Computer Emergency Response Team (CERT)

For Industrial Sector

Contents

1. Purpose of this Document

This document provides a detailed version of the Industrial Sectoral IT and OT CERT (Computer Emergency Response Team) RFP, designed to minimize misinterpretation and provide full clarity for Bidders. This document includes expanded context, detailed scope definitions, and clarification of expectations across delivery model for Industrial Sectoral lead to request for CERT Services and comply with NCSC published regulations**.**

2. Introduction

The Ministry of Industry and Trade (MIT) 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 Industrial CERT designed to provide cybersecurity incident collection received from Industrial entities, incident aggregation, and sector-specific threat analysis.

This RFP seeks proposals from qualified Bidders to deliver this CERT using the delivery model of on Premises approach for main components such as Infrastructure, SIEM, Threat Intelligence platform and case management system. The vulnerability scanning and risk rating solutions can be delivered via cloud-based approach.

The Industrial 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 is a specialized cybersecurity unit established at the Industrial sector level to monitor incidents received from Industrial entities, analyze, and coordinate responses to cyber incidents affecting the Industrial sector's digital and operational infrastructure. In addition to coordinating with Industrial entity SOCs and the National CERT, the Sectoral CERT will be responsible for managing 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 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 targeting Industrial infrastructure.
- Serve as a trusted incident aggregation and escalation point between regulated entities and the National CERT.
- Provide sector-specific threat intelligence analysis for the CERT entities to enhance response readiness.

- Support incident classification, prioritization, and reporting based on national guidelines and sector requirements.
- Ensure secure and standardized integration mechanisms for sector entities on-premises SOCs (or MSSPs).
- Conduct External Risk Rating 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 sector Entities published Services and integrate Vulnerability Management with Incident Management program
- Align with Standards and Recommended Practices for Industrial cybersecurity.

3. Scope of Work

3.1 General Requirements

- The CERT should cover incidents in both IT and OT environments specific to sector operations.
- 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 (Identification of the technologies of the CERT entities is subject to site visits)
- The CERT must support the onboarding of 5 entities. The onboarding of the entities will be during the implementation phase for the ready-to-onboard entities and for the remaining entities during the operation period. The readiness for the CERT entities will be evaluated during the site visits.
- The bidder should build an incident template that is in alignment with the sectoral and national guidelines and regulations published by the NCSC (Refer to NCSC Website for published regulations) for the format of communicating Industrial entity incidents with the Sectoral CERT and National CERT.
- The bidder must provide a solution that maintains high availability (HA) for the CERT infrastructure.
- The bidder Must incorporate industry standards including IEC 62443 for OT, 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.

- Bidder should submit the technical and financial proposals covering all components within this RFP.
- All Bidders may schedule site visits to assess:
    - Infrastructure of selected sample entities
    - Expected data flow and use cases
    - Integration requirements and technical limitations
    - Any related IT/OT/IoT infrastructure inquiries
    - 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 Sectoral CERT, including:

- Main Technology Components:
    - Security Information and Event Management (SIEM) system (will be only used for MIT and subordinate entities)
    - Integrated case management system for incident management (will be used to collect incidents from all CERT Industrial entities/members)
    - External vulnerability scanning capabilities for External Applications within Industrial sector
    - Sectoral Risk Rating solution (will be used as external Threat Assessment and Cyber Security rating)
    - Threat intelligence platform (will be used to integrate with NCSC Threat feeds)
- Infrastructure Requirements:
    - Enterprise-grade storage solution suitable for data requirements
    - High-availability server architecture
    - Network infrastructure
    - Next-generation firewall systems
- Resident engineer for operation
    - Dedicated L2 security Analysts for Cyber Security operation and CERT operation

3.3 Implementation Approach

- The expected model to work will be as follows:
    - 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 acceptance committee.

- Bidder should support the CERT during the project timeline. At the end of the project, Bidder should ensure that CERT team can handle the operation of the CERT.
- Project Roadmap:

Milestone	**Time**
Site Visit and Sizing	During tendering
Provide HLD	Awarding (technical and financial evaluation)
Provide LLD	
Provide Resident Resources CVs	
Supply HW and Licenses	Implementation Phase: 6 Months
Deployment	
Testing	
Accept HLD	
Accept LLD	
Accept Resident Resources CVs	
Initial Acceptance	
Start Production Licenses	Operation Phase: 3 Years
Operation of the CERT	
Final Acceptance	End of Project

- **During the implementation phase, the bidder should include following:**
  - Design a dedicated CERT infrastructure. The design should be approved by the sectoral CERT and NCSC.
  - 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. It is not accepted, to provide this solution as an embedded feature within the SIEM solution.
    - External Application Vulnerability Assessment: Refer to point 5.3 for Needed Features
    - Sectoral Risk Rating: Refer to point 5.4 for Needed Features
    - 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 CERT 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 operation phase the bidder should:**
  - Operate the Industrial CERT for 3 Years under defined SLAs
  - Maintain a full operational staff including Layer 2 Incidents Analysts preferable with Industrial sector knowledge
  - Perform ongoing threat analysis, entities coordination, and response support.
  - Deliver scheduled reporting: daily alerts, weekly incident summaries, monthly risk reports
  - Facilitate regular sectoral cybersecurity drills
  - All requirements Refer to 6.1, 6.2, 6.3 for Scope of support
  - Bidder will upgrade software regularly for free and any on-demand requirement by CERT on bidder's expenditure
  - All product/items supplied should be covered under 3 years' local support and maintenance
- **The bidder should assure the following:**
  - Capability-building and training for the in-house team by end of the first year.
  - Full transfer of operations, licenses, configurations, and knowledge to the Industrial Sectoral Authority by the end of the project.
  - Transfer does not disrupt CERT operations or degrade SLAs.

4. Bidder Qualification

- General Requirements:
  - The bidder must have valid partnership certificates for the provided solutions, and the partnership certificate must be attached to the technical offer. These certificates should remain valid or renewed until the end of the project.
  - Enterprise and commercial licenses provided must be 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, CVs must be attached to the offer.
- At least 2 references must be provided with similar size CERTs/SOCs, MIT has the right to contact the references to check.
- Bidder should provide any Hardware and associated equipment along with any intermediate Hardware and/or equipment to implement the solution successfully.

- Experience Requirements:
  - Minimum 5 years' experience in CERT/SOC establishment and operations.
  - Demonstrated cyber security experience with the Industrial sector or other critical infrastructure.
  - Experience with both IT and OT security environments, preferably in Industrial sectors
- 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, Industrial sector knowledge is preferred
  - Security Analyst: Minimum 5 year experience, incident response certified, preferable with OT operational environments or Industrial
  - 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 (preferred): Minimum 5 years' OT/ICS experience, preferably with Industrial operational technology systems.
  - Minimum team size: 4 dedicated professionals Preferred in Industrial sector.

5. CERT Technologies

5.1 Security information and Event Management Solution

The solution must provide the following **(Subject to sizing based on bidder site visits):**

- Accepted vendors:
  - Cisco Splunk
  - Elastic
  - IBM Qradar
  - Fortinet
- SIEM Sizing **(the bidder should calculate the parameters below and provide the suitable sizing in the bidder's offer based on site visits. Scientific proofs should be provided in the offer**):
  - Event Per Second
  - Log/day
  - Number of Managed Devices
- SIEM license should be a commercial license (not open-source).
- The SIEM should support the following:
  - Getting Logs from Devices in MIT.
  - The system should have preferably no limitation on the number of Log collectors installed. The bidder must clearly specify if there are any restrictions or limitations on the number of log collectors supported.
- The solution Should be expandable from License perspective. Bidder must specify how the licensing model supports scalability and future expansion, including any limitations or additional costs associated with increasing capacity.
- Event correlation and alert management using SIEM systems.
- The solution must be hosted in any Location MIT will determine, 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 centralized management of multiple tenants.
- The system license should not block or hard stop data flow even if the daily ingested data rate has exceeded the estimated capacity. Bidders must clearly describe the system's behavior when the licensed data ingestion capacity is exceeded, including:
  - Whether data ingestion continues uninterrupted,
  - The mechanism used to notify or handle license exceedances, and
  - Any additional costs, licensing adjustments, or operational limitations that may apply
- The license must allow unlimited users and agents while the daily ingest rate remains within limits. Bidders must specify whether any limitations apply to the number of users, agents, or endpoints under the provided license, and must disclose any additional costs and licensing constraints with scaling these components.
- The license must support continuous operation and scalability without requiring additional purchases or upgrades for the specified limits.
- Supports Log collection and analysis from but not limited:
  - Endpoints
  - Network devices

    - Security solutions (firewalls, IPS/IDS, etc.)
    - Public and private cloud services.
- The Solution should support Multiple integration Mechanisms:
    - Ability to conduct API integration with resources over Cloud, Office 365, and other components .
    - Support for standard log formats (syslog, SNMP, CEF, etc.)
- 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
    - Custom detection rule creation with version control
    - False positive suppression mechanisms with tuning feedback metrics
    - Threat correlation with resolution across other Members
    - User behavior analytics (optional and costed separately according to site visit)
- The Solution should Support for STIX/TAXII capabilities.
- For the Log Agent used, the following points should be collected:
    - Centrally managed agents via the SIEM (preferable).
    - Able to collect logs from (text, csv, …) files on Windows devices
    - Able to collect Security, System and Application event logs.
    - Perform File Integrity Monitoring (optional)
    - Perform Registry Monitoring (optional)
    - Monitor for removable devices (optional)
    - Execute PowerShell commands and send output back as logs (optional)
    - The Windows agent must send event data back to the SIEM components encrypted using HTTPS
    - Detect File Permission and Ownership changes.
- 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 must provide Alert suppression to reduce the number of repeated or duplicate detection alerts.
- The solution should support data masking (optional). The bidder should identify and describe any embedded features within the proposed solution that enhance data privacy and protection.
- SIEM must support multi-tenancy:
    - Ensure each tenant can access only its own data.
    - Provide a web-based portal with customizable dashboards and full Role-Based Access Control (RBAC) capabilities.

    - To ensure the integrity and confidentiality of the information collected from log sources, the solution should support granular Role-based Access control "RBAC" to limit certain users to access specific logs and down to fields level
- 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.
- The bidder should support operations that will help CERT to manage SIEM, the following 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 accepting the license from acceptance committee.
- The winner bidder should provide full documentation for the project, the below is the minimum accepted documents for the project:
    - low level design
    - high level design
    - Implementation manuals
    - backup / restore procedure
    - Full documentation
    - As-built documentation

5.2 Incident Collaboration / Case management system:

- The Solution should support Core Incident Management
    - Customizable security incident workflows with conditional routing based on type, severity, and CERT entity
    - Automated case creation from Industrial entities SIEM alerts detections.

- If the Industrial entity does not have a SIEM solution, cases should be created based on alerts from other security solutions available at the regulated entity (if applicable).
- Standardized incident categorization aligned with NCSC 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 5 CERT entities with 3 users per entity.
- Incident Collaboration should be used in for MIT and 5 CERT Industrial entities.
- The solution must have workflow to track the incidents and to support collaboration.
- The solution must support multi-factor authentication (MFA) for the users of the solution.

- The Solution should support Multi-tenant Support

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

- The Solution should support Incident Collaboration Features

  - Collaboration within incident cases
  - 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 communication with end users through different channels.
  - Digital evidence management with hash verification
  - Ability to push notifications, e.g. information when an Incident has been updated. These notifications also can be used in custom workflows
  - Integration with SMTP gateway for notifications
- The Solution should have capabilities of cyber intelligence

  - 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
  - Indicator of Compromise (IOC) extraction and management

- Two-factor authentication and granular access controls
- Integration with proposed MIT SIEM and CERT entity SIEM

- 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
- Other features:
  - Centralized, multi-tenant, web-based Cyber Incident Reporting, Ticketing, and Tracking System (on-premises).
  - Support API integrations for data exchange.
  - Support English and Arabic for all data entry and reporting.
  - Support bidirectional ticket creation and synchronization within the platform.
  - Ensure all communications are encrypted over trusted networks using standard security protocols.
  - Restrict API access based on IP whitelisting

5.3 External Application Vulnerability Scanner:

- The solution should cover 20 web applications as a base line with the ability to change (add/remove) applications without affecting the licenses
- The solution should automate black box or white 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 that are used by the CERT entities.
- Web Application Scanner should have RBAC user access management.
- Web Application Scanner can be on premise or cloud
- Web Application Scanner should support at least 2 users.

5.4 Sectorial Risk Rating Solution:

- 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 MIT 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 5 licenses for entities with ability to expand.
- The Solution must be able to show a list of infections, exposed services, list of vulnerabilities.
- The Solution must be able to report which CERT entities have security issues related to their current configuration such as mobile applications, SSL certificates, etc.
- The Solution must keep 12 months of historical data for each CERT entity 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.
- The solution should have the ability to show forensics related to infections, risk vectors and vulnerabilities related monitored and non-monitored entities within the sector.
- Solution should be able to provide the monitored IPs and Domains for CERT 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 show the list of products and services used by the monitored entities.
- 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 Support Country Based report for the CERT Analysis.
- The solution should be able to compare CERT entities' security ratings against each other.
- The platform comparison feature should display a security rating of multiple companies at once.
- The platform should have the ability to perform benchmarking at the sectorial level within Jordan and for the same sector regionally or worldwide.

5.5 Threat Intelligence platform (OpenCTI Community Version)

- Must be integrated with NCSC threat intelligence feeds.
- 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 feeds should be added to CERT Feeds.
- 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.
- Should be configured to allow for bidirectional sharing with Threat Intelligence Platforms (TIPs) used by CERT entities and NCSC

6. Security Support Services

6.1 Security Support Team Requirements:

- Level 1 (L1): To be primarily staffed by MIT personnel.
- Level 2 (L2) Support:

    - Minimum of 3 dedicated onsite L2 analysts with 2+ years of SOC experience
    - L2 Analysts will remain for the operation of the CERT for the 3 years project period.
    - 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 sector-specific systems and compliance requirements
    - Certifications required: Certified SOC Analyst

  General Requirements:

    - The bidder must mobilize the resident SOC Analysts within one month of the commencement date.
    - The CERT analysts must be the bidder employees.
    - The CERT analysts must Adhere to the CERT policies and procedures and shifts as per the CERT requirements.
    - The contract year for each resident Analyst is one year from the date of written acceptance for the employee, excluding any duration caused by the replacement or force major. Renewal of the contract is subject to approvals from MIT.
    - The employees have the right to have 14 day's annual vacation after coordinating with the responsible CERT Management.
    - Resident Analyst must be Jordanian.
    - All work Must be done on site.
    - All Salary/Compensation including but not limited to Income tax, social security participation is the bidder's responsibility, CERT will not hold any liability for any Salary/compensation for the bidder's employees. The bidder must mobilize the resident SOC Analysts within one month of the commencement date.

7 Core Infrastructure

7.1 General requirements:

- The Core Infrastructure consists of the following:
  - Next Generation Firewalls that will be used to secure CERT infrastructure and Site to Site VPN with CERT entities for incident 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 2025 at least
- All devices included in this tender are supplied in sealed boxes from the manufacturer.
- The infrastructure design and specifications should be verified with the vendors of required solutions.
- 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 preliminary acceptance date.
- 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.
- Accepted vendors for the Firewalls:
  - Fortinet
  - Palo Alto
  - Cisco
- Accepted vendors for the Network Devices:
  - HPE
  - DELL
  - Cisco
  - Fortinet
- Accepted vendors for the Server Nodes:
  - HP
  - Dell

- The proposed hardware must have the following components **(the bidder should calculate the proper specifications for the HW/SW below and provide the suitable sizing in the bidder's offer based on site visits. Scientific proofs should be provided in the offer):**

7.2 Next Generation Firewall (QTY 2)

- The bidder should consider providing at least the below features and capabilities based on the site visits
    - High FW Throughput (PPS)
    - Threat Protection
    - Dual Hot-Swappable AC input
    - IPsec VPN Throughput
    - License required: IPS, URL Filtering, Application Control, VPN
    - Any additional features

7.3 Core Switches (Qty 2)

- The bidder should consider providing at least the below features and capabilities based on the site visits
    - Switching capacity
    - High Switching bandwidth.
    - Uplink ports and SFP/SFP+
    - Any additional features

7.4 Access Switches (Qty 2)

- The bidder should consider providing at least the below features and capabilities based on the site visits
    - Switching capacity
    - High Switching bandwidth.
    - Uplink ports
    - Any additional features

7.5 Server Nodes:

- The bidder should consider providing at least the below features and capabilities based on the site visits
- Minimum 3 Nodes for high availability and performance based on HCI technology.
- HCI requirements
    - The HCI should Support VM Live Migration
    - The HCI should Support CPU/RAM Hot-add for online VMs
    - All the solution components (server hardware, hypervisor, software-defined-storage, data protection) must be managed from a single management.

- The Solution should be Hypervisor agnostic. (Must support: VMware, Hyper-V, AHV, etc)
- The solution must have the ability to natively present its storage services to VMs, Containers, and External physical servers as Block storage iSCSI or File storage or equivalent method.
- Data Availability: 99.99% data availability guaranty should be provided, other than that a redundant component should be added.
- The HCI should Support all major x86 operating systems including:
  - Windows Server All Supported versions
  - RHEL All Supported Version
  - CentOS All Versions required
  - Ubuntu All Versions required
  - SUSE Linux Enterprise Servers
  - Oracle Linux
- The management Solution must allow for seamless cluster expansion (Adding nodes) with no downtime.

- Virtualization
  - Bidder must offer suitable Virtualization solution and needed operating systems

7.6 Rack Cabinet:

- High Servers Rack, must be same brand as server and storages:
- PDUs: Redundant PDUs
- KVM: with cables and all accessories.
- Console: LCD Console with keyboard and pointing device.
- Support: 3 years support.

7.7 CERT Workstations:

- Number of workstations: 10 Units
- Minimum Specs:
  - Original Activation Windows 11 pro 64bit.
  - core i7 latest generations.
  - CPU: Intel (16 core, base frequency 2.6 GHz).
  - Display : Minimum 2*27 (same Brand as Workstation).
  - Storage: 1TB Nvme M.2 + 1 TB Nvme M.2(Boot).
  - Original Mouse and keyboard (same Brand as Workstation).
  - RAM: 16GB (DDR5).
  - Latest version of Microsoft Office.
- Accepted vendors:
  - Dell

- Lenovo
- HP

7.8 CERT Laptops:

- Number of Laptops: 5 Units
- Minimum Specs:
  - core i7 latest generations.
  - CPU: Intel (16 cores, base-frequency 3.0 GHz).
  - RAM: 16GB DDR5.
  - Storage: 2TB Nvme M.2.
  - Display: 15 inches.
  - Included: Original branded backpack (same as laptop).
- Accepted vendors:
  - Dell
  - Lenovo
  - HP

8 Project Management and Timeline

8.1 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 duration the provider should provide status reports to MIT and NCSC as follows:
  - Status reporting
  - requirements Documentation Progress tracing metrics
  - Executive-level reporting

8.2 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

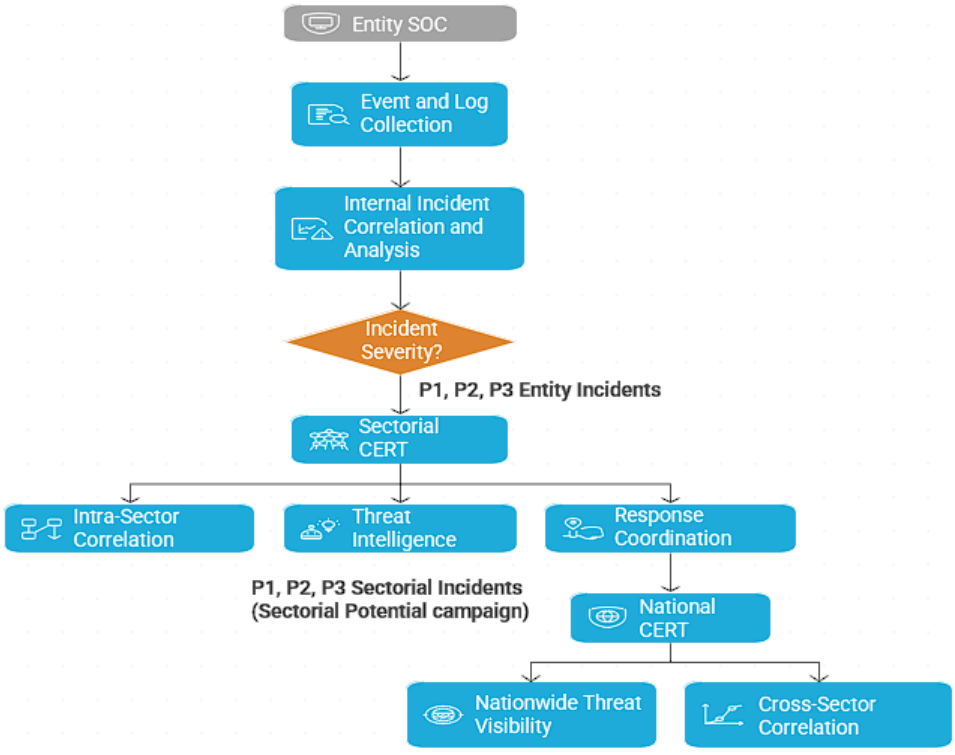
- Technical Evaluation - Minimum passing score: 80%

9.2 Detailed Technical Evaluation Criteria

Evaluation Criteria	Weight	Maximum Score	Sub-Criteria and Scoring
Technical Solution Architecture and Compliance	40%	40 points	○ Security solution design and capabilities (20) pt ○ Infrastructure architecture (10 pts) ○ Integration and scalability (10 pts)
Technology Partnerships and Licensing	10%	10 points	○ Vendor partnerships and certifications (5) pts) ○ License compliance and flexibility (5pts)
Model Delivery	10%	10 points	○ Delivery approach (5 pts) ○ SLA definitions and commitments (5 pts)
Implementation and Support Team Expertise and Staffing	10%	10 points	○ OT/IT security expertise (5 pts) ○ Certified Engineer per technology provided (5 pts)
Implementation Methodology	10%	10 points	○ Project management approach (10 pts)
Reference Projects and Experience	20%	20 points	○ CERT/SOC implementation experience (10 pts ○ Technology Reference for CERT Solutions (10 pts)
TOTAL	**100%**	**100 points**	**Minimum passing score: 80 points**

Jordan's Cybersecurity CERTs & SOCs Architecture

Entity > Sectorial CERT > National CERT Incident Management Flowchart



Appendix: Support Procedures (SLA)

The winning bidder is required to comply with the following:

1. Support activities are required to cover all components of the proposed solutions.
2. Response /Resolution Times and Severity Levels defined in the table below

Support Requirements

The winning bidder is required to provide the following:

1. Assign a contact person/account manager to be responsible of this contract
2. Assign a hot line number to be used for reporting severity 1 technical incidents
3. Define Escalation Procedure including the levels of escalation and name and contact details for contact person
4. Use a ticketing system that records all technical incidents reported by operational team, that can be accessed by CERT and generate reports of various CERT technical incidents
5. Issue a service report after each site visit, to register reported technical incident, root cause, and followed procedures till a successful resolution
6. Technical support is during the official working hours of the institution or outside the official working hours for emergency cases after the approval of the concerned department in the institution

Severity Levels

Severity One (Urgent)

A severity one (1) issue is a catastrophic production problem which may severely impact the Required Service\Solution Availability, in such case, part or all Required Service\Solution production components are down or not functioning; loss of production data or availability of services and no procedural work around exists.

Severity Two (High)

A severity two (2) issue is a problem where the Required Service\Solution is functioning but in a severely reduced capacity. The situation is causing significant impact to portions of business operations and productivity of Required Service\Solution. The system is exposed to potential loss or interruption of service.

Severity Three (Medium)

A severity three (3) issue is a medium-to-low impact problem which involves partial non-critical functionality loss one which impairs some operations but allows the Required Service\Solution users/administrators to continue to function. This may be a minor issue with limited loss or no loss of functionality or impact to the client's operation and issues in which there is an easy circumvention or avoidance by the end user.

Severity Four (Low)

Important problem but it can wait no loss of functionality or impact to the client's operation and issues in which there is an easy circumvention or avoidance by the end user.

Table 1: Response, Resolution, times for different severity levels

Severity	Response Time	Resolution Time
1	1 hour	4 hours.
2	3 hours	24 hours
3	4 hours	72 hours
4	8 hours	one week

* Support required being 24x7 basis

Where:

Response Time: Time taken to acknowledge receiving of reported technical incident calculated from the time sending an email explaining the technical incident, opening a ticket on bidder ticketing system, or conducting a phone call with the assigned support engineer by the bidder or bidder's first line of support.

Resolution Time: Time taken to solve the reported technical incident completely. Resolution Time is calculated from the end of the defined response time for each severity level as shown in the above table.

Escalation Procedure and Penalties:

For technical incidents classified as Severity Level 1, 2, 3 & 4, if bidder:

1. Passed the Response Time: first level of escalation will be applied by notifying bidder's Technical Support Manager or the assigned contact person.
2. Passed the Resolution Time: operational team is entitled to fix the problem and to apply penalty on the winning bidder in accordance with the following criteria in the below table and all costs incurred by operational team for fixing will be charged to the winning bidder.

Table 2: Penalties

Severity	Definition	Penalty
1	Must be done, essential to business survival. Business can't continue	A penalty of 100 J.D. shall be applied for each hour pass the resolution time. This penalty shall continue for the first 24 hours (100x24). If delay continues, then the penalty of 3000 J.D. per day shall be applied and for the maximum duration of 3 days; after that, 3rd party will be called to fix the problem.
2	Should be done, near essential to business survival.	A penalty of 1500 J.D. shall be applied for each day pass the resolution time. This penalty will be

		applied for the maximum duration of 4 days; after that, 3rd party will be called to fix the problem.
3	Could be done, high benefit to business if time and resources are available.	A penalty of 1000 J.D. shall be applied for each day pass the resolution time. This penalty will be applied for the maximum duration of 5 days; after that, 3rd party will be called to fix the problem.
4	Important problem but can wait	A penalty of 500 J.D. shall be applied for each day pass the resolution time. This penalty will be applied for the maximum duration of 10 days; after that, 3rd party will be called to fix the problem.