

The selected Proposer may also be engaged in professional services during the resultant contract term to conduct assessment services, as requested by the County, to identify vulnerabilities and potential threats to County's data and systems. These services, upon request from the County, may include:

- Cybersecurity risk assessment services to allow for ITD to proactively prioritize risks, allocate resources, and help prevent costly cyberattacks.
- Vulnerability Assessment and Management services to identify and prioritize vulnerabilities, this capability assists in maintaining the security posture of digital assets.
- Cybersecurity Consulting Services to address a comprehensive assessment of vulnerabilities, security strategy development, and incident response guidance. May include hands-on assistance to strengthen County security controls, configuration, and overall, the cybersecurity program.

Managed Cybersecurity Services Information and Event Management (SIEM) Portal

The proposed enterprise managed cybersecurity services shall include County access to a SIEM portal as part of the comprehensive offering to the County. The SIEM portal should include the following capabilities:

1. Ability to ingest telemetry of security value from multiple sources (cloud, network, Endpoint, application, etc.)
2. Multi-tenant interface including both tenant and MSSP views.
3. A well-documented RESTful API, with parity between GUI and CLI.
4. SAML (SSO) authentication with support for disparate authentication sources per tenant and the MSSP.
5. Ability to forward alert detections via Syslog, Webhook, API, etc.
6. Ability to persistently track hosts, Users, and detections over time.
7. Ability to import custom IOCs, both manually with STIX data files and programmatically from TAXII-compliant threat feeds to trigger detections, and export IOCs to STIX data files and TAXII-compliant threat feeds to support information sharing.
8. Ability to correlate multiple detections and suspicious activity together to detect advanced threats (campaigns).
9. Provide whitelist detections for future tuning.

10. Provide bulk-triage detections.
11. Provide incident response capabilities.
12. Provide automated response orchestration (SOAR)
13. Ability to ingest network event data from NDRs that contains data from NetFlow in addition to SPAN & TAP.
14. Ability to ingest DNS and cloud (O365/Azure) generated data.
15. Provide configurable and exportable dashboards.
16. Provide customizable MSSP branding in UI, reports, generated emails, etc.
17. Import 13 months of data from the County current SIEM tool, HELIX, to ensure compliance with security standards.

Further, the County is seeking SIEM portal integration with the following:

1. BMC Remedy Service Desk Cloud for IT Incident Management (create and update incidents). The County is operating the current BMC Helix ITSM V21.30.00 version.
2. Microsoft Entra ID for User provisioning (SCIM) c. Microsoft Defender (and any other EDR products) for endpoint security event detections and response actions
3. Smart DNS services for event detections
4. SolarWinds for network monitoring
5. ForeScout or Extreme Control for network access control
6. Correlate events/info/telemetry from the following sources:
   - Microsoft Defender and any other EPP or EDR products
   - Other network information toolsets
   - Windows, Linux, AIX, and Apple system events
   - DHCP
   - DNS or DNS filtering tool to enrich existing detections
   - Fortinet or like firewalls

Reporting

The proposed Solution should include reporting tools for exporting statistics and search results, as well as the ability to export/import inbound/outbound policies. Proposed Solution should include reporting tools for exporting statistics and search results, as well as the ability to export/import inbound/outbound policies. The Solution should be sized to receive, analyze, enrich, and correlate 75,000 Events Per Second (EPS), allowing for growth of approximately an additional 25,000 EPS per year that the Solution is in service. The proposed SIEM/SEIM solution must retain 90 days of events immediately on-line and searchable at all times. The proposed SIEM/SEIM solution must also retain 13 months of event data in an archived, yet still searchable, manner.

The proposed Solution should include reporting capabilities that provide the following ITD with:

1. Dedicated reporting portal with ability to respond to immediate threats.

2. Configurable/Customized ad hoc reporting capabilities in addition to any canned reports. Proposer should fully describe as part of their Solution offering the available reports and associated capabilities.
3. Robust reporting functionality to ensure that when a large number of records are used to perform ad hoc retrieval from the stored information, the performance will not be adversely affected.
4. Provide risk-based vulnerability reporting and prioritization. Including the capability to report potential motivations behind attacks.
5. Support User-specified parameters that constrain the report content to specific date/time periods, malware type, device, etc. All parameters should be printed within the report.
6. Reporting that contains a library of customization and parameters for filtering.
7. Reporting on the various trends by malware type, action taken, and component detected, etc.
8. Ability to export data in multiple formats, including comma delimited format (CSV), Microsoft Excel, HTML, XML, and PDF.
9. Provide real-time, customizable dashboards to display dynamic charts and graphs.
10. Provide reports that show how the Solution is identifying and mitigating malware on the County network.
11. Provide reports that show how the email spam, phishing and spoofing security solution identifies and mitigates threats to the County network.
12. Ability to report on the percentage of the County's environment with most recent security definitions.
13. Attribution information and SIEM Portal Reporting.
14. Provide reports for guided analysis and remediation based on intelligence gathered by the vendor, (i.e., "the next steps needed to contain this threat are xyz."
15. SIEM Extensible reporting features.

Implementation

The selected Proposer will be responsible for providing cloud hosted or on-site installation, setup, and configuration services for the proposed Solution, including project management to establish the Proposer-managed security services. On-site services can be supplemented by remote support upon approval of the County project manager. In addition to those tasks outlined below, the selected Proposer will also be responsible for testing the proposed Solution and ensuring proper functionality The proposed implementation should include at minimum, the following tasks:

1. If applicable, configure all consoles and integrations of managed systems, as applicable, for the entire infrastructure using the selected Proposer's best security guidelines and best practices for implementation within the County's environment. All components need to be properly sized to handle the amount of endpoint agents, network traffic, email traffic and logs generated by the County.
2. If applicable, setup, provision, and configure the cloud or Proposer-hosted environment. All components need to be properly sized to handle the amount of endpoint agents, network traffic, email traffic and logs generated by the County.

Deliverables after Implementation

1. Detailed documentation containing diagrams and specific configuration of the Solution including ALL components as implemented for the County.
2. Detailed documentation containing diagrams and specific configuration of the Solution to address lateral movement detection and sandboxing as implemented for the County.
3. Review configuration for all Solution components with designated County staff to verify best practices have been implemented.
4. License keys, as applicable.
5. Support contact information and customer account information.

Training

Proposed Solution training is to be provided in conjunction with implementation, and as needed, during the term of the resultant Contract for all components. The training can be conducted either virtually or onsite at the following location: 5680 SW 87th Avenue, Miami, FL 33173. The County expects to have a minimum of 30 attendees; training will be coordinated with the selected Proposer and ITD.

The training should include the following topics, with materials customized to address the County's specific Solution configuration and proposer-managed security services, at minimum and for all components:

1. Troubleshooting process
2. How to identify outbreak incidents
3. How to address spam, phishing, and spoofing attacks
4. How to address zero-day attacks
5. Assistance in automating response activities
6. How to use forensic tools
7. How to whitelist/backlist to exclude false positives from all components
8. How to implement upgrades of major revisions
9. How to deploy critical updates
10. How to configure personal firewall
11. How to deploy agents remotely without requiring physical access
12. How to verify end-point agent deployment throughout the environment
13. How to support the different operating systems agents
14. How to run template and/or predefined reports
15. How to create customized reports
16. How to support Citrix environment
17. How to support virtual shielding
18. How to manage and support the threat analysis
19. How to manage and support the email protection component

Maintenance Services

During the term(s) of the resultant Contract, the selected Proposer shall provide the County with maintenance services, as listed below.

1. All Licensed Software furnished by the Proposer must be of the most recent release and all software upgrades issued by the selected Proposer must be available to the County at no additional charge. The software maintenance plan shall include the option, in the County's sole discretion, of installation of new releases by the selected Proposer at no additional cost.
2. Periodic updates and upgrades shall include correction of substantial defects, bug-fixes, fixes due to conflicts with mandatory operating system security patches, and upgrades to new version releases. Updates and upgrades must maintain compatibility with the County's configuration.
3. Zero-Day attack patches for all components.
4. Updates to the Solution must be provided to remain compliant with current security standards and policies.
5. If applicable, Remote Access to any County server providing the application services either by SSL VPN, Encrypted Connection, or dedicated IP address; access will require prior approval from the County.

Technical Support Services

In addition to the technical support services provided via the Proposer-managed security services, the selected Proposer should have a technical support staff available 24 hours per day, seven days per week, 365 days per year, and a method in which service tickets can be submitted electronically via email or phone and tracked. A dedicated technical account manager knowledgeable in the Solution implemented by the County must be provided. The Proposer should make available to the County a Global Knowledge online database to research technical issues with any Solution component provided under the resultant contract used in connection with the services employed.

The County desires an escalation and response time as listed below:

Severity Level	Definition	Response Time	Status Update
1=Critical/Outbreak/Outage	A major component of the Solution, whether hardware or software, is in a non-responsive state, creating security vulnerabilities in the County environment. or A major security outbreak or breach occurs.	15 minutes	One (1) Hour

Severity Level	Definition	Response Time	Status Update
2=Urgent	Any component failure or loss of functionality not covered in Severity 1, which is hindering operations, such as, but not limited to: excessively slow response time; functionality degradation; error messages	One (1) Hour	Two (2) Hours
3=Important	Lesser issues, questions, or items that minimally impact the workflow or require a work around.	Four (4) hours	Four (4) hours
4=Minor	Issues, questions, or items that don't impact the workflow. Issues that can easily be scheduled such as an upgrade or patch.	8 hours	Weekly Status Call

Performance Credits

In the event that the selected Proposer is unable to meet the target times for response or frequency of updates for support incidents as mutually agreed to by the parties in the resultant Contract, the County may assess performance credits to be used by the County for the acquisition of additional products or services available from the selected Proposer or monetary deductions from the next available invoice. The County anticipates a credit amount of $3,000 per day for Severity Level 1 issues and $2,500 per day for Severity Level 2 issues that do not meet the established metrics. Additionally, should the selected Proposer fail to meet the annual uptime requirements specified in Section 2.3.1 for Cloud or Proposer-hosted Solutions, the County anticipates a credit amount of $3,000 per additional hour of downtime. The parties acknowledge and agree that the amount/value of such performance credits does not account for the full business damages experienced by the County as a result of an unresolved support Incident and shall not be construed to be an assessment of the value of damages.

Optional Products and Services

The optional products and services as detailed below and the associated pricing, if applicable, are considered optional and are not included in the Scope of Services. As such, information provided for such an optional products or services will **NOT BE SCORED** as part of the evaluation process but may be considered at the sole discretion of the County in the future resultant contract.

A. Hardware / Appliances: Proposers are encouraged to provide any hardware, software, and/appliances recommended to work with the Proposed Solution to allow for scalability and future expansion during the term of the resultant contract. The County, in its sole discretion, reserves the right to purchase the recommended hardware, software, and/or appliances during the term of the resultant contract, as applicable. All pricing shall be provided as an **Option** and not included as part of the evaluation criteria. The County will work with the Selected Proposer to review the current infrastructure and develop a mitigation plan as part of the services to be delivered under the resultant contract.