Establishment and Operation of Sectoral IT and OT CERT

Ministry of Health

1. Purpose of this Document:

This document provides a detailed and elaborate version of the Sectoral IT and OT CERT RFP, designed to minimize misinterpretation and provide full clarity for Bidders. This document includes expanded context, detailed scope definitions that comply with NCSC published regulations.

2. Introduction and Context

The Health CERT is launching a strategic initiative to build cyber resilience across all regulated entities within its domain. A cornerstone of this initiative is the establishment of a dedicated Sectoral CERT designed to provide cybersecurity incident collection received from entities, incident aggregation, and sector-specific threat analysis.

The Sectoral CERT will integrate with National CERT operated by the Jordanian National Cybersecurity Center (NCSC) and will serve as a critical layer in Jordan's national cyber defense ecosystem.

The Sectoral CERT (Computer Emergency Response Team) is a specialized cybersecurity unit established at the sector level to monitor incidents received from entities, analyze, and coordinate responses to cyber incidents affecting the sector's digital and operational infrastructure. In addition to coordinating with entity SOCs and the National CERT, the Sectoral CERT is responsible for building and operating its own infrastructure—including threat detection systems to secure the infrastructure, secure communication channels, and incident management platforms to effectively deliver CERT services such as threat intelligence, incident response support, and sector-wide risk mitigation across interdependent critical infrastructure systems.

2.1 Health CERT Objectives

- Provide centralized cybersecurity incidents collection from all entities within the sector.
- Enable cross-entity incident correlation and early detection of coordinated adversary attacks.
- Serve as a trusted incident aggregation and escalation point between regulated entities and the National CERT.
- Offer sector-specific threat intelligence analysis to enhance response readiness.
- Support incident classification, prioritization, and reporting based on national guidelines.
- Ensure secure and standardized integration mechanisms for entity on premises SOCs (or MSSPs).
- Conduct External Sectorial Risk Assessment for the entities within the Sector
- Integrate with NCSC Threat Intelligence program and re-use it for all Sector entities.
- Conduct regular External Vulnerability Assessment for Entities published Service and integrate Vulnerability Management with Incident Management program

3. Scope Of work (SoW):

3.1 General Requirements

- The CERT Should cover incidents both IT and OT environments specific to health sector.
- OT systems include but are not limited Medical Devices.
- Each regulated entity will transmit only security incidents (P1, P2, P3), not raw logs or telemetry data and it will be integrated with CERT incident management Solution.
- The CERT must support the onboarding of approximately ١٠ entities.
- The bidder should build an incident template that is in alignment with the sectoral and national guidelines and regulations published by the NCSC for the format of communicating entity incidents with the Sectoral CERT and National CERT.

- The bidder must provide a solution that maintains high availability (HA) for the infrastructure but not necessarily for the SIEM Storage that can follow sectoral requirements on incident storage and archiving for one year.
- Must incorporate industry standards including IEC 62443 for OT and ISO 27001 for IT.
- All solutions must ensure data confidentiality, segregation, and role-based access control. This is important to ensure process safety and operational integrity within the regulated sector entities.
- The solution must allow for future scalability, including integration of new entities and new data sources.

- All Bidders may schedule site visits to assess:

    - Infrastructure of selected sample entities
    - Expected data flow and use cases
    - Integration requirements and technical limitations
    - CERT room site preparation requirements
    - This activity is crucial for accurate technical sizing and costing.

3.2 Technology Stack

This RFP encompasses the comprehensive design, implementation, and initial operation of the Health Sector CERT, including:

- Main Technology Components:
    - Security Information and Event Management (SIEM) system (will be only used for Ministry of Health Public Locations such as (Hospitals, Directorates, etc.)
    - Integrated ticketing system for incident management (will be use collect incident from all CERT entities/members)
    - External vulnerability scanning capabilities
    - Threat intelligence platform (will be use to integrate with NCSC Threat feeds)
- Infrastructure Requirements:
    - Enterprise-grade storage solutions
    - High-availability server architecture
    - Network infrastructure (switches, routers)
    - Next-generation firewall systems
- Facility Requirements:
    - Preparation of Dedicated secure physical space for CERT operations
    - Access control and physical security measures

3.3 Supply, Installation, and Commissioning

- The expected model to work is:
    - Initial implementation of the Security technology and infrastructure.
    - Operational support during the transition phase.
    - Engineering services for ongoing maintenance.

- Licenses of all Software should start only after the system is properly received by the receiving committee, minimum 4 months will be accepted but Bidder should align this with Project Plan,
- Bidder should do transition during the project timeline from Sectoral CERT team as 20% of the CERT team and they should include 80% from the Bidder's team. At the end of the project Bidder should ensure transition of the operation of the CERT by 80% of the CERT Team with 20% support of the Bidder's team.

- **During the Detailed design and architecture of the proposed solution bidder should include following:**
    - Design a dedicated CERT infrastructure owned by the Health CERT
    - Deliver full infrastructure including:
        - SIEM (Security Information and Event Management) : Refer to point 5.1 for Needed Features
        - Incident Collaboration Case Management and Reporting Refer to point 5.2 for Needed Features
        - External Application Assessment Refer to point 5.3 for Needed Features
        - Sectorial Risk Assessment Refer to point 5.4 for Needed Features
        - MISP for threat intelligence integration with NCSC Please Refer to 5.5 for scope
        - Bidder should deliver a secure infrastructure (Firewalls with IPS, AV, VPN, and supports MFA) and establish a secure interface with the Entities and National CERT for incident escalation from entities to Sectoral CERT and from Sectoral CERT to National CERT. Please refer to Section 7.1, 7.2, 7.3 for requirements.

- All required items, Hardware/ equipment for implementing the solution will be the responsibility of the bidder which includes providing delivery, installation and commissioning.

- **During Operate Phase: the bidder should follow:**

  - Operate the CERT for 3 Years under defined SLAs.
  - Maintain a full operational staff including:
    - Tier 1& 2 Incidents Analysts
    - L3 CERT and Team Leads
    - Threat Intel Analysts
  - Perform ongoing threat analysis, entity coordination, and response support.
  - Deliver scheduled reporting: daily alerts, weekly incident summaries, monthly risk reports.
  - Facilitate regular sectoral cybersecurity drills.
  - All requirement Refer to 6.1 , 6.2, 6.3 for Scope of operate
  - Bidder will upgrade software regularly for Free and any on demand requirement by regular body by bidder's expenditure.
  - All product/items supplied should be covered under 3 years' local support and maintenance

- **During Delivery Phase bidder should do following:**

  - Execute full transfer of operations, licenses, configurations, and knowledge to the Sectoral Authority.
  - Provide capability-building and formal training for the in-house team.
  - Ensure transfer does not disrupt CERT operations or degrade SLAs.

4. Bidder Qualification:

- General Requirements:
  - The bidder must have a valid partnership certificate for the provided solutions, and the partnership certificate must be attached to the technical offer.
  - Enterprise and commercial license must be provided valid for 3 years from the Acceptance of the system through the Receipt Committee.
  - The bidder must have at least three certified engineers on the proposed solutions, C. V's must be attached to the offer.

- At least 2 references must be provided with similar size, CERT has the right to contact the references to check.
- Bidder has to mention Hardware and associated equipment's along with any intermediate Hardware and/or equipment's to implement the solution successfully.

- Experience Requirements:
  - Minimum 5 years' experience in CERT/SOC establishment and operations
  - At least 2 completed CERT implementations for government or critical infrastructure
  - Demonstrated experience with Health sector or similar critical infrastructure
  - Experience with both IT and OT security environments
  - Minimum 3 managed security services implementations
- Technology Partnership Requirements:
  - Valid partnership certificates for ALL proposed technology solutions
  - Authorized reseller/partner status with technology vendors
  - Access to vendor technical support and escalation
  - Training certification from technology vendors
- Technical Team Qualifications:
  - CERT building consultant with Minimum 10 years' cybersecurity experience, CISSP certified
  - L3 Security Analysts: Minimum 5 years each, incident response certified
  - SIEM Specialist: Minimum 5 years SIEM experience, vendor certified
  - Network Security Engineer: Minimum 5 years' experience, with highest certificate in product proposed.
  - OT Security Specialist: Minimum 2 years OT/ICS experience
  - Minimum team size: 5 dedicated professionals

5. Lot 1: Security Center Technology

5.1 Security information and Event Management Solution

The solution must provide the following (The values are baseline; bidders must visit the site, adjust them as needed according to the bidder's proposed solution, and include the calculations in the technical proposal. These values are binding on the contractor, provided that they are not less than the baseline values):

- SIEM Sizing:
    - Event Per Second:.12000 EPS
    - Log/day: 150 GB/Day
    - Number of Managed Devices: up to 900
- SIEM platform should not be based on Open Source
- The SIEM should support the following:
    - Getting Logs through log collector from IT Devices in MoH Networks
    - The system should have no limitation on the number of Log collectors installed.
- The solution Should be expandable from License perspective
- Event correlation and alert management using SIEM systems.
- The solution must be hosted in Jordan Digital Center in Al-salt (or in any Location the MoH will determined), all relevant work must be onsite.
- The platform must be able to be deployed using Virtual Machine approach.
- The Solution Should Support Multi-tenant by nature
- The solution must allow management centralization of multiple deployments
- Supports Log collection and analysis from:
    - Endpoints
    - Network devices
    - Security solutions (firewalls, IPS/IDS, etc.)
    - Public and private cloud services.
- The Solution should support Multiple Integration Mechanisms:
    - Ability to ingest logs from diverse sources (firewalls, IDS/IPS, endpoint security, Servers, Application.)
    - **Ability to conduct API integration with resources over Cloud, Office 365, and other components**
    - Support for standard log formats (syslog, SNMP, CEF, etc.)
    - Support Collection of Performance metrics via polling (Interface utilization, errors, sent and received bytes, CPU, Memory, Process utilization)
- Retain logs for a minimum of 1 year with 3 months as default and quick search ability.
- The solution should have multiple Detection Capabilities
    - Out-of-box detection for MITRE ATT&CK techniques (minimum 90% coverage)
    - Custom detection rule creation with version control and collaborative editing
    - False positive suppression mechanisms with tuning feedback metrics
    - Threat correlation with resolution across other Members
    - User behavior analytics
- The Solution Should Support for STIX/TAXII capabilities and providers should provide well-known Threat Feeds as part of the SIEM implementation
- In case Log Agent used, the following points should be collected:
    - Centrally managed agents via the SIEM. No separate Management or management console.
    - Able to collect logs from text files on Windows devices
    - Able to collect event logs other than Security, System and Application
    - Perform File Integrity Monitoring
    - Perform Registry Monitoring
    - Monitor for removable devices
    - Execute PowerShell commands and send output back as logs

    - The Windows agent must send event data back to the SIEM components encrypted using HTTPS
    - Detect File Permission and Ownership changes.
- The solution must be deployed in distributed architecture for storage, log ingestion, and visualization.
- The SIEM should have capability to Automate by executes remediation script that can also be executed automatically
- The SIEM solution must provide the option to create and store more than one replica, further enhancing data protection. Providers should elaborate on their replication capabilities and procedures.
- The solution should have ability to monitor performance measures (CPU, RAM, Disk Space, Interfaces Status)
- The solution should have context-aware GenAI assistant that simplifies and automates critical analyst activities such as :
    - Threat investigation/response intel & actions
    - Best practice recommendations and guidance
    - SIEM query/report creation
- Solution must provide event correlation and machine learning to detect advanced and behavioral-based attacks, detailing their analytic capabilities and the strategies employed.
- The solution must be able to define behavioral detections with event sequences.
- The solution must offer different data storage tiers. Most recent data should be queried faster compared to older and less frequently accessed data. The provider is required to provide details on their different data tiers and how data is moved across tiers.
- The solution Architecture should support data distribution into multiple nodes to allow parallel reading data from these nodes.
- The solution must have embedded workflow to track the incidents and to support collaboration.
- The solution must provide Alert suppression to reduce the number of repeated or duplicate detection alerts.
- The solution must provide an orchestration platform to manage multiple SIEM deployment and versions.
- The solution must be able to perform anomaly detection rules by Machine Learning.
- The solution should have the capability to operate AI and machine learning on the same platform, without any additional product licensing.
- The proposed solution must be deployed considering high availability, the bidder must describe how this is achieved in his proposal.
- The solution must support cascaded event forwarding to forward logs using multiple agents/collectors to reach the destination.
- Provide support operations, that will help CERT to manage SIEM, the follow is expected to be included in this service:
    - Rules management and updates
    - Parse new log sources into the SIEM
    - Deployment of the SIEM solution optimally set up for CERT specific needs.
    - Expert-driven initial configuration, and re-configuration of CERT system as needed, adapting to changing demands.

- Implementing system enhancements and updates to keep CERT operations at the cutting edge of technology.
- Executing upgrades, ensuring CERT system remains up-to-date with the latest advancements.
- Bug fixes, addressing any issues promptly and thoroughly.
- Detailed problem and performance analysis, identifying potential obstacles and opportunities for optimization.
- Assist in third party integrations.

- 3-Year management of the above services starting from the license activation date.
- Winner bidder should provide full documentation for the project, the below is the minimum accepted documents for the project:
  - low level design
  - Implementation manuals
  - backup / restore procedure
  - Full documentation

5.2 Incident Collaboration / Ticketing system:

- The Solution should support Core Incident Management
  - Customizable security incident workflows with conditional routing based on type, severity, and CERT member
  - Automated ticket creation from SIEM alerts detections
  - Standardized incident categorization aligned with predefined security taxonomy
  - Flexible prioritization framework allowing both automated and manual scoring
  - SLA tracking with escalation paths customized to incident characteristics
  - Comprehensive audit trail of all incident activities with timestamp preservation
  - The license should cover 10 CERT members.

- The Solution should support Multi-Member Support
  - Multi-tenant architecture with configurable information sharing between CERT members
  - Role-based access control matching CERT team structure
  - Custom dashboards for CERT members and CERT
  - Customizable notification rules for different stakeholder groups
  - Ability to support Evidence upload capabilities

- The Solution should support Incident Collaboration Features
  - Real-time chat and collaboration within incident tickets
  - Shift handover functionality with summary generation
  - The solution should allow incident management to collaborate with problem management to identify underlying causes of recurring incidents and implement preventive measures.
  - The solution should allow service desk agents to communicate with end users through different channels: Chat, mail, etc
  - Digital evidence management with hash verification

- Ability to push notifications directly in the browser, e.g. information when an Incident has been updated. These notifications also can be used in custom workflows

- The Solution should have capabilities of intelligent Cyber Security
    - The solution should allow CERT to Define and track key performance indicators (KPIs) to measure the effectiveness of incident management processes and identify areas for enhancement.
    - Threat intelligence integration with automatic correlation to similar incidents
    - MITRE ATT&CK mapping for tactics and techniques identification
    - Secure evidence storage with chain of custody tracking
    - Indicator of Compromise (IOC) extraction and management
    - Two-factor authentication and granular access controls
    - Integration with proposed SIEM's or CERT technologies

- The Solution should have capabilities of Reporting & Analytics
    - Customizable dashboards for operational, tactical, and strategic levels
    - Trend analysis across incident types, members, and time periods
    - Performance metrics against defined SLAs and response objectives
    - Automated report generation for executive briefings
    - Historical analytics for identifying recurring issues

5.3 External Application Vulnerability Scanner:

- The solution should cover 20 web applications as a baseline with ability to change (add/remove) applications without affect the licenses
- The solution should automate front-end or black box testing of web apps against OWASP Top 10 and SANS Top 25 vulnerabilities
- The solution should have Advanced Crawling capabilities to identify and scan all branches and paths in web applications including JavaScript-heavy web applications with ability to perform authenticated crawling
- The solution should have Advanced authentication handling including multi-factor and SSO systems
- The solution should support Schedule Tests at Desired Interval
- The solution should support detailed Results with Suggested Remediation. And each vulnerability found can be drilled down to get detailed information on the issue along with suggested remediation steps
- The solution should have the capability of URL Fuzzy
- The solution should have integration with CI/CD and WAF technologies.
- Web Application Scanner should have RBAC user access management

5.4 Sectorial Risk Assessment and Rating:

- The Solution should provide a comprehensive suite of tools for measuring and benchmarking security performance, mitigating third-party and fourth-party risks, and visualizing and remediating risk throughout an organization's digital footprint

- The Solution should identify critical areas of risk throughout a digital ecosystem for the sector and regulated entities under it
- The subscription must compromise an unlimited number of users, and the MOH has the right to delegate access to the platform to those licenses, in which each has access only to their own data/analysis/dashboard
- The Solution should cover 10 licenses for entities with ability expand
- The Solution must be able to provide the security rating of the entire sector and to compare the rating of the industry across the countries (at least 3 countries).
- The Solution must be able to show a list of infections, exposed services, list of vulnerabilities, and list of peer-to-peer activity
- The Solution must be able to report which CERT members from the Critical National Infrastructure have security issues related with their current configuration such as mobile applications, SSL certificate, etc.
- The Solution must keep 12 months of historical data for each CERT member that belongs to the Critical National Infrastructure.
- Solution must have pre-built connectors for Common Event Format (CEF) and LEEF (Log Event Extended Format) or other formats to be able to integrate the real-time API with Proposed SIEM.
- Solution should be able to provide the monitored IPs and Domains of Critical National ulnfrastructure for duly authorized National Entities
- The solution should be able to show indicators of compromise, infected machines, improper configuration and poor security hygiene by constituent
- The solution should be able to maintain a historical rating of all companies that are being tracked in a portfolio
- The security rating should be based on data that is externally accessible only
- The solution should be able to include an asset risk matrix to categorize risks by severity and by the importance of an asset.
- The solution should be able to CERT members security ratings against each other
- The platform comparison feature should display a security rating of multiple companies at once.

5.5 Threat Intelligence platform (MISP)

- MISP must be integrated with NCSC threat intelligence feeds.
- MISP should be configured to deliver comprehensive, timely, and actionable intelligence covering diverse threat indicators
- Intelligence should include malicious IPs, domains, URLs, file hashes, and emerging threat actor TTPs
- Threat intelligence must be regularly updated with defined refresh intervals
- Open-Source Threat feed should be added to CERT Feeds.
- MISP should be integrated with the SIEM proposed through STIX/TAXII standards or out of box integration only.
- Threat feeds must support integration with the SIEM proposed through STIX/TAXII standards or out of box integration only.
- MISP should be configured to allow for bidirectional sharing with Threat Intelligence

Platforms (TIPs) used by CERT members and NCSC

5.6 Establishing CERT processes and Procedures:

- Establish CERT management framework That includes following frameworks:
  - Establish a Threat management framework.
  - Establish a Vulnerability management framework.
  - Establish an Incident management framework.
- Develop the Security Monitoring process:
  - 24x7 real-time monitoring
  - Alert triage and correlation
  - Cross-system event analysis
  - SOC use case Management
  - False positive tuning
- Develop the SOC Incident Management process:
  - Incident Management Process
  - Full Incident Response Plan (IRP)
  - SOC Run Book process for Major Incident types
  - Incident Handover Process
- Develop the CERT Administration process:
  - Notifications and Escalation Process
  - Reporting and Documentation Process
  - Incident Closing and lessons learned process
  - Change Management Process
  - Human Power Assessment
  - Log Backup/Restore Procedure
  - Devices On-Boarding Process
  - Device Off-Boarding Process
- Vulnerabilities and Threat Management processes
  - Unauthorized Access detection Processes
  - Denial of Service Detection Processes
  - Malicious code detection Processes
  - Unlawful Activity Detection Processes
  - SOC Infra Assets Management Process
  - CERT's / IOCs Incident Handling Process
  - Vulnerability/Threat Advisory process
  - Threat Intelligence collection and IoC Management
- CERT SOC KPI's:
  - Develop CERT KPI's and get CERT member approval
  - Build KPI's based on CMM levels and define Required Data Sources for calculation
  - Define How Sector Cyber Security Maturity will be defined based on KPI's collected

6. Lot 2: Security Support Services and Training

6.1 Security Support Team Requirements:

- Level 1 (L1): To be primarily staffed by MOH personnel (after initial training period)
- Level 2 (L2) Support:

- Minimum of 3 dedicated L2 analysts with 3+ years of SOC experience
- Available on-call 24/7/365 with maximum 30-minute response time for critical incidents
- Expertise in advanced threat hunting, incident analysis, and complex alert triage
- Capability to handle sophisticated malware analysis and network forensics
- Experience with healthcare-specific systems and compliance requirements
- Certifications required: Certified Incident Response

- Level 3 (L3) Support:

  - Minimum of 2 dedicated L3 security experts with 5+ years of specialized experience
  - Deep expertise in advanced persistent threats (APTs) targeting healthcare
  - Capability to perform in-depth forensic analysis and threat intelligence
  - Experience in incident response for critical healthcare infrastructure
  - Certifications required: Certified Incident Response

6.2 On-Site Support Requirements:

- L2/L3 specialists must be able to deploy on-site within required SLA for critical incidents
- Quarterly on-site presence for proactive threat hunting and system hardening
- Physical presence required during major security events or infrastructure changes
- Ability to coordinate with MOH CERT when necessary

6.3 Training Requirements:

- SIEM Threat Hunting Training specifics:

  - L2 and L3 level training for 8 team members
  - Comprehensive Training covering advanced SIEM configuration, custom rule creation, threat hunting methodologies, and healthcare-specific threat patterns
  - Structured training program delivered in different Training (divided into initial, advanced, and specialized healthcare-focused phases)
  - Hands-on labs with simulated healthcare attack scenarios
  - Assessment components to measure effectiveness

- Training Materials and Resources:

  - Comprehensive documentation requirements
  - Recorded sessions for future reference
  - Healthcare-specific threat hunting resources

7. Lot 3 (Core Infrastructure)

7.1 General requirements:

- The Core Infrastructure consists of the following:

- Next Generation Firewall that will be used to secure CERT infrastructure and Site to Site VPN with CERT members for Log collection
- Core Switches for main Connectivity for the infrastructure
- Switches that will be used for CERT connectivity.
- Storages to support Log retention with multiple Tier storage
- Servers that are used as computing nodes in a clustered configuration
- Computers and Laptops that will be used for employees and CERT Analyst

- For hardware devices, the devices must be new and manufactured during 2024 at least
- All devices included in this tender are supplied in sealed boxes from the manufacturer.
- The bidder is committed to guarantee the devices for a period of (36) months from the date of final acceptance of the bid materials.
- Any Hardware and network component, network switches, license and cables to be added to connect the proposed solution is bidder responsibility.
- The supplier is obligated to provide compliance matrix with links to the specifications.
- The device warranty (spare parts and on-site maintenance) is at least 3 years, including software updates or spare parts starting from the final acceptance date.
- All Hardware Must be from the same vendor
- All needed cables and SFP must be included in the setup to have the cluster working.
- Any Hardware, network component, network switches, license and cables to be added to connect the proposed solution is bidder responsibility.
- The proposed hardware must have at least the following specs **(estimated and subject to tuning based on bidder site visits):**

7.2 Next Generation Firewall (QTY 2)

- FW Throughput (PPS): Minimum 200 Mpps.
- Threat Protection Throughput: 15Gbps
- Dual Hot-Swappable AC input
- Ports: 4 * 10 GE ports, 4 * 1GE SFP+ port
- IPsec VPN Throughput: 30 Gbps
- License required: IPS, URL Filtering, Application Control

7.3 Core Switches (Qty 2)

- Supports a minimum of 1.5 Tbps. switching capacity
- Supports a minimum of 8 GB RAM (DDR4)
- Supports a minimum of 4 * 100GE QSFP+ uplink ports and 48 x 1/10 SPF/ SFP+.

7.4 Access Switches (Qty 2)

- Supports a minimum of 128 Gbps. switching capacity
- Supports a minimum of 4 * 10GE SFP+ uplink ports and 24 x 1 GE ports.

7.5 Servers and Storage

- MOH are looking for a Servers solution with the following specs:
- Total number of nodes = 5
- Each node must have the below specs:
    - 2 x Intel Xeon-Gold processor 2.9 GHz/ 20-core
    - RAM: 6 x 64GB Memory Module (5600MHz DDR5 RDM)
    - NVMe: 10 x 7.68 TB NVMe
    - 2 x 10GE SFP+ ports per node for management
    - 4 x 25/10GbE ports.

- Redundancy and resiliency levels:
    - N+1 for CPU and RAM
    - N+1 for storage
    - Provide at least 100 TB of usable storage with N+1 considerations.
    - 500GB of usable RAM with N+1 considerations.
- Each HCI node must support a minimum of:
    - 10GE SFP+ network ports
    - 1/10GBaseT Copper ports
    - 1Gbe Ethernet port for management
- The bidder must have partnership with the technology provided.
- At least 3 years 24x7 support for hardware and software, with NBD hardware replacement
- The support contract must include free-of charge replacement of the SSDs that reach the write data limit.
- The bidder must provide the following details:
    - At least three certified engineers on the proposed technology
    - At least 5 comparable references in country (please provide details)
    - At least 3 Official Training Seats on proposed technology.

7.6 ToR Switches (Qty : 2)

- ToR Switches must be from the same Manufacturer as computing cluster nodes, storage nodes.
- ToR to aggregate Compute Nodes Network Uplinks, and Communication between computing cluster nodes and storage controllers and Object storage nodes.
- At least two ToR Switches, with two 40/100G Stacking links.
- Each switch must have at least 48 x 25G and 6 x 40/100 uplinks.
- Min 1 x 40G QSFP+ LC must be provided per switch for uplinks connectivity
- All needed transceivers to connect with all compute nodes and storage must be provided (DAC can be accepted for the connectivity of compute nodes).
- All Ports must be activated and fully licensed from Day one.
- Must support hot swappable power supply units and fans.

7.7 Rack Cabinet 42U (800mmx1200mm)

- High Servers Rack, must be same brand as server and storages:
- PDUs: Redundant PDUs 7.3kVA (Vertical) with at least 20 outlets per PDU.
- KVM: 16 Ports with 16 cable and all accessories.
- Console: 18.5" LCD Console with keyboard and pointing device.
- Support: 3 years support.

7.8 SOC Analyst Workstations (8 Units Required)

Workstation Minimum Requirement Specifications

- **Processor:** Intel Core i7-13700 (8-core, 3.4GHz base)
- **Memory:** 32GB DDR4 expandable to 64GB
- **Storage:** 1TB SSD
- **Graphics:** Dedicated GPU with dual DisplayPort/HDMI outputs
- NVIDIA RTX 4060 or AMD RX 7600 (minimum 8GB VRAM)
- **Motherboard:** Business-grade with multiple PCIe slots and USB ports

Connectivity Requirements:

- **Video Outputs:** Minimum 2x DisplayPort 1.4 or HDMI 2.1 ports
- **Network:** Gigabit Ethernet (RJ45) + Wi-Fi 6E capability
- **USB Ports:** Minimum 6 USB ports (2x USB 3, 4x USB 2.0)
- **Audio:** Integrated audio with line-in/line-out and microphone support

Monitor Specifications (16 Units Total - 2 per Workstation)

- **Size: 24–27-inch professional grade LCD/LED**
- **Resolution: Minimum 2560x1440 (QHD) or 1920x1080 (FHD)**
- **Panel Type: IPS or VA for wide viewing angles**
- **Refresh Rate: 75Hz minimum (120Hz preferred)**
- **Response Time: ≤5ms**

Connectivity:

- **DisplayPort 1.4 and HDMI 2.1 inputs**
- **USB hub with 2-4 USB 3.0 ports**
- **Internal Speakers**

Accessories per Workstation

Input Devices:

- **Mouse and Keyboard**
- **Professional headset with noise cancellation and microphone**

Monitor Mounts:

- **Dual monitor desk mount or monitor arms**
- **Cable management system**
- **Adjustable height desk (sit/stand capability preferred)**

7.9 Wall-Mount Screen 65" Qty. 4

- **4K QLED Screen**

- **All Needed accessory to Connect one Workstation Computer (must be Provided same as 7.8 section specification) to all 4 Screens**

8. Lot 4: Room Facility [Site Preparation] :

MINISTRY of Health will Prepare a room to be Acting as CERT Room, however, the winning Bidder should prepare the room as following.

8.1 Room Renovation

The renovation of the CERT room, which includes several essential upgrades to ensure it meets operational and security standards. The renovation should include closing all windows to ensure privacy and security, painting the walls for a clean, professional look, additionally, a Wall Mount Screen will need to be installed for enhanced monitoring. Any other necessary modifications or equipment required for the proper functioning of the SOC should be included in the renovation plan. This will ensure that the room is fully optimized for its intended use.

8.2 Cameras

Qty.: 4 IP indoor 5MP to be connected to the existing MOH CCTV

Supply and installation of cameras (in/out) the SOC Room and Integration with existing monitoring systems. Calibration and configuration to ensure optimal performance in diverse environments.

8.3 Lighting Units

Qty. : 4

Installation of energy-efficient lighting systems in the SOC room. The lighting should be advanced ceiling lighting units. Energy-efficient and compatible with the operational environment.

8.4 Access Control System

Qty: 1

- **Finger print , Ethernet port , audio /visual indication of acceptance or rejected push button use for exit ,**
- **Face recognition**
- **Magnetic lock**

Supply and installation of a door access control unit with face recognition features. Integration with the facility's existing security infrastructure. Configuration for real-time monitoring and access logging.

Project Management and Timeline

8.5 Project Management

- The solution provider must document the Project management methodology within the proposal.
- The solution provider must have document risk and issue management processes within the proposal
- Solution provider should provide dedicated Project manager who has qualifications and experience
- During the project solution the provider should provide status reports as follows:
    - Status reporting
    - requirements Documentation
    - Progress tracking metrics
    - Executive-level reporting

8.6 Post-Implementation Support

- Solution Providers should detail their approach to transitioning from project to operational status, including a stabilization period with enhanced support levels.
- Solution Providers should specify the duration and level of post-go-live support, including on-site presence, dedicated resources for issue resolution, and executive sponsorship.
- Solution Providers should provide knowledge transfer methodologies to ensure CERT team can effectively operate all implemented systems and follow established processes.
- Solution Providers should outline their commitment to periodic health checks, technology roadmap reviews.

9. EVALUATION CRITERIA

9.1 Evaluation Methodology

- Technical Evaluation (70%) - Minimum passing score: 80%
- Financial Evaluation (30%) - Only for technically qualified bidders
- Evaluation Committee:
    - Technical evaluation by specialized technical committee
    - Financial evaluation by procurement committee
    - Final ranking by combined technical and financial scores

9.2 Detailed Technical Evaluation Criteria

Evaluation Criteria	Weight	Maximum Score	Sub-Criteria and Scoring
Security Center Technology Solution	35%	35 points	o SIEM solution design and capabilities (20 pts) o Ticketing system solution (10pts) o Integration and scalability (5pts)
Core Infrastructure	12%	12 points	o All core infrastructure component.
Technology Partnerships and Licensing	10%	10 points	o Vendor partnerships and certifications (5 pts) o License compliance and flexibility (5pts)
Scope of Work (SoW)	10%	10 points	o SoW delivery approach (10 pts)
Build and Operate Team Expertise and Staffing	8%	8 points	o L1/L2/L3 team qualifications and certification(5 pts) o OT/IT security expertise (3 pts)
CERT Processes and Procedures	10%	10 points	o Incident management frameworks (4 pts) o SOC operational procedures (3 pts) o KPI and reporting frameworks (3 pts)
Implementation Methodology	5%	5 points	o Project management approach (5 pts)
Reference Projects and Experience	5%	5points	o CERT/SOC implementation experience (5 pts
Site Preparation	5%	5 points	o **Site Preparation**
TOTAL	**100%**	**100 points**	**Minimum passing score: 80 points**

سيتم تقييم العروض الفنية وفقا للمعادلة التالية:

$$\text{الوزن الفني للمناقص} = \frac{\text{التقييم الفني للمناقص}}{\text{اعلى تقييم تم الحصول عليه}} * ٧٠$$

9.3 Financial Evaluation Criteria

Financial Scoring Formula:

$$\text{الوزن المالي للمناقص} = \frac{\text{اقل سعر تم الحصول عليه}}{\text{التقيم المالي للمناقص}} * ٣٠$$

9.4 Combined Final Score:

الوزن الاجمالي لكل عرض = الوزن الفني + الوزن المالي

سيتم الاحالة على المناقص صاحب العرض الذي حاز على الترتيب الاعلى وفقا للمعادلة الوزنية الاجمالية اعلاه.

- **علما بأن علامة النجاح للعرض المالي والفني هي ٥٦%**

Jordan's Cybersecurity CERTs & SOCs Architecture

National CERT

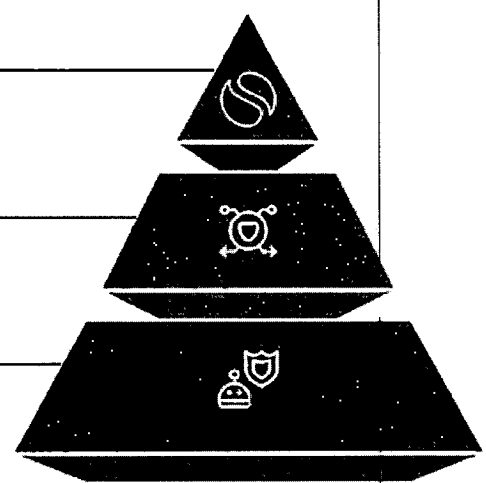
Centralized visibility and response coordination

Sectorial CERT

Coordinated defense within specific sectors

Entity SOC

Decentralized operations for local threats



Entity > Sectorial CERT > National CERT
Incident Management Flowchart