بسم الله الرحمن الرحيم

Ministry of Economic Development, Transport and Trade
Male', Republic of Maldives

ވިޔަފާރި، ޓްރާންސްޕޯޓް، ފަރާތްތަކާއި ވިއުޅުންތަކުގެ ވަޒާރާ
މާލެ، ދިވެހިރާއްޖެ

SHOPPING FOR CYBER PROOFING TRADIAN (NSW): SUPPLY, INSTALLATION, AND COMMISSIONING OF A UNIFIED AI-DRIVEN SECURITY OPERATIONS PLATFORM AND NETWORK OPERATIONS CENTER (NOC) / SECURITY OPERATIONS CENTER (SOC) CONTROL ROOM LED DISPLAY SOLUTION INCLUDING TECHNICAL SUPPORT AND PROFESSIONAL SERVICES

for

Maldives Innovation & Digital Company Limited (MINDCo)

ANNEX1-REQUEST FOR QUOTATION (RFQ)

Source of Funding: ADB Loan 3794 – MLD and ADB Grant 0646 – MLD

RFQ Ref: RFQ/2026/004

South Asia Subregional Economic Cooperation
National Single Window Project

SECTION A
SCOPE OF WORK

Under the National Single Window Platform digital initiative, Maldives Innovation and Digital Company (MINDCo) seek to enhance its cybersecurity resilience through the implementation of a next-generation, Unified Security Operations (SecOps) platform. This Request for Proposal (RFP) invites qualified and experienced Systems Integrators to submit proposals for the **SUPPLY, INSTALLATION, AND COMMISSIONING OF A UNIFIED AI-DRIVEN SECURITY OPERATIONS PLATFORM AND NETWORK OPERATIONS CENTER (NOC) / SECURITY OPERATIONS CENTER (SOC) CONTROL ROOM LED DISPLAY SOLUTION INCLUDING TECHNICAL SUPPORT AND PROFESSIONAL SERVICES**.

The scope of work encompasses the design, supply, installation, configuration, integration, testing, commissioning, and knowledge transfer of:

- A unified Security Operations platform delivering endpoint security for all critical endpoints including servers, Cyber Risk Exposure Management for critical on-premises assets, Cloud Risk Management for cloud assets, Agentic Security Information and Event Management (SIEM) with basic Security Orchestration, Automation and Response (SOAR) capability, Network Detection and Response (NDR), and a Unified Security Monitoring and Management platform.
- A high-resolution fine-pitch indoor LED display system for the NOC/SoC control room, comprising LED display modules, video processing and control system, mounting infrastructure, accessories, and spare components.

MINDCo has established a mission-critical Data Centre environment comprising HPE server infrastructure virtualized to run RedHat Enterprise Linux workloads, Fortinet Security Fabric (FortiGate next-generation firewalls, FortiManager, FortiSwitch), Cisco Distribution Switches, Aruba Core Switches, and centralized log collection via SolarWinds Kiwi Syslog Server. The proposed solution shall ensure compatibility with the existing infrastructure, provide unified visibility across the security stack, minimize operational complexity, and support optimal and continuous operations for the National Single Window Platform.

The supplier shall be an experienced and reputable systems integrator with thorough knowledge and understanding of enterprise security solutions, with a proven background in installing, configuring, and maintaining such systems in high-availability government and enterprise environments.

SECTION B – CLIENT REQUIREMENTS

SUPPLY, INSTALLATION, AND COMMISSIONING OF A UNIFIED AI-DRIVEN SECURITY OPERATIONS PLATFORM AND NETWORK OPERATIONS CENTER (NOC) / SECURITY OPERATIONS CENTER (SOC) CONTROL ROOM LED DISPLAY SOLUTION INCLUDING TECHNICAL SUPPORT AND PROFESSIONAL SERVICES

#	Description
1	**SUPPLY, INSTALLATION, AND COMMISSIONING OF A UNIFIED AI-DRIVEN SECURITY OPERATIONS PLATFORM AND NETWORK OPERATIONS CENTER (NOC) / SECURITY OPERATIONS CENTER (SOC) CONTROL ROOM LED DISPLAY SOLUTION INCLUDING TECHNICAL SUPPORT AND PROFESSIONAL SERVICES**
1.1	**Enterprise SecOps Software Licenses (2-Year License)** • The vendor shall supply all necessary software licenses for a unified SecOps platform, including but not limited to: • Unified Security Monitoring and Management Platform • Agentic SIEM Module - Data Ingestion: 25GB/day with 30 Days Retention • Agentic SIEM Module - Archive Data Retention: 60 Days • Endpoint Detection and Response (XDR) for Endpoints (including servers): 30 Endpoints • Network Detection and Response (NDR): Virtual Appliance, 500Mbps Throughput • Cyber Risk Exposure Management: 50 Assessed Devices and Network Infrastructure Devices • Cloud Risk Management: 5 Cloud Assets
1.2	**Professional Services for Implementation, Configuration, Integration and Knowledge Transfer for Enterprise SecOps Platform**
1.3	**Network Operations Center (Noc) / Security Operations Center (Soc) Control Room LED Display Solution**
1.4	**Professional Services for Installation, Configuration, and Knowledge Transfer for NoC/SoC Control Room LED Display**
1.5	**Technical Support and Comprehensive Maintenance Services**
1.6	**Training and Knowledge Transfer**
1.7	**Sign-Off Documentation and As-Built Documentation**

SECTION B
TECHNICAL REQUIREMENTS

#	Description	Qty
1	**SUPPLY, INSTALLATION, AND COMMISSIONING OF A UNIFIED AI-DRIVEN SECURITY OPERATIONS (SECOPS) PLATFORM AND NETWORK OPERATIONS CENTER (NOC) / SECURITY OPERATIONS CENTER (SOC) CONTROL ROOM LED DISPLAY SOLUTION INCLUDING TECHNICAL SUPPORT AND PROFESSIONAL SERVICES**	**1 LOT**
1.1	**Enterprise SecOps Software Licenses (2-Year License)**	**1 Bundle**
1.1.1	General Platform Capabilities • Unified SIEM, XDR, and SOAR Platform: Integrated SIEM log management, XDR telemetry correlation, and SOAR orchestration in a single cloud-native platform. • Agentic AI Architecture: AI agents that autonomously detect, investigate, and respond to threats with minimal human intervention. • Natural Language Security Operations: Enable analysts to interact using natural language queries for investigation and response. • Multi-Tenancy Support: Multiple business units with isolated views and role-based access controls within a single console. • High Availability and Service Resilience: Enterprise-grade availability with documented SLAs and fault tolerance mechanisms.	1 Nos
1.1.2	AI-Driven Detection & Threat Intelligence • Behavioral Anomaly Detection: ML-based identification of deviations from normal user and entity behavior. • Custom Detection Rule Creation: Custom correlation rules and detection models for organization-specific threats. • Threat Intelligence Integration: Global and third-party threat intelligence feeds with automatic IoC matching. • MITRE ATT&CK Mapping: Automatic mapping of detected threats to MITRE ATT&CK TTPs. • Zero-Day Threat Protection: Detection of unknown malware without signature reliance.	
1.1.3	Data Ingestion & Log Management • Third-Party Log Source Support: Ingest logs from Fortinet, Cisco, Aruba, HPE, Kiwi Syslog, identity providers, and cloud platforms. • Flexible Data Retention: Customizable retention based on log type and compliance requirements. • High-Volume Data Ingestion: Real-time processing of 25GB/day with minimal latency. • Data Compression and Optimization: Indexing, compression, and deduplication for storage and query performance.	
1.1.4	Investigation & Threat Hunting • Unified Search Across Data Sources: Single search interface for native telemetry, third-party logs, and historical data. • AI-Powered Investigation Assistance: AI-driven tools accelerating triage, analysis, and incident response. • Threat Hunting Query Library: Predefined and custom threat hunting queries. • Attack Chain Visualization: Visualize attack progression and relationships between events, users, devices, and processes. • Retroactive Threat Detection: Scan historical data with new detection models and threat intelligence	
1.1.5	Automated Response & SOAR • Security Playbook Automation: Pre-built and customizable playbooks for automated incident response.	

	• Endpoint Response Actions: Automated isolation, process termination, and malware scanning. • Identity and Access Response: Integration with identity providers for user disable, password reset, and force sign-out. • ITSM and Case Management Integration: Bi-directional sync with ticketing systems. • Third-Party Security Tool Orchestration: API-driven orchestration across third-party security tools.	
1.1.6	Compliance & Security • Compliance Framework Support: GDPR, NIS2, NIST CSF, ISO 27001, PCI DSS, HIPAA, SOX. • Audit Trail and Tamper-Proof Logging: Comprehensive, tamper-proof audit logs of all actions and changes. • Data Encryption in Transit and at Rest: Industry-standard encryption. • Multi-Factor Authentication and SSO: SAML 2.0 and MFA with mobile authenticator apps. • Role-Based Access Control (RBAC): Fine-grained RBAC with custom role creation and asset visibility scoping.	
1.1.7	Performance & Scalability • Elastic Cloud-Native Architecture: Auto-scaling without manual capacity planning. • Query Performance at Scale: Sub-second query performance across large datasets. • Pre-Ingestion Data Filtering: Filter unneeded logs before ingestion to manage costs. • Global Search Performance Limits: Documented search performance limitations and result pagination.	
1.1.8	Integration & API Access • Comprehensive RESTful API: Well-documented, secure RESTful APIs for all platform functions. • Native SIEM Integration: Native connectors for major third-party SIEM platforms. • Cloud Platform Integration: AWS, Azure, GCP security monitoring and response. • Identity Provider Integration: Entra ID, Okta, Google Workspace for authentication and monitoring. • SASE and Network Security Integration: Integration with SASE solutions and network security vendors.	
1.1.9	Operational Management • Expert Support: 24/7 technical support with documented response times and escalation procedures. • Managed SIEM Services (Optional): Optional managed services for SIEM operations. • Sandbox Integration: Malware sandbox for dynamic file detonation and analysis.	
1.1.10	License • Agentic SIEM Module - Data Ingestion: 25GB/day with 30 Days Retention, 2-Year License • Agentic SIEM Module - Archive Data Retention: 60 Days, 2-Year License	
1.1.11	**Endpoint Detection and Response (XDR)** • Real-time behavioral analysis and threat detection for Windows and Linux endpoints, including RedHat Enterprise Linux server workloads. • Automated response actions: endpoint isolation, process termination, file quarantine, and malware scanning. • Threat intelligence integration and automated IoC matching across endpoints. • MITRE ATT&CK mapping for all detected endpoint threats. • Offline protection mode with local policy caching. • Agent-based deployment with optimized resource utilization. • Integration with the unified platform for cross-layer correlation and unified endpoint visibility. • Support for virtual server environments and container-aware detection where applicable. • License: Endpoint Detection and Response (XDR), 2-Year License	30 Nos
1.1.12	**Network Detection and Response (NDR) - Virtual Appliance, 500Mbps** Intrusion Prevention System (IPS) • Real-time network traffic inspection and threat detection at packet and application layer.	1 Nos

	• Vulnerability Protection via Virtual Patching: IPS rules blocking exploit traffic targeting unpatched vulnerabilities; protection against zero-day exploits 90-120 days before vendor patches are available. • IPS Rule Management & Customization: Granular control per-policy, per-computer, or per-segment; Detection mode for safe testing; individual rule exceptions. • Attack/Threat Classification & Categorization: Logical categories enabling risk-based response. • High-Speed Network Processing: Line-rate performance through optimized network processors; full throughput regardless of rule set size. <u>Network Detection and Response (NDR)</u> • Network behavior analysis and anomaly detection: Baseline establishment with detection of compromised systems, lateral movement, and data exfiltration. • Threat Investigation Center with correlated threat intelligence; retro-scan capability for command and control communications. • Real-time alerting and threat notification with severity ranking and contextual information. • Encrypted traffic inspection (TLS/SSL): Advanced TLS Traffic Inspection supporting TLS 1.2/1.3; detection of malware and C2 inside encrypted channels. • Threat intelligence integration: Global threat intelligence (including zero-day disclosures) plus external threat feeds via API and SIEM integration; automatic updates. <u>Network Asset Discovery & Vulnerability</u> • Network device and asset discovery: Passive and active scanning with unified asset inventory spanning on-premise, cloud, and hybrid environments. • Vulnerability assessment on discovered network assets: Risk-scoring based on criticality, exploitability, and active threat intelligence. <u>Automated Response & Containment</u> • Automated response actions: Block IPs, disable user accounts, isolate network segments, escalate to SOC. • Threat containment and isolation: Endpoint-level network isolation and network-level firewall blocking; automatic sandbox detonation. <u>Logging, Compliance & Performance</u> • Network security logging and audit trails: Comprehensive logs of IPS detections, firewall blocks, and anomalies; queryable and forwardable to Kiwi Syslog and external SIEM via TLS or UDP. • PCI-DSS, HIPAA, SOC 2 compliance support for network controls. • High-throughput network processing (500Mbps sustained) with sub-millisecond detection latency. • Scalability: Support for thousands of concurrent network flows with stateful connection tracking. • Flexible deployment: Virtual appliance form factor deployable within the Client's HPE virtualized infrastructure. <u>Management & Security</u> • Integration with existing security tools: Native API integrations; SIEM connectors; SOAR automation. • Single management console unified with the SecOps platform. • Encrypted management communication (TLS 1.2/1.3) and data encryption at rest. • FIPS 140-2 compliance support. • Role-based access control (RBAC) with granular predefined and custom roles. • REST API for automation and orchestration with OAuth 2.0 and webhook support. • Centralized policy deployment with version control and staged deployment capability. • High availability and appliance failover with offline policy caching and local fail-open mode. • Disaster recovery with automated backups and configuration snapshots. <u>License:</u> • Network Detection and Response (NDR) - Virtual Appliance (2-Year License)	
1.1.13	**Cyber Risk Exposure Management - 50 Assessed Devices, 2 Year License** <u>General Capabilities</u>	1 Nos

- Unified visibility into cyber risk exposure across on-premises, cloud, and hybrid environments.
- Continuous monitoring and identification of entry points exploitable by attackers.
- Translation of cyber risks into business-relevant terms for executive reporting.
- Support for both reactive threat response and proactive risk management.
- Risk scoring considering asset criticality, vulnerabilities, threat activity, and control effectiveness.

<u>Asset Discovery & Management</u>

- Automatic discovery of all managed and unmanaged assets across the organization.
- Identification and monitoring of internet-facing and external attack surface assets.
- Asset categorization, tagging, grouping, and criticality assessment.
- Asset relationship visualization showing connections between assets.
- Visibility into device hardware information and configurations.

<u>Vulnerability Management</u>

- Comprehensive vulnerability assessment across operating systems and applications.
- Prioritization based on exploitability, exposure, and threat intelligence.
- Vulnerability metrics including mean time to patch and average unpatched time.
- High-impact CVE filtering for focused remediation.
- Integration with third-party vulnerability scanners.

<u>Risk Assessment & Prioritization</u>

- Dynamic risk scores to assets monitored over time.
- Detailed risk indicators: risk type, triggering events, and risk levels.
- Quick and frictionless risk assessments across on-premises and cloud assets.
- Filtering and querying based on risk criteria (discovery date, criticality, internet exposure, device category).
- Risk event lifecycle management: dismissal, acceptance, remediation tracking, in-progress status.

<u>Attack Path Analysis & Prediction</u>

- Prediction of potential attack paths from an attacker's perspective.
- Identification of entry points and choke points in attack chains.
- Proactive remediation recommendations for critical assets in attack paths.
- Visualization of cloud asset relationships including AWS and Azure environments.

<u>Identity Security & Access Management</u>

- Assessment of identity security posture and identity-related risks.
- Integration with Microsoft Entra ID for identity asset discovery and management.
- Monitoring of user and device risk scores.
- Identification of privilege escalation risks and excessive permissions.

<u>Compliance & Security Posture Management</u>

- Compliance management for industry standards and frameworks.
- CIS Benchmarks support for AWS, Azure, Google Cloud.
- Control effectiveness and maturity evaluation.
- Cloud Infrastructure Entitlement Management (CIEM).
- Infrastructure-as-code security scanning (CloudFormation, Terraform).

<u>Threat Intelligence & Detection</u>

- External threat intelligence informing risk prioritization.
- Internal detection data integration for comprehensive threat visibility.
- MITRE ATT&CK framework mapping.
- Historical cyber incident data and financial impact records.

<u>Automation & Orchestration</u>

- Automated threat response through security playbooks.
- Automation for vulnerability detection events and remediation.
- Integration with third-party SOAR platforms.
- Automated response: endpoint isolation, file quarantine, network blocking.

	<u>Reporting & Dashboards</u> • Executive dashboards with business-relevant risk metrics. • Standardized and customizable report generation. • Drill-down capabilities for detailed analysis. • Tracking of remediation progress and mitigation effectiveness over time. <u>Integration & Data Sources</u> • Integration with AWS, Azure, Google Cloud. • Agentless vulnerability and threat detection for cloud workloads. • Integration with endpoint security platforms and telemetry collection. • Network vulnerability scanning and sensor data integration. • SIEM integration for centralized event correlation. • Third-party security tool integration via APIs. • Multiple data ingestion: Syslog, REST API, agent-based log forwarding. <u>SaaS & Cloud Application Security</u> • Visibility into cloud application usage (sanctioned and unsanctioned). • Microsoft 365 SaaS security posture management. • API risk visibility and security assessment. • Malware scanning for cloud storage and SaaS applications. <u>Training & Awareness</u> • Security awareness training capabilities. • Phishing simulation campaigns. <u>Deployment & Scalability</u> • Cloud-based SaaS platform requiring minimal infrastructure. • Scalable to enterprise environments. • Multi-tenancy support. • Rapid deployment with minimal configuration.	
1.1.14	**Cloud Risk Management - 5 Cloud Assets, 2 Year License** • Continuous security posture management for cloud workloads and services across AWS, Azure, and GCP. • Cloud asset discovery, inventory, and relationship mapping. • Cloud configuration assessment against CIS Benchmarks and compliance frameworks. • CIEM capabilities: detection of excessive permissions, privilege escalation, and entitlement risks across cloud identities. • Cloud vulnerability scanning and agentless threat detection. • Integration with the unified platform for unified cloud and on-premises risk visibility. • Infrastructure-as-code security scanning (CloudFormation, Terraform). • API risk visibility and security assessment for cloud-native applications.	1 Nos
1.2	**Professional Services for Implementation, Configuration, Integration and Knowledge Transfer for Enterprise SecOps Platform**	**1 Service**
1.2.1	<u>Project Management</u> • Dedicated Project Manager. • Detailed project plan with milestones, resource allocation, and risk management.	
1.2.2	<u>Solution Design & Architecture</u> • As-is assessment of existing Fortinet, Cisco, Aruba, HPE, RedHat, and Kiwi Syslog infrastructure. • To-be SecOps architecture design aligned to National Single Window security requirements. • Network topology and data flow diagrams for platform deployment. • Sizing and capacity planning for SIEM ingestion and NDR traffic analysis.	
1.2.3	<u>Installation & Deployment</u> • Installation and baseline configuration of the unified platform and all licensed modules. • Deployment of endpoint agents across 100 endpoints including HPE virtualized RedHat servers.	

	• Deployment and configuration of NDR virtual appliance within the existing virtualized environment. • Configuration of data ingestion pipelines from Fortinet (FortiGate, FortiManager, FortiSwitch), Cisco switches, Aruba core switches, HPE servers, RedHat operating systems, and Kiwi Syslog Server. • Configuration of Agentic SIEM data parsing, normalization, and correlation rules.	
1.2.4	Integration Services • Bi-directional integration with Fortinet Security Fabric for threat intelligence sharing and automated response. • Integration with existing Kiwi Syslog Server for log forwarding and archival. • SIEM connector configuration for third-party devices. • SSO/SAML 2.0 integration with Client identity provider. • SOAR playbook development for common incident types (malware, lateral movement, data exfiltration).	
1.2.5	Configuration & Tuning • Baseline security policy configuration. • Custom detection rule creation for National Single Window specific threat scenarios. • Risk scoring calibration for Cyber Risk Exposure Management based on Client asset criticality. • False positive tuning and threshold optimization. • Dashboard and report customization for executive and operational stakeholders.	
1.2.6	Testing & Commissioning • Functional testing of all SecOps modules. • Integration testing with existing infrastructure. • Performance validation: SIEM query response, NDR throughput, endpoint agent resource utilization. • User acceptance testing (UAT).	
1.2.7	Local 2-Year On-site Technical Support Services and Labour for Enterprise SecOps Platform	1 Service
1.2.8	Local 2-Year SW Configuration, Migration Services, and Change Request for Enterprise SecOps Platform	1 Service
1.3	**Network Operations Center (Noc) / Security Operations Center (Soc) Control Room LED Display Solution**	**1 Bundle**
1.3.1	LED Display Modules • Display Technology: Fine-pitch indoor full-color LED display with SMD triad LED pixel configuration. • Pixel Pitch: 1.25 mm (P1.2 category) with pixel density of 640,000 dots/m². • Module Dimensions: 300 mm (W) × 168.75 mm (H) with module resolution of 240 × 135 pixels. • Cabinet Dimensions: 600 mm (W) × 337.5 mm (H) × 29.5 mm (D); cabinet area 0.2025 m²; cabinet weight ≤ 3.4 kg. • Cabinet Material: Aluminium die-casting with front maintenance capability for all components. • White Balance Brightness: 600 cd/m² with color temperature adjustable from 3,000 K to 10,000 K. • Viewing Angle: 160° (H) / 160° (V). • Contrast Ratio: 5,000:1. • Color Uniformity: ≤ ±0.003 Cx, Cy. • Brightness Uniformity: ≥ 97%. • Refresh Rate: 3,840 Hz with frame frequency of 60 Hz. • Grey Level: 16-bit processing depth. • Driving Method: Constant current driving. • Input Voltage: 100–240 VAC ± 10%.	100 Module
1.3.2	Mounting Brackets • Type: Modular ultra-thin mounting bracket compatible with 600 × 337.5 mm cabinet form factor.	25 Nos

	• Design: Wall-mount or structural support bracket with precision alignment capability for seamless cabinet splicing. • Material: High-strength steel or aluminum alloy with anti-corrosion coating. • Adjustability: Support for fine-tuning of cabinet position to ensure flush alignment and gap consistency.	
1.3.3	Cabinet Frame • Type: 600 × 337.5 mm cabinet frame structure with integrated dual receiving card and dual power supply slots. • Compatibility: Support for COB, HOB, and SMD LED lamp boards (FHD/UHD resolution). • Design: Highly integrated and lightweight; easy disassembly of lamp board, power supply, and receiving card. • Maintenance: Complete front maintenance capability with modular structure design.	25 Nos
1.3.4	Video Processing System • Video Wall Controller Chassis: 6-slot standard rack-mount chassis (2U form factor) with mixed installation of input and output boards. • Chassis Features: 4.5-inch full-color touch LCD panel; 2 × USB 2.0 + 1 × Type-C interface; 1 × 1000 Mbps Ethernet control port; RS-232/485 serial interface; Genlock synchronization input and loop-through output. • Power: 100–240 VAC, 50/60 Hz. • Processing Depth: 8/10 bit with signal sampling quality up to RGB 10:10:10. • Video Wall Functions: Support for up to 8 video walls; 128 preset scenes; windowing, roaming, and arbitrary layer windowing; background image support (3 × 2K); subtitle overlay (24 total, 3 per wall, 512 characters each). • Input Boards: 4K HDMI input board (2 channels, HDMI 2.0, 4K@60 Hz, HDCP 2.3); 4K DisplayPort input board (2 channels, DP 1.2, 4K@60 Hz, HDCP 2.3). • Output Boards: 4K HDMI output board (2 channels, HDMI 2.0, 4K@60 Hz); support for LED screen custom resolution output up to 8.84 MP per port. • Decoding Capability: 48 channels of 1080p@30 fps; support for H.264, H.265, Smart264, Smart265, MJPEG. • HDR Support: HDR10 and HLG compliant with SMPTE ST 2084/SMPTE ST 2086 standards. • Audio: 48 kHz sampling rate; HDMI composite audio; 3.5 mm audio input/output on main control board. • 01 Nos x Chassis • 02 Nos x Input Board (4K HDMI). • 01 Nos x Output Board (4K HDMI).	01 Nos
1.3.5	LED Controller • Type: 20-port 2-in-1 LED controller with 1U rack-mount chassis. • Video Input: 1 × HDMI 2.0 (4K@60 Hz, HDCP 2.2), 1 × HDMI 1.4 (1080p, HDCP 1.4), 1 × DVI (1080p, HDCP 1.4). • Video Output: 20 × RJ-45 Gigabit Ethernet ports; maximum loading capacity 13 MP; single port load 650,000 pixels (width 144–8192, height 64–8192). • Video Loop Output: 1 × HDMI 2.0 + 1 × DVI for cascading or monitoring. • Video Live View: 1 × HDMI 1.4 output at 720p@60 Hz. • Audio: 1 × 3.5 mm audio output; HDMI embedded and in-band audio input support. • Control: 2 × 10/100/1000 Mbps Ethernet ports (RJ-45); RS-485 central control serial port; IR remote control and RF remote control support. • Display: 128 × 64 full-color OLED non-touch screen. • Brightness Control: 1 to 100 tunable (level-by-level white balance). • Input Frame Rate: 25 Hz to 120 Hz. • Power: 100–240 VAC, 50/60 Hz; average consumption ≤ 43 W. • Operating Environment: -10°C to 50°C; humidity 10% to 90% RH.	01 Nos

1.3.6	Accessories • 01 Nos x Front Maintenance Tool • 02 Nos x Main Power Cable • 05 Nos x Main Network Cable (Cat6 UTP) • 08 Nos x LED Module (same specification as primary modules) - Spare • 01 Nos x HUB Board - Spare	01 Nos
1.3.7	Local 2-Year On-site Technical Support Services and Labour for NoC/SoC Control Room LED Display System	1 Service
1.3.8	Local 2-Year HW Configuration, Migration Services, and Change Request for NoC/SoC Control Room LED Display System	1 Service
1.4	**Professional Services for Installation, Configuration, and Knowledge Transfer for NoC/SoC Control Room LED Display**	**1 Service**
1.4.1	Project Management • Dedicated Project Manager. • Detailed project plan with milestones, resource allocation, and risk management.	
1.4.2	Solution Design & Architecture • NOC/SoC control room LED display layout design, viewing distance analysis, ambient lighting assessment, and ergonomic positioning. • LED display signal path architecture: video wall controller input mapping, LED controller port allocation, and source switching logic.	
1.4.3	Installation & Deployment • LED display system installation: cabinet frame assembly, module mounting, bracket alignment, structural integrity verification, and seismic anchoring where required. • Video wall controller and LED controller rack-mount installation, power distribution, cabling management, and signal path verification. • LED display pixel mapping, color calibration, brightness uniformity adjustment, and white balance tuning across all modules. • Power and network infrastructure readiness verification for both SecOps platform and LED display system. • LED display integration with video wall controller for multi-source content display: SOC dashboards, NOC monitoring, CCTV feeds, and emergency alert overlays. • Content management system configuration for dynamic dashboard rotation and scheduled display layouts. • Video wall controller scene preset configuration for different operational modes: normal monitoring, incident response, executive briefing, maintenance mode.	
1.4.4	Testing & Commissioning • LED display pixel defect inspection, dead pixel mapping, color consistency verification, and refresh rate validation. • Video wall controller input/output signal path testing, source switching validation, and failover verification. • LED display thermal stress testing under continuous 24-hour operation.	

1.5	**Technical Support and Comprehensive Maintenance Services (2-Year)**
	• Service Level Requirement
	    ○ 8×5 Local Technical Support.
	    ○ Critical (P1): 1-hour response, 4-hour resolution
	    ○ Medium (P2): 4-hour response, 24-hour resolution
	    ○ Low (P3): 24-hour response, 72-hour resolution
	• Proactive health monitoring and monthly platform health checks for SecOps infrastructure.
	• Software patch management and version upgrades.
		1 Service

	• LED display preventive and corrective maintenance • Escalation path to manufacturer's support and engineering teams for both SecOps and LED display systems. • Quarterly business reviews and platform optimization recommendations. • On-site support availability within 4 hours for critical issues affecting SecOps or LED display operations.	
1.6	**Training and Knowledge Transfer**	**1 Service**
1.6.1	<u>On-the-Job Training and Knowledge Transfer</u> • Duration: 2 days of structured on-the-job training at Client premises, scheduled during or immediately following system commissioning. • Training Modules: • Platform Administration: System configuration, tenant management, user and role administration, policy deployment, health monitoring. • Threat Investigation & Hunting: Search syntax, query building, attack chain analysis, retroactive hunting, IoC investigation. • Incident Response & SOAR: Playbook execution, alert triage, automated response actions, case management, escalation procedures. • Compliance & Reporting: Dashboard customization, report generation, compliance framework mapping, audit log review. • System Maintenance: Patch management, backup verification, log archival review, performance monitoring. • LED Display Operation: Content switching, source management, scene presets, brightness control, daily operation procedures. • LED Display Maintenance: Front maintenance techniques, module replacement, controller status monitoring, fault identification.	1 Nos

1.6.2	<u>OEM Certified Instructor-Led Classroom Training</u>
	• Training Type: OEM Certified instructor-led classroom training delivered at an authorized training center.
	• Number of Participants: 02 (two) Client personnel.
	• Course: Security Operations (SecOps) - In-depth training on unified platform administration, SIEM operations, XDR management, SOAR playbook development, threat hunting, and incident response.
	• Course Materials: Official OEM courseware, lab manuals, and certification exam vouchers.
	• Lab Environment: Hands-on access to OEM-provided training labs.
	• Travel and Logistics (All-Inclusive for 2 Participants)
	  ○ Return Airfare: Return airfare from Malé to the designated training destination (nearest authorized training center).
	  ○ Full Board Lodging: Hotel accommodation with meals for the full duration of training.
	  ○ Transportation: Airport transfers, daily transportation between hotel and training facility.
		1 Nos

1.7	**Sign-Off Documentation and As-Built Documentation** • As-built architecture diagrams and network topology for SecOps platform. • Detailed configuration baselines and policy documentation. • Operational runbooks and standard operating procedures (SOPs) for SecOps and LED display operations. • LED display system wiring diagrams, signal path documentation, mounting structure details, and power distribution layout. • User manuals and quick reference guides for both SecOps platform and LED display system.	**1 Service**

SECTION C
PRE-QUALIFICATION

Parties interested in delivering the scope of work outlined in Annex I must meet the Section C Pre-Qualification requirement below:

a) **Experience**.
Proof of supply of similar items to other organizations within the last 5 years. (Bidders should submit purchase orders or letters from organizations mentioning successful delivery and implementation.)

b) **Mandatory Documents:**
- Company Registration Certificate
- GST Registration Certificate
- Tax Clarence Certificate (last 30 days from the date of bid submission)
- Last 2 Year Financial Statements
- All the other relevant documents required/mentioned to submit in this bid document.

c) **Manufacture Authorization / Accreditation:**
A firm that does not manufacture or produce the goods it offers to supply shall submit the Manufacturer's Authorization Letter to demonstrate that it has been duly authorized by the manufacturer or producer of the goods to supply and install the goods and service in the Republic of Maldives.

d) **Delivery and Installation:**
Delivery and installation should be completed within 45 days of receiving the purchase order.

e) **Resources:**
The vendor MUST have the following full-time OEM Certified Professional/Engineer to provide all professional services. All relevant engineer(s) certificates and supporting documents shall be included with the proposal. Required certificates of the engineer(s):

Implementation and Technical Support Engineer Certificate:
- IT Project Management or IT Service Management
- OEM Certifications for the proposed SecOps Platform

Migration and Integration Engineer Certificate:
- Fortinet Certified Fundamentals in Cybersecurity
- Fortinet Certified Associate in Cybersecurity
- Fortinet Certified Professional Network Security
- HPE Accredited Technical Professional Storage Solution
- Cisco Certified Specialist – Enterprise Core
- Cisco Certified Specialist – Security Core
- Cisco Certified Network Professional Enterprise (CCNP – Enterprise)
- Cisco Certified Network Professional Security (CCNP – Security)

11th Floor, Velaanage, Male', 20096, Republic of Maldives
Head Office Tel: +960 3323668 Hotline: 1500
www.trade.gov.mv
ވެލާނާގެ 11 ވަނަ ފަންގިފިލާ، މާލެ، 20096، ދިވެހިރާއްޖެ
ހެޑް އޮފީސް ފޯން: +960 3323668 ހޮޓްލައިން : 1500

It is mandatory that the supplier attaches a professional certificate of engineering and other related reference documents. The supplier shall submit the following documents:

a) Certification copies of the relevant training.
b) ID card OR passport copy of the engineer.

The bidder must read, understand, and comply with all areas of this RFQ. Any other information passed during the information session or any information passed via email shall be considered as a requirement of this RFQ.

-- END --