بسم الله الرحمن الرحيم

Secretariat of Kulhudhuffushi City Council
Kulhudhuffushi, Rep of Maldives

Terms of Reference (TOR): Procurement of an Extended Detection and Response (XDR) Platform with Managed Detection and Response (MDR) Services.

1. Project Overview

Kulhudhuffushi Council seeks to procure an Extended Detection and Response (XDR) platform coupled with locally delivered Managed Detection and Response (MDR) services to strengthen its cybersecurity posture against evolving threats.

1.2 Key Requirements

- **Licensing:** 100 endpoint licenses with twelve-month coverage.
- **MDR Services:** 24/7/365 MDR services delivered from a Maldives-based Security Operations Center (SOC).
- **XDR Platform:** Commercial XDR platform meeting all specified technical requirements (enterprise-grade solution).
- **Deployment:** Cloud deployment with on-premises migration capability for future flexibility.

2. Vendor Eligibility Criteria

To be considered for this procurement, vendors must meet **all** the following requirements:

2.1 Legal and Registration Requirements

- Registered and incorporated under the laws of the Republic of Maldives.

2.3 Partnership and Authorization

- Authorized partner of the XDR platform's manufacturer.
- Valid manufacturer authorization letter for the proposed XDR platform.

2.4 Local Capacity Requirements

- Minimum five (5) locally based incident response engineers certified on the proposed XDR platform.
- All engineers must be direct employees of the vendor (no subcontracting of MDR staff).
- Security Operations Center **physically located in the Maldives**.
- Valid Maldives Police Service background clearance reports for all proposed MDR team members.

3. XDR Platform Technical Requirements

- **Product:** The Commercial Extended Detection and Response (XDR) platform (enterprise-grade) meets all requirements.
- **License Quantity:** 100 endpoints (devices)

- **License Period:** 12 months from activation
- **Deployment Model:** Cloud-based (Software-as-a-Service), with optional on-premises management server migration if required
- **Platform Coverage:** Compatible with Windows, macOS, and Linux operating systems
- **Data Retention:** Minimum 90 days of data retention for analysis and forensics

3.1 Endpoint Protection Features

- **AI-Driven Malware Detection:** Behavioral AI-based malware detection (signature-independent, relies on behavior analytics rather than known signatures).
- **Ransomware Protection:** Built-in ransomware protection with automated file recovery/rollback capabilities.
- **Fileless Attack Defense:** Detection and prevention of fileless attacks and in-memory threats.
- **Integrated Firewall & Control:** Integrated endpoint firewall and application control features.
- **Full Endpoint Visibility:** Comprehensive visibility into file activity, process execution, network connections, and registry changes on each endpoint.

3.2 Threat Detection and Analytics

- **Real-Time Detection:** Real-time threat detection with minimal false positives.
- **Detection Rules:** Pre-built detection rules with the ability to create and customize additional rules.
- **Threat Hunting:** Advanced threat hunting capabilities, including a dedicated query language for deep analysis.
- **Log Ingestion & Correlation:** Ability to ingest and correlate third-party logs (e.g. from firewalls, proxies, IDS/IPS, and SIEM systems) for centralized analytics.

3.3 AI-Enhanced Security Capabilities

- **Natural Language Queries:** Support for natural language threat hunting and Indicator of Compromise (IOC) queries to simplify complex searches.
- **AI-Enriched Alerts:** AI-enriched alert summaries that provide context and recommended actions.
- **Proactive AI Suggestions:** AI-suggested threat hunting queries based on emerging threat landscapes and patterns.

3.4 Integration and Interoperability

- **Open API Integration:** RESTful API available for integration with external systems (SIEM, SOAR, ITSM/ticketing platforms).
- **SIEM/SOAR Compatibility:** Compatibility with major Security Information and Event Management and Security Orchestration, Automation and Response tools to enable data sharing and automated response.

- **Infrastructure Integration:** Real-time alert integration with other infrastructure data sources (network devices, servers, etc.) for a comprehensive threat of visibility.

3.5 Management and Administration

- **Unified Console:** Unified management console for centralized monitoring, policy configuration, and enforcement across all endpoints.
- **Centralized Updates:** Centralized deployment of agent updates with no forced reboots (non-disruptive updates to endpoints).
- **Access Control:** Granular role-based access control for administrators and analysts using the platform.
- **Compliance Reporting:** Built-in compliance reporting capabilities (templates/reports for standards such as PCI DSS, HIPAA, SOC 2, etc.).

4. Managed Detection and Response (MDR) Service Requirements

4.1 Service Delivery Model

- **Continuous Monitoring:** 24/7/365 threat monitoring, investigation, and response by the service provider.
- **Local Operations:** All services are delivered by a Maldives-based SOC facility.
- **In-House Staff:** All SOC personnel are direct employees of the vendor (no outsourcing of monitoring or response functions).

4.2 Service Components

- **Onboarding Support:** Guided onboarding process and deployment assistance for the XDR platform.
- **Custom Detection Rules:** Development and tuning of custom threat detection rules tailored to the organization's environment and suspicious activity patterns.
- **Threat Hunting Campaigns:** Conducting regular proactive threat hunting campaigns to identify hidden or advanced threats.
- **Continuous Rule Improvement:** Ongoing custom detection rule development and refinement as new threats and client needs emerge.
- **Incident Collaboration:** Collaborative incident investigation and mitigation support (working with the Council's IT/security team during incidents).
- **Incident Response Retainer:** An incident response retainership covering all licensed endpoints, ensuring that incident response services are available on demand for those systems.

4.3 Response Time Commitments

The MDR provider must adhere to the following maximum response times based on incident severity:

- Critical incidents: 1-hour maximum response time
- High severity: 2-hour maximum response time
- Medium/Low severity: 8-hour maximum response time

Response time is measured from the detection of an actionable security incident to the initiation of remediation actions by the MDR team.

4.4 Compliance and Regulatory Requirements

- Full compliance with applicable Maldives data protection regulations for handling sensitive data.
- Adherence to national cybersecurity standards and any sector-specific regulations.
- Clear communication protocols for alert notifications and incident status updates (ensuring the Council is informed of threats and response progress in a timely manner).

5. Deployment and Support and Training

5.1 Deployment Flexibility

- **Migration:** Support for migrating from a cloud-hosted deployment to an on-premises environment if future policies or preferences require it.
- **Hybrid Deployment:** Capability for hybrid deployment, allowing management of both cloud and on-premises endpoint environments seamlessly.
- **Automated Deployment:** Availability of automated endpoint agent deployment mechanisms (to rapidly install the XDR agent across all endpoints).
- **On-Premises Option:** Ability to transition to an on-premises management server provided by the platform vendor, if required by the Council.

5.2 Technical Support

- **24/7 Support:** 24/7 technical support availability, with defined incident escalation procedures (global support access and local escalation as needed).
- **Customized Playbooks:** Customizable incident response playbooks tailored to the Council's environment, provided as part of the service.
- **Automated Workflows:** Support for configuring automated workflows within the XDR platform or associated tools to streamline detection and response processes.

5.3 Training

- A total of 4 IT staff members should be trained. Software-based training must be delivered physically to these IT staff members.
- The cost incurred for conducting the training must be included in the bid. This must include all expenses related to the trainers' travel, accommodation, and meals.
- Council will provide a hall for conducting the training. Furthermore, the training must be arranged within 10 days of the completion of this work.
- The total cost of the work will only be paid upon the successful completion and delivery of the training.

Secretariat of Kulhudhuffushi City Council
Kulhudhuffushi City, Maldives

6. Submission Requirements

6.1 Mandatory Documents

Vendors must include the following documents in their proposal submission:

- Company Registration Certificate (proof of incorporation in Maldives).
- Company Profile sheet (updated within the last 4 months).
- GST Registration Certificate.
- Manufacturer Authorization Letter for the proposed XDR platform (Proof of authorization from the solution vendor).
- Maldives Police Service reports (background clearance) for all proposed MDR team members.
- Quotation or Financial Proposal (with all prices in Maldivian Rufiyaa and inclusive of GST).
- Technical Proposal (detailed as described below).

6.2 Technical Proposal Contents

The technical proposal must include:

- **Deployment Plan:** A detailed deployment plan for the XDR platform and services, with timeline and milestones from project kickoff to full operation.
- **Technical Details:** Technical specifications of the proposed solution and architecture diagrams illustrating how the XDR platform and MDR service will be implemented in the Council's environment.
- **Service Level Agreements:** A description of Service Level Agreements (SLAs), including guaranteed response times for various incident severities (as outlined in this TOR).
- **Local Delivery Confirmation:** A confirmation statement that MDR services will be delivered by a Maldives-based SOC with staff who are direct employees of the vendor.
- **Project Team Profile:** Proposed project team profiles, including:
    - Relevant XDR platform certifications held by each team member (demonstrating expertise in the proposed solution).
    - Role assignments and responsibilities for this project (e.g., Project Manager, Lead Analyst, Incident Responder, etc.).