Hutchison Ports Abu Qir Containers Terminals S.A.E

(Private free Zone Company)

Request for Tender

For

Supply, Installation, Configuration, Testing, Implementation and Commissioning of

Managed Security Service Provider (MSSP)

for Hutchison Ports Abu Qir Containers Terminals *S.A.E Start-up*

Reference No. (T/AQCT/T/02/2026)

(Version 1.0)

May 2026

1 INTRODUCTION

1.1 Our work

Hutchison Ports Abu Qir Containers Terminals S.A.E is a part of the Hutchison Port Holdings' (HPH) global network of container terminals. HPH is the leading independent port developer and operator in the world. In its short operating target, HUTCHISON PORTS ABU QIR CONTAINERS TERMINALS S.A.E need to establish itself as the preferred terminal operator by achieving high levels of operating efficiency and customer satisfaction.

1.2 Purpose

Hutchison Ports Abu Qir Containers Terminals S.A.E invites qualified partners to submit their best competitive solutions to provide a comprehensive solution for deferent services and hardware to have excellent implementation and cover all technical requirement to achieve operation needs.

1.3 PRE-QUALIFICATION CRITERIA

1- The bidder provides an undertaking that the TECHNOLOGY PROVIDER shall provide Direct Premium support for the supplied hardware including system software.
2- All service requests for MSSP security solutions should be received, managed, executed, and tracked to closure by the TECHNOLOGY PROVIDER. Bidder should submit declaration letter stating the same, accompanied by similar declaration from the Hardware TECHNOLOGY PROVIDER.
3- Hutchison Ports Abu Qir Containers Terminals reserves the right to accept or reject any bid or to annul the bidding process and reject all bids at any time prior to award of the Contract / Purchase Order without assigning any reason whatsoever and without thereby incurring any liability whatsoever to the affected Bidder(s). Mere submission of tender documents shall not mean fulfilment of requirements of eligibility of the Bidder(s).
4- The quantities mentioned in the tender are indicative, and the actual number may vary depending on the requirement. While placing the order, Hutchison Ports Abu Qir Containers Terminals S.A.E may increase or decrease the quantities of items in the

tender or request to deliver the items in patches according to the needs and the bidder shall be bound to supply the quantities of items so ordered.

5- Bidders must submit below documents

a- Bidder's and TECHNOLOGY PROVIDER's declaration letter stating that implementation and all service requests for MSSP security solution would be received, managed, executed, and tracked to closure by TECHNOLOGY PROVIDER.
b- Direct Premium Support undertaking from TECHNOLOGY PROVIDER which should be minimum of 24x7 remote support with maximum resolution time of Next Business Day (NBD).
c- Delivery plan & schedule.
d- Bill of material and quantity with TECHNOLOGY PROVIDER Product and Services Part No.
e- Completed technical specifications.
f- Product brochures and cross reference document pertaining to technical specification (as relevant).

2 MSSP SECURITY SOULTION

2.1 PURPOSE OF THE PROJECT:

The purpose of this RFP is to invite technically and commercially competitive proposals from reputed manufacturers/authorized representatives for an **MSSP Security solution**. The vendor engagement will involve Supply, Installing, Configuring, Testing, Implementing, Commissioning, and training of the new solution, as well as providing incident and product support as per Scope of work and Technical Specifications given in this RFP, at Hutchison Ports Abu Qir Containers Terminals two Datacenters.

2.2 SCOPE of work

The broad scope of work as detailed in this section refers to the Hardware and System software that is procured through this tender and used for Supply, Installing, Configuring, Testing, Implementing, Commissioning, and training of the **MSSP Security solution** at the two primary Datacenter's at Hutchison Ports Abu Qir Containers Terminals S.A.E. this scope of work shall include, but not be limited to, the following:

2.2.1 GENERAL CONDITIONS

- For the purpose of this RFP, the term "TECHNOLOGY PROVIDER" refers to the Prime Bidder submitting the proposal. The Prime Bidder may be a third-party MSSP and is not required to be

the original manufacturer of the supplied hardware or software. Any obligations related to firmware updates, spare parts, EOL/EOS, or hardware warranty apply only where the Prime Bidder supplies such hardware/software as part of the solution. The Prime Bidder remains fully responsible for delivering all MSSP services and coordinating with any manufacturers or partners as required.

- The MSSP solution must be cloud-native, and all SIEM/SOC capabilities shall be delivered as a cloud service.
- If the bidder's proposed architecture requires on-premises log collectors (physical or virtual) to gather or normalize logs before forwarding them to the cloud SIEM, the bidder shall supply such collector appliances as part of the proposal.
- In this case, all hardware-related requirements in this RFP — including warranty, spare-parts availability, firmware and BIOS updates, EOL/EOS restrictions, and 5-year support commitments — shall apply only to the supplied collector appliances.
- The TECHNOLOGY PROVIDER shall be doing Project Management for the entire Project from commencement to final handing over for live use. The proposed solution must be supported for a period of 1 year as per RFP and Abu Qir Containers terminal's (AQCT) requirement.
- The TECHNOLOGY PROVIDER must prepare architecture design, optimize network to increase performance, documentation, project plan and training as part of the implementation services.
- Installation and configuration of supplied hardware associated system software and system integration must be carried out by TECHNOLOGY PROVIDER.
- Bidder/TECHNOLOGY PROVIDER should propose highly scalable solutions. Solutions with limited scalability would not be acceptable to Hutchison Ports Abu Qir Containers Terminals. Solutions which are not mature for over 1 year should not be quoted.
- The TECHNOLOGY PROVIDER shall provide a comprehensive Project Plan including Risk, Quality, Migration, Conversion, Resource, Change and Communication Management Plan. The bidder must submit a detailed plan for implementation of the solution. The plan should include the full scope of the project as mentioned above. On acceptance of such plan by Hutchison Ports Abu Qir Containers Terminals, the TECHNOLOGY PROVIDER is required to carry out the implementation, customization as applicable including supply, installation, and testing of solution etc. The TECHNOLOGY PROVIDER shall also handle all matters relating to the configuration and operation of the system including but not limited to application, system interfaces, documentation, user manual and training for the successful implementation of the system. The project plan update to be published bi-weekly till the project completion.
- The Bidder/TECHNOLOGY PROVIDER shall be responsible for performing the necessary changes in the configuration required for Hardening and/or request directed by security team & audit team.
- The Bidder/TECHNOLOGY PROVIDER shall be responsible for firmware patches/bugs, fixes BIOS upgrade and Version Upgrade of software.

- The Bidder/Technology Provider shall be fully responsible, at no additional cost, for performing all necessary configuration changes, tuning, and integration activities on the existing firewalls and security solutions owned by the Client to ensure proper implementation, operation, and security of the proposed solution.
- The Bidder shall ensure that all changes are executed in compliance with the Client's security policies, industry best practices, and applicable regulatory requirements. Any misconfiguration, service disruption, or security incident resulting from these activities shall be the sole responsibility of the Bidder.
- The Bidder shall coordinate all changes in accordance with agreed change management procedures and shall ensure minimal impact on ongoing operations. In case of any service disruption, the Bidder must restore services within the agreed Service Level Agreement (SLA) timelines. Furthermore, the Bidder shall document all configurations and changes performed and provide full handover documentation to the Client upon completion.
- The Bidder shall provide a formal and enforceable Service Level Agreement (SLA) for the Managed Security Services (MSSP) solution, including but not limited to : guaranteed service availability, 24/7 monitoring, defined incident response and resolution times by severity level, escalation procedures, and periodic reporting. The SLA shall include measurable Key Performance Indicators (KPIs) and applicable service credits or penalties in case of non-compliance.
- The Bidder/TECHNOLOGY PROVIDER shall be responsible for generation, and submission of necessary documents required during various phases of project viz. planning, installation, commissioning, rollout, acceptance testing, project diagrams and other reports etc. All such documents shall commence only after the same is approved by Hutchison Ports Abu Qir Containers Terminals.
- The Bidder/TECHNOLOGY PROVIDER should provide a detailed project plan in terms of activity and phase-wise timelines (no. of days) required for executing the project with the details of deliverables and milestones including the delivery of Server components. The Bidder/TECHNOLOGY PROVIDER shall inform the name of the Project Manager who would be the single point of contact during the complete project implementation.
- The TECHNOLOGY PROVIDER must analyze, review, and gather performance metrics and ensure it performs optimally.
- The Bidder/TECHNOLOGY PROVIDER shall be responsible for installing / configuring of all patches / updates / upgrades required for the offered solution without any extra cost to Hutchison Ports Abu Qir Containers Terminals during the warranty period.
- All service requests for MSSP Appliance should be received, managed, executed, and tracked to closure by the TECHNOLOGY PROVIDER and not through Authorized Service Provider.
- The bidder shall Plan & Design the Architecture services from the TECHNOLOGY PROVIDER. The entire hardware and software supplied under this RFP must be installed and configured by TECHNOLOGY PROVIDER only & TECHNOLOGY PROVIDER must submit a report indicating

compliance to reference architecture and best practices. The bidder to make necessary arrangements for the same and Hutchison Ports Abu Qir Containers Terminals will not pay any additional cost for implementation/configuration by TECHNOLOGY PROVIDER.

- Hutchison Ports Abu Qir Containers Terminals reserves the right to shift the equipment to a suitable location depending upon the need. The Bidder will arrange to uninstall, shift the equipment, re-install, configure and commission the same at the shifted location and making the entire system operational without any additional cost to Hutchison Ports Abu Qir Containers Terminals, however, Hutchison Ports Abu Qir Containers Terminals will bear the transportation charges and transit insurance.
- All related documents, manuals, catalogues, and information furnished by the bidder shall become the property of the Hutchison Ports Abu Qir Containers Terminals. Detailed process documentation, and SOP‟s (Standard Operating Procedure) should be submitted before project signoff.
- Hutchison Ports Abu Qir Containers Terminals may opt for Audit through a third party Authorized Agency or by the Terminal officials for the supplied hardware and Software. Successful bidder is required to coordinate with the Terminal Officials& Audit agency execute relevant test cases.
- Hutchison Ports Abu Qir Containers Terminals will have a periodic review of technology. Successful bidder will supply the models approved as per technical aspects. In case any of the models becomes end of support during entire contract period, then Successful bidder will provide the latest model available at no extra cost to Hutchison Ports Abu Qir Containers Terminals without disruption in performance of services/applications.
- During the Contract Period, in case there is hardware failure three or more times in a period of less than three (3) months, then it shall be replaced by equivalent or higher-level new equipment by the Successful bidder at no cost to the Hutchison Ports Abu Qir Containers Terminals.
- The Bidder/TECHNOLOGY PROVIDER must Proposed “turnkey” MSSP security solution.
- The successful bidder must conduct a mandatory Proof of Concept (POC) to validate the MSSP solution capabilities, including SIEM (preferred Microsoft Sentinel), SOC monitoring, threat detection, and integration with existing tools. The POC must be approved by Hutchison Ports Abu Qir Container Terminals IT management before full deployment.
- The MSSP solution must provide comprehensive security monitoring for both IT and OT environments, including ICS/SCADA systems and industrial network protocols. The vendor shall ensure integration with OT security tools (e.g., Claroty) or provide native OT monitoring capabilities.
- The MSSP shall perform OT/ICS monitoring based on telemetry provided by the existing OT security tools (e.g., Claroty, or equivalent solutions already deployed by the Customer). The MSSP is not required to deploy new OT sensors unless explicitly requested by the Customer.

- OT monitoring shall rely on passive integrations only (API, syslog, or collector-based ingestion) and shall not require active scanning or direct interaction with PLCs, RTUs, or SCADA controllers. The MSSP is responsible for processing, correlating, enriching, and escalating OT alerts, but operational control and direct remediation actions within the OT environment remain with the Customer's OT team.
- If the bidder requires additional OT data sources, these must be clearly identified in the proposal, along with required access, connectivity, and deployment considerations.
- The proposed solution should include security data collection, data analysis, reporting, incident detection, semi-automated and automated response, compliance with relevant regulations, and threat intelligence features.
- The proposed solution should have advanced data enrichment, reporting, analysis, alarm, event management, threat detection, correlation, threat intelligence and incident response capabilities.
- The proposed solution should support data collection with SYSLOG, SSH, SMB, API, FLOW, SFTP, WMI protocols.
- The proposed solution should provide a suitable framework for future expansions and integration with other 3rd Party solutions and IoT Devices.
- During the data collection process, the data generated, the time of receipt and the time of data creation should be recorded separately.
- The proposed system will be able to enrich the data collected from the sources by feeding from global and local Cyber Threat Intelligence Services.
- The proposed system will be able to trigger alerts incase where logs aren't collected for a specific period using any kind of health check feature
- The proposed solution should be able to automatically analyze the number of EPS on the proposed system and inform via SMS/mail in case of anomaly increase or decrease at the determined rate.
- The MSSP shall not charge additional fees for cases where a special correlation is required to be written on the proposed solution.
- The proposed solution should support proactive investigation and threat hunting.
- The proposed solution should support automated and semi-automated response features.
- The proposed solution should collect logs from log data sources available in distributed networks.

2.2.2 DELIVERY ACCEPTANCE TEST

- The successful bidder shall submit test report. The report should include the below contents:
    a. Test case
    b. Test case description

c. Expected result
d. Actual result
e. Pass / fail
f. Screen capture of the result

2.2.3 SUPPLY AND DEPLOYMENT

- The MSSP solution must be delivered as a cloud-native service with high availability (HA), ensuring resilience and business continuity.
- All components required for MSSP service delivery—such as computing resources, storage, management consoles, orchestration tools, and security analytics—must be provisioned and configured by the TECHNOLOGY PROVIDER or authorized partner prior to activation, enabling rapid onboarding.
- The successful bidder shall provide all necessary cloud resources, licenses, and configurations required for the full functionality of the MSSP solution, including:
  - ✓ 24/7 Security Operations Center (SOC) monitoring
  - ✓ SIEM platform for log collection, correlation, and dashboards
  - ✓ Threat detection and response capabilities
  - ✓ Threat intelligence feeds
  - ✓ Compliance and regulatory reporting tools
- The bidder is responsible for end-to-end deployment, including:
  - ✓ Secure connectivity between the MSSP platform and Hutchison Ports Abu Qir Container Terminals' infrastructure (on-premises and cloud).
  - ✓ Integration with existing security tools (Qualys, Nessus, CrowdStrike, Microsoft defender, Zscaler, Palo Alto, FortiGate, F5, Imperva, Cloudflare WAF).
  - ✓ Configuration of dashboards, alerts, and reporting as per agreed requirements.
- A comprehensive project execution plan must be submitted prior to implementation, ensuring zero disruption to network security. The plan must include:
  - ✓ Secure onboarding process
  - ✓ Data residency compliance
  - ✓ Risk mitigation measures during migration
- The bidder shall provide all necessary documentation, including:
  - ✓ Operational and user manuals
  - ✓ Hardening guides
  - ✓ System test reports
  - ✓ Architecture diagrams
- The bidder must ensure that all cloud services, APIs, and integrations required for MSSP functionality are provisioned. Any missing components identified during deployment must be provided at no additional cost or delay.
- The bidder and TECHNOLOGY PROVIDER are responsible for testing the MSSP platform to ensure proper operation, including:
  - ✓ HA failover testing
  - ✓ Security validation

- ✓ Performance benchmarking
- ✓ Verification of SOC alerting and incident response workflows

- The bidder shall provide a detailed RACI for detection, triage, containment, eradication, recovery, and communications; a Runbook Library and Change Control process covering SIEM rules, SOAR playbooks, and integrations, with monthly governance reviews.
- For all endpoints and servers covered by CrowdStrike MDR, the MSSP's role is monitoring, correlation, enrichment, and escalation only. Endpoint response authority (including actions such as host isolation, quarantine, RTR commands, IOC blocking, or policy modification) remains strictly with CrowdStrike MDR and the Customer.
  The MSSP shall:
- Integrate CrowdStrike telemetry and detections into the SIEM/SOAR.
- Create and tune use cases and correlation rules involving CrowdStrike events.
- Escalate endpoint-related incidents to CrowdStrike MDR based on the agreed workflow and track them to closure.
- Not perform any endpoint-level actions in CrowdStrike Falcon unless the Customer provides explicit written authorization for a specific case.
- This limitation applies only to endpoint and server response.
- It does not limit the MSSP's authority for network, firewall, WAF, or Zscaler containment actions as defined in this RFP.
- The MSSP vendor shall be responsible for supplying any hardware or software necessary to operate log collectors within Hutchison Ports Abu Qir Container Terminals' data centers. These collectors must securely forward logs to the cloud MSSP platform without introducing additional agents on endpoints or servers beyond approved solutions (CrowdStrike and Microsoft Defender).

2.2.4 CONFIGURATION AND COMMISSIONING

- The successful bidder shall be responsible for commissioning the MSSP solution by securely integrating it with Hutchison Ports Abu Qir Container Terminals' infrastructure (on-premises and cloud) and configuring all services according to the compliance requirements and international cybersecurity best practices.

- The configuration must include:

  - ✓ Unified management interfaces for SOC operations, SIEM dashboards, incident response workflows, and reporting.

  - ✓ Integration with existing security tools (Qualys, Nessus, CrowdStrike, Microsoft Defender Zscaler, Palo Alto, FortiGate, F5, Imperva, Cloudflare WAF).

  - ✓ Secure onboarding of log sources, endpoints, network devices, and cloud workloads.

- The TECHNOLOGY PROVIDER and bidder will be responsible for:

  - ✓ Provisioning and configuring all necessary cloud resources and licenses for MSSP services.

- ✓ Setting up high availability (HA) across multiple cloud regions or availability zones.
- ✓ Configuring SIEM correlation rules, alerting thresholds, and dashboards for real-time monitoring.
- ✓ Enabling threat intelligence feeds and automated response playbooks.

- The vendor shall configure OT log sources and ensure secure integration with SIEM (Preferred Microsoft Sentinel). Commissioning must include validation of OT alert ingestion and correlation with IT events.
- Acceptance Criteria for Commissioning
  1. Functionality Tests
     - ➢ Verification of MSSP platform functionality, including:
       - ✓ SIEM log ingestion and correlation
       - ✓ Threat detection and alerting
       - ✓ Patch and update management for MSSP components
       - ✓ Secure network connectivity between MSSP and client infrastructure
       - ✓ Dashboard monitoring of system health (CPU, memory, storage, alerts)
     - ➢ Validation of compliance reporting capabilities.
  2. Failover Tests
     - ➢ High availability and disaster recovery validation.
     - ➢ Testing automated failover for SOC monitoring and SIEM services.

2.2.1 TECHNICAL SPECIFICATION FOR MSSP SECURITY SOLUTION

Item	Description	Qty	UOM
MSSP Subscription	Fully managed MSSP service for 1 year, including 24/7 SOC monitoring, threat detection, incident response, and compliance reporting	1	Year
SIEM Platform	Preferred Microsoft Sentinel – Cloud-native SIEM with log ingestion, correlation, dashboards, and alerting	1	Tenant
Threat Intelligence	Global threat intelligence feeds integrated into MSSP platform	Included	EA
Endpoint & Network Integration	Integration with existing tools (Qualys, Nessus, CrowdStrike, Microsoft Defender, Zscaler, Palo Alto, FortiGate, F5, Imperva, Cloudflare WAF)	Included	EA
OT Security Monitoring	Coverage for OT environments integrated into MSSP service	Included	EA
AD Monitoring	Continuous monitoring of Active Directory and Azure AD integrated into MSSP service	Included	EA
Compliance Reporting	Automated compliance reports (ISO 27001, GDPR, local regulations)	Included	EA

HA & DR	High availability across multiple cloud regions and disaster recovery capability	Included	EA
Log Retention	Minimum 6 months (3 Hot Data/Index Data and Cold Data/Archive Data) log retention in compliance with regulatory requirements	6	Month
Incident Response SLA	Critical IT or OT incidents response within 15 minutes, high severity within 30 minutes, and forensic report within 48 hours	Included	EA
Onboarding & Configuration	Secure onboarding of all log sources, endpoints, and network devices	Included	EA
Support	24/7 support and escalation procedures	1	Year

Log Source	Vendor	Site 1	Site 2	Site 3	Site 4	**Total**
Firewall(s)	Palo Alto, FortiGate	12	4	6	2	**24**
NAC(s)	Cisco ISE, Huawei Imaster, FortiNAC	4	2	4	2	**12**
WAF(s)	F5, Cloudflare	2	1	2	0	**5**
EDR/XDR	CrowdStrike	1				**1**
Web Filtering	Zscaler	1				**1**
PAM		1	0	0	0	**1**
Vulnerability	Qualys, Nessus	2	1	1	1	**5**
Physical Server(s)		10	25	15	2	**52**
Virtual Server(s)		75	60	80	0	**215**
M365		1				**1**
Switch(s)	Cisco, Huawei, Fortinet	50	105	85	10	**250**
Wireless	Cisco, Altai, Huawei, Fortinet	5	2	0	1	**8**
Workstation(s)		235	100	120	100	**555**
						1130

- **Agent Installation Restriction**
  - ✓ The MSSP vendor must NOT install any additional agents on endpoints or servers other than CrowdStrike or Microsoft Defender. The vendor must integrate with these existing solutions for endpoint detection and response, leveraging their APIs and capabilities for threat detection, response automation, and forensic analysis.
  - ✓ This restriction also applies to any form of data collection agents, service daemons, monitoring probes, or log forwarders on Customer infrastructure. All log collection must be performed using existing solutions (CrowdStrike, Microsoft Defender) or standard interfaces (API, syslog, CEF, connector-based ingestion). No additional host-based agents are permitted on any Customer server, endpoint, VM, or OT asset.
  - ✓ The MSSP shall not install any agents or software components on Customer endpoints, servers, Domain Controllers, or OT assets, even if the MSSP uses its own SIEM platform. All data collection must be performed using standard interfaces such as Windows Event

Forwarding (WEF), syslog/CEF, API-based ingestion, cloud connectors, and integrations with existing solutions (CrowdStrike, Microsoft Defender, AD/Azure AD APIs). No MSSP proprietary agent is permitted anywhere in the Customer environment.

- **SIEM Management**
  - The MSSP vendor must provide end-to-end management of the SIEM platform (Preferred Microsoft Sentinel), including:
    - ✓ Initial configuration and onboarding of all log sources.
    - ✓ Continuous tuning and optimization of correlation rules and alerts.
    - ✓ Patch and update management for SIEM components.
    - ✓ Dashboard customization and reporting.
    - ✓ Integration with threat intelligence feeds and automated response playbooks.
    - ✓ Continuous monitoring and tuning
    - ✓ Rule creation and correlation logic
    - ✓ Patch and update management
    - ✓ SIEM availability: 99.9% uptime guaranteed.
- **SOC Operations**
  - 24/7 monitoring by a dedicated Security Operations Center (SOC).
  - Real-time detection and response to security incidents.
  - Threat hunting and proactive analysis.
- **Integration Requirements**
  - Seamless integration with existing security tools:
    - ✓ Vulnerability scanners (Qualys, Nessus)
    - ✓ Endpoint protection (CrowdStrike, Microsoft Defender)
    - ✓ Web filtering (Zscaler)
    - ✓ Firewalls (Palo Alto, FortiGate)
    - ✓ WAF (F5, Imperva, Cloudflare)
  - The MSSP solution must monitor Active Directory and Azure AD for suspicious activities, including:
    - ✓ Privilege escalation attempts
    - ✓ Unauthorized changes to Group Policy Object (GPO)
    - ✓ Account lockouts and brute-force attempts
    - ✓ Detection of Kerberos attacks (Golden Ticket, Pass-the-Hash)
    - ✓ Integration with Microsoft Sentinel for AD audit logs
- **Compliance & Reporting**
  - Automated compliance reports for ISO 27001, GDPR, and local regulations.
  - Audit-ready reporting capabilities.

- **High Availability & Disaster Recovery**
    - MSSP platform must operate in HA mode.
    - Disaster recovery plan with defined RPO/RTO.
- **Log Retention**
    - Minimum 6 months log retention in compliance with regulatory requirements.
    - Daily alerts for critical incidents.
    - Weekly operational reports.
    - Monthly compliance and performance reports.
- **Security & Privacy**
    - Data residency compliance (region to be specified).
    - Encryption in transit and at rest.
    - Role-based access control (RBAC).
- **Incident Response**
    - Critical incidents: Response within 15 minutes.
    - High severity incidents: Response within 30 minutes.
    - Medium severity incidents: Response within 4 hours.
    - Low severity incidents: Response within 24 hours.
- **Escalation Procedures**
    - Defined escalation matrix for unresolved incidents.
    - 24/7 contact availability for emergency escalation.
- **Forensic analytics capabilities**
    - The MSSP vendor must provide forensic analytics capabilities to investigate security incidents, including:
        - ✓ Log correlation and timeline reconstruction
        - ✓ Evidence collection and preservation
        - ✓ Root cause analysis and attack path mapping
        - ✓ Support for legal and compliance reporting
- OT Security Monitoring
    - Threat detection mapped to MITRE ATT&CK for ICS.
    - Continuous monitoring of segmentation between IT and OT networks.
    - Ability to ingest OT logs and alerts into SIEM for unified visibility.
    - Integration with existing OT security platforms (Claroty or equivalent).

- SOAR & Automation
    - Playbooks for common incidents (credential leakage, malware on endpoint, malicious URL, suspicious sign-in, C2 beacon, data exfil alerts).
    - Approval gates for containment actions (e.g., isolate endpoint via CrowdStrike, block IP on Palo Alto/FortiGate, apply WAF rule).
    - Rollback procedures and audit logs.
    - All automated or semi-automated SOAR actions that involve endpoint or server containment through CrowdStrike Falcon (e.g., isolate host, quarantine, RTR commands, policy updates) shall be configured as recommendation-only and routed to CrowdStrike MDR and the Customer for execution. The MSSP shall not perform endpoint containment directly.
    - This restriction applies only to endpoint and server's actions. The MSSP retains full authority (based on the RACI and approval gates) to execute or automate network-level containment actions, such as:
    - IP/domain blocking on Palo Alto or FortiGate
    - URL/user policy actions in Zscaler
    - Virtual patching or rule deployment on WAF platforms
    - Firewall rule adjustments
      These network actions remain fully within MSSP responsibility.
    -
- Scalability
    - The MSSP solution must be highly scalable, allowing the addition of new log sources, connectors, or collectors without service disruption. The architecture should support horizontal scaling to onboard additional nodes or resources as the environment grows, ensuring performance and availability remain unaffected.

2.3 Security and Compliance

- The Bidder /TECHNOLOGY PROVIDER Should ensure necessary security features are built into the proposed MSSP solution.
- The Bidder /TECHNOLOGY PROVIDER is responsible for remediation of cybersecurity vulnerability on software and hardware with no additional cost to Hutchison Ports Abu Qir Containers Terminals
- The Bidder /TECHNOLOGY PROVIDER is responsible for Implementation of security measures and policies in alignment with ISO, PCI-DSS, and other relevant compliance standards.
- The Bidder /TECHNOLOGY PROVIDER is responsible for Configuration of integrated security features such as encryption, access controls, and advanced threat protection.

- The Bidder /TECHNOLOGY PROVIDER Should ensure necessary compliance and security hardening as per Hutchison Ports Abu Qir Containers Terminals policies/requirements and submitting recommendations for further improvements to mitigate any possible threats, effective compliance check, better visibility and controls, etc.

2.4 Training and Documentation

- The Bidder /TECHNOLOGY PROVIDER Should Ensuring a smooth handover with detailed documentation and training provided to the Hutchison Ports Abu Qir Containers Terminals IT team.
- Installation and Configuration Documentation (documentation shall include screenshots for steps performed). Standard Operating Procedures (SOP) to be provided for startup-shutdown of MSSP solution, startup-shutdown of individual host.
- The bidder/TECHNOLOGY PROVIDER shall provide detailed drawings of the installed setup after completion of the project. This will also include the printout of important configuration settings of the solution.
- The TECHNOLOGY PROVIDER should provide detailed architecture of the provided solution along Installation and Administration guide which must include High level Design (HLD) and Low-Level Design (LLD).
- MSSP solution diagram.
- detailed BOQ for proposed MSSP solution.
- separate sheet for specification/white paper of the products.

2.5 Project Reporting and Handover

- Submission of commissioning reports detailing the deployment and configuration of the MSSP solution.
- Provision of a comprehensive project completion report summarizing all activities, configurations, and outcomes.

2.6 Maintainability and Warranty Support

The scope under warranty shall cover providing services as described below:

All delivered Hardware and System software in this tender should be monitored and serviced in such a manner to ensure maximum uptime and performance levels. The guarantee / warranty should be of

highest nature extended by the TECHNOLOGY PROVIDER on the date of participation in the Tender (Necessary documentary evidence to be submitted).

2.6.1 MAINTAINABILITY

- The Bidder will have to submit an undertaking from TECHNOLOGY PROVIDER assuring the availability of requisite spare parts for hardware (if any) the maintainability period of 5 (five) years from the date of installation.
- The software & hardware quoted by bidder in this RFP should not be declared as End of Life (EOL) or End of Support (EOS) by the TECHNOLOGY PROVIDER within the 5 years of Purchase order / contract period. In the event of the supplied equipment being declared End of support/End of Life during the contract period of 5 (five) years, the bidder must replace the equipment with equipment having equivalent or higher model.

2.6.2 WARRANTY SUPPORT

- Original Equipment manufacturers (TECHNOLOGY PROVIDER) should have online 24 x 7 support for any hardware or software related issue. The proposed solution should have one window support solution for all the components including hardware, firmware and software used. The support should be from TECHNOLOGY PROVIDER.
- MSSP solution must have direct TECHNOLOGY PROVIDER, L1, L2 and L3 support, 24x7x365 days with unlimited incident support (Telephonic / Web / Email) and technical contacts / contract within 4-hour response time including the unlimited upgrades and updates during tender specific warranty period.
- Provide on-site comprehensive warranty for the supplied items - equipment / system / subsystems (hardware and system software) for a period of one year with 24x7 x 365 remote support and maximum resolution of NBD. The hardware equipment (if any) should be guaranteed / warranted against all defects and failure, and such guarantee / warranty shall include replacement of defective parts / equipment and / or repair of the same free of cost. All warranty shall be onsite. The bidder should confirm in their response that the support during warranty period would be carried out by the TECHNOLOGY PROVIDER for the respective equipment / peripheral. The bidder should also ensure that the SLA (24 x 7 x 365 support with maximum resolution time of NBD) is adhered to, and this must be articulated in the bid response as well. Warranty shall also cover the following:

    a) Installation / re-installation / maintenance / reconfiguration of System software and other supplied software

    b) All system patches, upgrades, service packs etc. of the OS and all other software supplied must be made available free of charge.

    c) Support for integration and update of infrastructure / network configuration and change management of the entire solution (existing as well as that procured as scope of this tender) to meet business requirements.

d) Any change in the IP scheme, if required, limited to all the equipment installed at the Data Centre should be done in consultation with Hutchison Ports Abu Qir Containers Terminals IT team.

- The non-delivery of services or non-response or any breach of information will lead to penalty. The penalty is applicable in respect of non-delivery of services/ support as per the requirement of this RFP.

- In case of item replacement with new one, the new item must be at least same model, and in case the replacement is higher model must be compatible with Hutchison Ports Abu Qir Containers Terminals S.A.E. environment and technically approved by Hutchison Ports Abu Qir Containers Terminals S.A.E
- Exit, Transition & Handover Requirements
  - ✓ Exit & Transition Obligations
    At contract termination (for any reason), the MSSP shall provide full transition assistance to ensure continuity of security operations. All transition deliverables must be provided at no additional cost, except for optional extended support requested by the Customer.
  - ✓ The MSSP must deliver the following within the exit period:
    - ➢ Export of all log data stored in the SIEM (hot and cold), in a standard open format (JSON, CSV, CEF, or Syslog).
    - ➢ Export of all detection rules, including correlation rules, SIEM queries, analytics, normalization logic, and custom use cases created during the service period.
    - ➢ Export of all SOAR playbooks, including automated actions, workflows, and integrations.
    - ➢ Export of all dashboards, reports, and visualizations used by the SOC.
    - ➢ Export of all runbooks, incident handling procedures, and RACI documentation.
    - ➢ Complete incident history, including alerts, escalations, analyst notes, response actions, and timelines.
    - ➢ List of all onboarded log sources, ingestion methods, and configurations.
    - ➢ Assistance to the new MSSP for up to 30 days (knowledge transfer, Q&A, onboarding support).
    - ➢ All detection content, playbooks, runbooks, configurations, and custom development performed under this contract become the intellectual property of Hutchison Ports Abu Qir Containers Terminals S.A.E.
    - ➢ The MSSP shall not restrict, limit, license, or charge for any content developed for the Customer during the contract period.

2.7 UPGRADES AND UPDATES

- The bidder shall be required to provide all future updates and upgrades for the proposed Solution/Appliance/hardware & software provided free of charge during the contract period. If, however, the upgrades/updates are not available then the support for the implemented Solution/ Appliance/hardware & software should be available at

any point of time. The solution (software or hardware or both) provided by the successful bidder should not be declared end of sale within 3 years of sign-off of the project. If at all the solution (software or hardware or both) is declared end of sale within 3 years of signing off, the successful bidder must provide the upgraded version (software or hardware or both) free of charge, to the Hutchison Ports Abu Qir Containers Terminals.

- The solution should provide seamless upgrade for (but not limited to) Firmware, Hypervisor, Storage OS, SDS software, BIOS and other such functions which are required in the solution. All patches for the complete hardware and software solution must come from a single validated source. It should be possible to apply and upgrade all software and Hardware related firmware and patches from the same GUI that is used to manage the MSSP (It should not use the hardware management console for doing firmware upgrade of hardware)

2.8 Additional Consideration

- Payment terms per project - 25% in advance against non-conditional LG, 25% after delivery of Items, 40% after final commissioning & signoff -10% retention until end of the warranty period (Can be released against Non - conditional LG)
- MSSP Service Payment Terms (Cloud / Subscription Components)
  The payment structure described above applies only to hardware or on-premises components (e.g., log collectors) supplied under this RFP.
- For all cloud-native MSSP services (SIEM, SOC, SOAR, threat intelligence, incident response, monitoring, compliance reporting), the payment schedule shall follow a subscription model, billed annually in advance or quarterly, without retention.
- Retention shall not apply to subscription- based MSSP services.
- In the event the bidder provides a combined hardware + cloud MSSP proposal, the bidder must clearly separate hardware payment milestones and service subscription payments in the financial proposal.

3 PREPARATION OF BID

3.1 Language of Bid

The Bid prepared by the Bidder, as well as all correspondence, documents relating to the Bid exchanged by the Bidder and HUTCHISON PORTS ABU QIR CONTAINERS TERMINALS S.A.E, supporting documents, and printed literature shall be written in English.

3.2 Documents Comprising the Bid

Each bid shall be in two parts: -

A. Part I- Technical Proposal.
B. Part II- Price Proposal.

The two parts should be in two separate covers, each super-scribed with the name of the Project as well as “Technical Proposal” and “Price Proposal” as the case may be.

Most provide the technical proposal in hardcopy and softcopy.

The Supplier cannot quote for the project in part.

3.2.1 PART I - TECHNICAL PROPOSAL.

The technical proposal should reflect the ability of service supplier and must include the following:

1- Company profile with previous implemented project.
2- The vendor must be partner of delivered device model and certified.
3- The delivered solution including OS and software must pass the vulnerability security scanner and hardening based on CIS standard.
4- A project plane must be provided for implementation.
5- Solution design and architecture to be deliver and approve by HUTCHISON PORTS ABU QIR CONTAINERS TERMINALS S.A.E before project start up.
6- Deliver project documentation samples from previous project to HUTCHISON PORTS ABU QIR CONTAINERS TERMINALS S.A.E as guidance before starting project implementation.
7- A project documentation must be delivered after project completed.
8- The project is a turnkey solution.
9- Delivery and acceptance criteria for each implemented point in the project will be reviewed by HUTCHISON PORTS ABU QIR CONTAINERS TERMINALS S.A.E before start implementation.

3.2.2 PART II - PRICE PROPOSAL.

1- Company Financial Documents
2- All prices should be itemized.
3- All prices are in USD or Egyptian pound.
4- For only suppliers located on Egypt Payment in EGP according to central bank charges in time of payment

5- Price excluding VAT and customs fees.
6- All items will be delivered by CIF
7- 2025 company's budget

3.3 Submission of Bids

1- **Sealing and Marking of Bids:** The Bidders shall seal the envelopes containing "Technical Bid" and "Price Bid" separately and the two envelopes shall be enclosed and sealed in an outer envelope. The Bidder should additionally submit soft copies of the Technical Specification in the form of CD.
2- **Deadline for Submission of Bids:** Bids must be received by HUTCHISON PORTS ABU QIR CONTAINERS TERMINALS S.A.E at the address specified, no later than the date and time specified in the Invitation to Bid.
3- HUTCHISON PORTS ABU QIR CONTAINERS TERMINALS S.A.E may, at its discretion, extend this deadline for the submission of Bids by amending the Bid Documents, in which case, all rights and obligations of HUTCHISON PORTS ABU QIR CONTAINERS TERMINALS S.A.E and bidders, previously subject to the deadline, will thereafter be subject to the deadline as extended.
4- **Clarification of Bids:** During evaluation of the Bids, HUTCHISON PORTS ABU QIR CONTAINERS TERMINALS S.A.E, at its discretion, may ask the bidder for clarification of its Bid. The request for clarification and the response shall be in writing, and no change in the prices or substance of the Bid shall be sought, offered, or permitted.

4 TERMS AND CONDITIONS

4.1 Assignment

The Supplier shall not assign, in whole or in part, its obligations to perform under the Contract, except with the HUTCHISON PORTS ABU QIR CONTAINERS TERMINALS S.A.E's prior written consent.

4.2 Bidders:

The qualified bidder for this tender and his sub contactors must be Partner in the scope of requested equipment.

4.3 Quantities

Material quantities as specified are approximate and no guarantee is implied that the exact amount will be purchased.

4.4 Response and Resolution

The response and resolution time is mentioned for each service project in scope section.

4.5 Prices:

a) The prices are deemed to include all costs, freight and other expenses (without customs, taxes) incurred by Supplier in delivering the goods to the location as specified by Hutchison Ports Abu Qir Containers Terminals S.A.E and performing his obligations under this Agreement.
b) The prices are fixed and shall not be subject to any variation. The supplier shall absorb the parts and labor of any missing components, if any, required to connect the items purchased by Hutchison Ports Abu Qir Containers Terminals S.A.E under this Agreement.

4.6 Risk, Loss or Damage

HUTCHISON PORTS ABU QIR CONTAINERS TERMINALSS.A.E, unless stated the otherwise, shall not be responsible for any risk, loss or damage caused by events beyond HUTCHISON PORTS ABU QIR CONTAINERS TERMINALSS.A.E's control, including but not limited to the goods which are in the course of delivery to HUTCHISON PORTS ABU QIR CONTAINERS TERMINALSS.A.E, whether by land, sea or air, that will include any governmental or customs regulations.

4.7 Delivery Time

The SUPPLIER shall deliver the goods to HUTCHISON PORTS ABU QIR CONTAINERS TERMINALS S.A.E in accordance with the project schedule. In the event that SUPPLIER fails to deliver the goods on time, HUTCHISON PORTS ABU QIR CONTAINERS TERMINALS S.A.E shall have the right to cancel the order and/or claim any other form of relief or damages from supplier.

4.8 Acceptance by HUTCHISON PORTS ABU QIR CONTAINERS TERMINALS

All deliveries of goods shall be subject to inspection and shall not be deemed to have been accepted until HUTCHISON PORTS ABU QIR CONTAINERS TERMINALS S.A.E furnished SUPPLIER with a formal acceptance notice. The signing of the Delivery Note by HUTCHISON PORTS ABU QIR CONTAINERS TERMINALS S.A.E is not deemed to be acceptance.

4.9 Warranty:

SUPPLIER warrants that goods delivered shall be free from defects in materials and workmanship. SUPPLIER undertakes to replace any defective parts and components and make good all defects in the goods swiftly and bears all costs including transport charges for replacing and repairing the defective goods.

4.10 Payment

Each Project will have its own Payment terms.

HUTCHISON PORTS ABU QIR CONTAINERS TERMINALS S.A.E shall assess a penalty on deliveries, which are not made in accordance with the project schedule; Penalty shall be in the amount of 1% percent of the section purchase price per week up to a maximum penalty of 10% of the purchase price.

4.11 Contract Terms and Conditions

HUTCHISON PORTS ABU QIR CONTAINERS TERMINALS S.A.E shall provide the supplier with all necessary documents to facilitate issuance of annual permanent gate permits for the supplier's technical support team and to be able to access sites at any time, in the event that the supplier was unable to issue a yearly permit.

The supplier has the responsibility of in/out transport of the spare parts needed inside the HUTCHISON PORTS ABU QIR CONTAINERS TERMINALS S.A.E locations as

HUTCHISON PORTS ABU QIR CONTAINERS TERMINALS S.A.E will help the supplier to get their custody book.

The supplier shall not alter, modify or change any configuration on any hardware/software without a written permission from HUTCHISON PORTS ABU QIR CONTAINERS TERMINALSS.A.E.

5 DISCLAIMER

The information contained in this Request for Quotation (RFQ) document or information provided subsequently to bidder(s) or applicants whether verbally or in documentary form by or on behalf of Hutchison Ports Abu Qir Containers Terminals S.A.E, is provided to the bidder(s) on the terms and conditions set out in this RFQ document and all other terms and conditions subject to which such information is provided.

This RFQ is neither an agreement nor an offer and is only an invitation by Hutchison Ports Abu Qir Containers Terminals S.A.E to the interested parties for submission of bids. The purpose of this RFQ is to provide the bidder(s) with information to assist the formulation of their proposals. This RFQ does not claim to contain all the information each bidder may require. Each bidder should conduct its own investigations and analysis and should check the accuracy, reliability and completeness of the information in this RFQ and where it is necessary to obtain independent advice. Hutchison Ports Abu Qir Containers Terminals S.A.E makes no representation or warranty and shall incur no liability under any law, statute, rules or regulations as to the accuracy, reliability or completeness of this RFQ. Hutchison Ports Abu Qir Containers Terminals S.A.E may in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information in this RFQ.