Request for Proposal (RFP)

To

Onboard Cyber Threat Intelligence (CTI) Services

RFP: IT-26-27-265
Date: 20th Nov 2026

This Document is the property of Multi Commodity Exchange of India Ltd (MCX). It may not be copied, distributed, or recorded on any medium, electronic, or otherwise, without MCX written permission. Use of contents given in this document, even by the authorized personnel/agencies for any other purpose other than the purpose specified herein, is strictly prohibited as it shall amount to copyright violation and thus shall be punishable under the Indian law

Internal

Introduction

MCX India Limited Background

Multi Commodity Exchange of India Limited (MCX), India's first listed Exchange, is a state of-the- art, commodity derivatives exchange that facilitates online trading of commodity derivatives transactions, thereby providing a platform for price discovery and risk management. The Exchange, which started operations in November 2003, operates under the regulatory framework of Securities and Exchange Board of India (SEBI).

Considering regulatory requirements in India (SEBI, CERT-In, NCIIPC etc.) and increasing innovative cyber risk threats, malwares and threats emanating from emerging technologies MCX have implemented Cyber Security technologies.

Objectives

The MCX seeks proposals from qualified and experienced service providers to onboard end-to-end **Cyber Threat Intelligence (CTI) Services** on a **continuous basis for a contract period** (extendable subject to satisfactory performance and internal approvals). The bidder shall ensure strict compliance with the Cybersecurity and Cyber Resilience Framework (CSCRF) and advisories/circulars issued from time to time by **SEBI**, **NCIIPC**, **CERT-In**, and other applicable statutory or regulatory authorities.

Sites to Cover

MCX office at Mumbai and DR site at Gift City, Gandhinagar, Gujarat.

Scope of Work

The engagement aims to onboard **Cyber Threat Intelligence (CTI) Services** on a continuous basis to proactively monitor the global, regional, and financial-sector threat landscape, map relevant threats directly to the Organisation's technology environment, and deliver clear, actionable intelligence outputs.

The selected bidder shall operate its own proprietary/commercial intelligence platforms, dark web monitoring tools, and threat feeds **entirely within the bidder's own environment**, deploying skilled analysts to deliver outcomes without requiring any vendor tool deployment or direct API/technical integration into the MCX security stack:

- **Monitor and identify emerging threats, active campaigns, and exploited vulnerabilities** across the external attack surface, dark web, deep web, and financial market ecosystem.
- **Contextualise and map daily findings directly to the MCX's specific asset inventory and technology stack** to eliminate noise and false positives.
- **Deliver curated, false-positive-vetted daily threat feeds** in standard, ready-to-use formats for the internal analysts to review and apply across internal controls.

Internal

- **Provide clear, prioritised actionable** (blocking recommendations, detection logic, patching priorities, and takedown support) alongside executive visibility via an **Executive Dashboard** and monthly reports.
- **Strengthen human-layer resilience** through periodic, threat-informed employee security awareness slides.

Focused Area

The scope of this engagement is to provide continuous CTI Services across MCX covering the following four core domains:

A. Daily Threat Monitoring, Environment Mapping & Curated Feed Delivery
B. Dark Web, Deep Web & External Attack Surface Surveillance
C. Financial Market, Vulnerability, Malware & Supply Chain Intelligence
D. Executive Visibility, Strategic Reporting & Employee Awareness

A. Daily Threat Monitoring, Environment Mapping & Curated Feed Delivery

1. **Environment-Mapped Daily Findings:** Continuously track global cyber campaigns, APTs, ransomware groups, and zero-day exploits, filtering and mapping findings specifically against MCX's technology stack, applications, and network footprint.
2. **Curated Daily Threat Feeds:** Collect, validate, score, and de-duplicate high-confidence Indicators of Compromise (malicious IPs, domains, URLs, and file hashes) delivered daily as standalone intelligence packages for MCX's internal SOC team to review and ingest into internal security controls.
3. **Clear Actionable Recommendations:** Accompany every finding with explicit, step-by-step mitigation instructions, recommended hunting queries, blocklists, and compensating controls.

B. Dark Web, Deep Web & External Attack Surface Surveillance

1. **Dark Web & Deep Web Monitoring:** Continuously monitor dark web forums, marketplaces, encrypted messaging channels, and ransomware leak sites for compromised organisational/employee/privileged credentials, leaked source code, confidential data, planned attack chatter, and third-party vendor exposure.
2. **External Attack Surface & Brand Protection:** Monitor internet-facing assets externally for exposed services, misconfigurations, spoofed domains, fraudulent mobile trading apps, and brand impersonation targeting employees, brokers, or investors, including end-to-end takedown assistance.

Internal

C. Financial Market, Vulnerability, Malware & Supply Chain Intelligence

1. **Stock Exchange & BFSI Sector Intelligence:** Maintain dedicated tracking of threats targeting trading platforms, clearing/settlement systems, broker interfaces, API gateways, market data feeds, and DDoS/availability disruption campaigns.
2. **Vulnerability & Zero-Day Exploitation Intelligence:** Track newly disclosed CVEs and zero-days actively exploited in the wild that impact MCX's infrastructure, providing risk-based prioritisation.
3. **Supply Chain & Third-Party Monitoring:** Monitor breaches, software supply chain compromises, and credential leaks involving critical technology vendors and service providers.

D. Executive Visibility, Strategic Reporting & Employee Awareness

1. **Executive Dashboard & Monthly Reporting:** Maintain and update an Executive Dashboard alongside delivering comprehensive monthly threat landscape and service performance reports.
2. **Employee Awareness Enablement:** Translate real-world phishing, social engineering, and credential-theft trends into concise, ready-to-use awareness slide decks for internal staff training.

Key Focused Area

The bidder's managed service team and off-premises monitoring tools shall maintain continuous external and dark-web intelligence coverage across MCX's critical ecosystem:

- Core Trading & Exchange Infrastructure: Trading platforms, clearing and settlement systems, and market data distribution channels.
- External & Participant Interfaces: Broker/trading-member portals, public websites, API gateways, and mobile applications.
- Data Centres: Public-facing footprints and technology stacks supporting on-premises data centres.
- Perimeter & Communication Channels: External exposure of firewalls, WAF, VPN/remote access gateways, DNS, and email domains.
- User & Privileged Identities: Employee accounts and privileged credentials exposed externally or on the dark web.
- Third-Party & Supply Chain Vendors: Critical technology partners, software vendors, and managed service providers.

Deliverables

The service provider shall utilize its own off-premises tools and deployed analysts to deliver the following **six (6) core mandatory deliverables** on schedule:

Internal

- **Monthly Threat Intelligence Report:** Comprehensive monthly analysis covering global and financial-sector threat trends, top targeted TTPs (mapped to MITRE ATT&CK), summary of dark web/brand findings, vulnerability exploitation trends, SLA compliance metrics, and strategic security recommendations.
- **Daily Findings & Environment Mapping Report:** Daily intelligence bulletin detailing newly identified threats, active campaigns, dark web exposures, and exploited CVEs—explicitly mapped to the MCX's asset inventory, software versions, and business relevance.
- **Executive Dashboard:** Interactive, executive dashboard providing real-time visibility into active threats, severity distribution, IOC trends, dark web alerts, vulnerability exposure, and action-item closure status via secure browser access.
- **Daily Validated Threat Feed:** Daily curated, false-positive-vetted IOC package (malicious IPs, domains, URLs, file hashes) delivered in structured, analyst-ready formats (CSV, JSON) for the analysts to review and apply to internal security controls.
- **Employee Awareness Slides:** Periodic (monthly/quarterly) ready-to-present awareness slide decks highlighting current phishing lures, social engineering tactics, credential hygiene, and financial-sector scam trends tailored for internal employees.
- **Clear Actionable (With Every Alert & Report):** Every finding, daily report, and critical alert must include specific, implementable remediation steps—such as recommended SIEM/XDR search logic, firewall/WAF blocklists, patching priorities, password reset triggers, or domain takedown actions—for execution by MCX's internal teams.
- **Minimum Mandatory Fields for All Intelligence Findings:**
    - Date of Discovery (First Seen & Last Seen)
    - Threat Category / Threat Actor / Campaign Name
    - MITRE ATT&CK Tactic & Technique Mapping
    - Mapped Organisational Asset / Technology Stack & Business Relevance
    - Severity Rating (Critical / High / Medium / Low) & Confidence Score
    - CVE ID, CVSS v3 Score, EPSS Score, and Active Exploitation Status (for vulnerabilities)
    - Validated IOCs & Supporting Evidence (e.g., dark web screenshots, domain registration details)
    - Clear Actionable & Compensating Controls
    - Current Status (Open / Actioned / Mitigated / Closed)

Methodology Requirements

- **Service Delivery & Resource Deployment Model:** Clear specification of the dedicated/shared analyst team structure (Threat Intelligence Analysts, Dark Web Specialists, Malware/Vulnerability Researchers, and Service Delivery Manager), escalation matrix, and analyst qualifications.

Internal

- **Off-Premises Tooling & Intelligence Sources:** Overview of the bidder's internal CTI platform, commercial/open-source intelligence feeds, dark web crawling infrastructure, and external attack surface discovery tools.
- **Environment Mapping & False-Positive Elimination Process:** Step-by-step methodology for ingesting MCX's asset/technology profile within the bidder's secure environment, correlating global threats against internal technologies, and validating IOCs before release.
- **Secure Deliverable & Dashboard Access Mechanism:** Procedures for securely transmitting the daily IOC feed and daily/monthly reports (e.g., encrypted portal, SFTP, or encrypted email) and securing browser access to the vendor-hosted Executive Dashboard (MFA, RBAC).
- **Data Handling, Segregation & Confidentiality:** Strict controls ensuring MCXw's shared asset inventory, watchlists, and intelligence findings are logically segregated from other clients inside the bidder's environment, encrypted at rest and in transit, handled solely by background-verified personnel, and compliant with Indian data localisation rules.

Regulatory and Industry Compliance

- SEBI CSCRF
- NCIIPC
- CERT-In Guidelines
- DPDPA
- NIST
- Latest ISO 27001
- MITRE Attack

Submission of Proposal

For submission process and any pre-bid query, please send the mail to **Mr. Prakash Komu – prakash.komu@mcxindia.com – 9920381998** with RFP name and number in the subject line.

Selection Weightage Criteria

Technical 70% - Commercial 30%
Threshold for Technical Selection – 55 out of 70

Errors and Omissions

Recipients are requested to promptly notify MCX of any errors, omissions, or discrepancies identified in this RFP document. This ensures that all parties have accurate and complete information for preparing their proposals.

Internal

Bidder's Profile

Consultancy firm meeting the eligibility criteria described in the following section will be considered for evaluation. MCX Group reserves the right to change or relax the eligibility criteria to ensure inclusiveness.

Sr. No	Requirements	Compliance (Yes/No)	Details
1.	The service provider may be a Private/ Public Limited Indian Company under Indian Laws. The Service Provider shall submit the Certificate of Incorporation along with the Technical Bid in respect of this requirement.		
2.	The service provider should be a minimum of 3 years old and have provided a similar type of services to Govt. / Public Sector Companies/corporates.		
3.	Bidder should be Cert-IN empanelled for the entire period of the engagement		
4.	Bidder should have past implementation experience of given activities in this RFP in scheduled BANKS / MIIs Exchanges.		
5.	Turnover of listed scheduled commercial bank under Top 50 list where bidder has implemented the		
6.	The service provider should have the domain knowledge in the areas of capital market, financial trading and exchange related businesses for at least the last 3 years.		
7.	The service provider should have required ISO & other certification.		
8.	The service provider should have an Income Tax PAN and should have submitted IT returns for the last 3 years.		

Internal

Sr. No	Requirements	Compliance (Yes/No)	Details
9.	The service provider should be registered with appropriate authorities under Employees Provident Fund and Employees State Insurance Acts or any other labor authorities including under the contract labor. Not applicable to BIDDERS based outside India.		
10.	The service provider should have registration under the shops & establishments act.		
11.	The service provider should furnish three references; the references should testify to the performance.		
12.	The service provider engaged with MCX / attending the MCX premise should comply with all the required statutory norms. Service Provider should adhere to all applicable laws, rules and regulations in carrying out the Services.		
13.	The service provider personnel visiting the MCX premises should be insured in all aspects by vendor.		
14.	The service provider should ensure that its personnel will adhere to the MCX code of conduct, processes and policies while at MCX's premises.		
15.	The service provider shall be responsible for compliance with all statutory provisions relating to minimum wages, Employees Provident Fund, Employees State Insurance, service tax and any other laws/ taxes/ acts/ rules etc. governing the matter/ issues etc.		
16.	The service provider shall also be liable for depositing all taxes, levies, cess etc. on account of the service rendered by it, to the concerned tax collection authorities from time to time as per extant rules and regulations on the matter. Not applicable to Bidders based outside India.		
17.	The service provider shall observe the highest standard of ethics during the MCX procurement process and Execution of the PO / service / support / contract		

Internal

Sr. No	Requirements	Compliance (Yes/No)	Details
18.	The service Provider should ensure jurisdiction must be in India and as per Indian Law.		
19.	The service provider must warrant that there are no legal actions being taken against it for any cause in any legal jurisdiction. If such an action exists and the Audit firm considers that it does not affect its ability to deliver the requirements stated in this RFP, an undertaking specifying the nature of the legal action and the reasons why this shall not affect the Audit firm's ability to deliver shall be provided.		
20.	The service provider should not have been blacklisted by SEBI, RBI, NCIIP or any other Government agencies. Audit firm must certify that effect.		
21.	The service provider must have a minimum of three (3 nos.) professionals who hold professional certifications like CISA/ DISA/ CISM/ CISSP assigned for this project with at least 8 years of experience each (other than project lead). Project lead should have Minimum 15 years of domain knowledge in the areas of capital market, financial trading and exchange related business.		
22.	The service provider must have experience of providing similar services. Minimum 3 similar projects in the areas of Cyber Security and Resilience with BFSI (preference if done in Stock Exchanges/ Clearing Corporation/ Leading Brokerage firms will be preferred.		
23.	Internal system and Cyber Audit, IT & Process Consultancy Services must either be a core activity of the firm or carried out by a regular departmental set up of the firm.		
24.	All the activities and services as per RFP to be performed on site and Consultant will not be provided remote access/ VPN.		
25.	Total No. of clients in India for the bidder for similar support services		

Internal

Sr. No	Requirements	Compliance (Yes/No)	Details
26.	Turnover and Net Profit of the company for last FY 2025-2026(Rs. In Crores)		
27.	Number of Certified Technical Employees (CEH, OSCP, CISA, ISO, CISM, CISSP etc.)		
28.	Key clients (past and present): (any three names with their contact's name & number)		
29.	Specific experience with any BFSI / MIIs		
30.	Turnaround time for onboarding the services		
31.	Approach and Methodology; The service Provider should have CERT-IN empanelled and ISO, SOC 2 and other industry certification.		
32.	Alignment with Scope: Adherence to regulatory requirements. Coverage of continuous 24x7 CTI monitoring, dark web/external surveillance, environment-mapped daily findings, daily feeds, Executive dashboard, monthly reports, awareness slides, and clear actionable.		

**Technical shortlisting of bidders will be based on the SOW & Bidders Profile.*

Technical Proposal

Bidders to share the company profile which should include the following parameters in pdf or pptx format.

1. Bidders company achievements.
2. Similar work experience in BFSI / MIIs, if any.
3. Specific experience with any BFSI / MIIs.
4. Turnaround time for onboarding the services.
5. Detailed Project Plan and other required activities as per Scope of Work.
6. Detailed Phase wise timelines for project completion.

Terms of Empanelment

The contract for the engagement will be for 1 years (extendable subject to satisfactory performance and internal approvals). Given the continuous nature of Cyber Threat Intelligence (CTI) operations, service delivery shall follow an ongoing operational cadence across the contract period as outlined below:

Internal

- Initial Onboarding & Dashboard Setup: Completion of asset/technology stack profiling, watchlist configuration, monitoring activation, and establishing of the Executive Dashboard upon contract signing.
- Threat Monitoring, Environment Mapping & Curated IOC Feeds: Ongoing surveillance throughout the contract period, including daily delivery of validated threat feeds, daily environment-mapped findings with clear actionable, and real-time notifications for critical threats.
- Monthly Threat Intelligence Report: Submission of the comprehensive Monthly Threat Intelligence Report, SLA compliance summary, and Executive Dashboard every month.
- Employee Awareness Slides & Executive Briefings: Delivery of tailored Employee Security Awareness Slide Decks and Financial-Sector / Threat Actor Landscape Briefings in each quarter.
- Service Sign-Off & Billing Alignment: Ongoing service delivery and SLA adherence shall be consolidated and reviewed on a Quarterly basis for formal sign-off.

Confidentiality

The RFP document is strictly confidential and is not to be disclosed, reproduced, published in any manner, transmitted, or otherwise made available by the Recipient to any other party. MCX may update or revise the RFP document or any part of it at its sole discretion. The Recipient acknowledges that any such revised or amended document received by it, shall be subject to the same terms and conditions as this original and subject to the same confidentiality undertaking. All Information pertaining to the Exchange obtained by the service provider because of participation in this RFP / project is confidential and must not be disclosed without prior written authorization from the Exchange.

The MCX reserves the right to amend or modify the contents of RFP at any time before date of bids submission. The decision of the Management Committee of MCX shall be final.

SLA & Penalties

SLA

(a) Project working days as per general working hours (0930 to 0630hrs) in a week till the completion of project.
(b) The Bidder to align qualified team member/s for the project.
(c) Project to start within 07 days post order confirmation.
(d) Monthly delivery of the reports, presentation with 100% coverage of scope as per regulatory requirements.

Internal

Penalty

(a) If there is a delay in the project kick-off, 0.25% of the PO cost will be imposed on per day.
(b) Non-adherence to the point (d) of SLA will attract penalty, 0.25% of the PO cost will be imposed on per day

Termination of Contract Clause

MCX may terminate the contract with 30 days written notice. However, immediate termination is applicable under the following conditions:

- Gross negligence or breach of contract.
- Repeated SLA violations (3 or more within a contract period).
- Repeated violation of confidentiality, client's data privacy, compliance, or security policies the assigned resource (2 or more within contract period)
- Breach of any material terms of the contract by the vendor.
- Failure to deliver services as agreed SLAs or performance standards.

Upon termination:

All documentation, access credentials, and tools must be handed over to client.

Commercial Format

Sr. No	Description	Charges in Rs. (INR)
1	The project/services fees will cover all aspects of scope of work as per the RFP for the overall project.	
Total Fee		
Taxes Extra		
Terms & Conditions		**Vendor Confirmation**
The Exchange would not make any payments in respect of any other charges/reimbursement of expenses like traveling, boarding & lodging, conveyance, etc and for any visits to Exchanges offices during the tenure of the project and the same should be included in the above-mentioned cost.		
Exchange will deduct the tax at source, if any, as per the prevailing laws.		
Bi-annually within 45 days post sign-off from MCX IS team. The signoff document should be submitted along with each invoice for the payments.		

Internal

Notification:

MCX Group may in its absolute discretion apply selection criteria specified in the document for evaluation of proposals for short listing / selecting the eligible Bidder. MCX Group is not obliged to provide any reasons for any such acceptance or rejection as evaluation process in entirely internal.

The Exchange reserves the right to amend or modify the contents of RFP at any time before the date of bids submission. The decision of the Management Committee of MCX Group shall be final Submission of proposal notifies deemed acceptance of terms as mentioned in this RFP by Bidder.

Confidentiality

The RFP document is strictly confidential and is not to be disclosed, reproduced, published in any manner, transmitted, or otherwise made available by the Recipient to any other party. MCX Group may update or revise the RFP document or any part of it at its sole discretion. The Recipient acknowledges that any such revised or amended document received by it shall

be subject to the same terms and conditions as this original and subject to the same confidentiality undertaking. All Information pertaining to the Exchange obtained by the Service Provider because of participation in this RFP / project is confidential and must not be disclosed without prior written authorization from the Exchange.

Termination Clause

If the services are not found to be satisfactory or if any non- compliance in services with respect to RFP delivery terms, MCX Group reserves the right to terminate the contract / Purchase Order (PO) giving notice to the bidder. The bidder should refund the payment made by MCX Group, if any.

Failure of point of this RFP MCX may terminate the agreement by giving 30 days' written notice, without assigning any reason.

Concentration Risk

Have you provided Similar services to other MII or Exchange, if yes provide the details?
Are you providing any service in MCX, if yes provide the order details (Purchase Order No)?

Internal

IT Act & Free from Malware/Backdoor Certificate (If applicable)

Information Technology Act Clause – Free of Malware/Backdoor/Harmful code

The Vendor understands and acknowledges that certain systems/computer resources/equipment/setups of MCX are identified as a Critical Information Infrastructure ("CII"). Therefore, All the Laws/ rules/ regulations and guidelines applicable to CII's and Protected Systems including the *"Information Technology Act, 2000"* and *"Information Security Practices and Procedures for Protected Systems",* set out in Gazette notification dated 22nd May 2018, shall be applicable to MCX.

The Vendor represents and warrants that: (1) the Vendor and/or its personnels shall always comply with the required laws, regulations and guidelines, applicable to the them, to ensure safety and security of MCX's CII's and Protected Systems; (2) the Vendor and/or its personnels shall not damage/harm MCX's systems/computer resources/equipment/setups; (3) the Vendor and/or its personnels shall not try to obtain unauthorized access to MCX's systems/computer resources/equipment/setups; (4) Vendor and/or its personnels shall not plant or place any harmful code, virus, self-propagating program, Trojan horse, trap door, backdoors or any other kind of harmful code or program in MCX's systems/computer resources/equipment/setups; (5) The Vendor and its personnel shall not leak and/or misuse the information stored and available on MCX's systems/computer resources/equipment/setups. Furthermore, the Vendor agrees to indemnify and keep indemnified, hold harmless and defend MCX against any/all loss, claims damage and penalty, that may be incurred by MCX, due to breach of Vendor's representations and warranties, as mentioned in this provision. In addition to the above the Vendor may also be liable for the punishment and/or penalty prescribed under the applicable laws (including of Information Technology Act, 2000).

Internal