Indian Institute of Technology Jodhpur
N.H. 62, Nagaur Road, Karwar, Jodhpur - 342030, Rajasthan (India)
☎ *0291-280 1252* | ✉ *office_cse@iitj.ac.in*
Website: Department: https://www.iitj.ac.in/computer-science-engineering |
IITJ: www.iitj.ac.in

INDIAN INSTITUTE OF TECHNOLOGY JODHPUR

Request For Technical Information and Pro Forma Quotations For

Procurement of Equipment and Software for Cyber Security Centre

1. Introduction

The Indian Institute of Technology Jodhpur (IIT Jodhpur) intends to procure **equipment and Software for the Cyber Security Centre** for academic and research purposes.

Before initiating the formal procurement process, the Institute invites **Technical Information And Indicative Pro Forma Quotations** from eligible Original Equipment Manufacturers (OEMs) or their authorized representatives.

2. Purpose

The objectives are to:

- Obtain technical information from prospective OEMs/authorized representatives.
- Obtain indicative Pro forma quotations for estimating the procurement cost.

3. Disclaimer

This document is issued **only for obtaining technical information and indicative Pro Forma quotations.**

Submission of information under this proposal:

- shall **not** be treated as a financial bid;
- shall **not** constitute any commitment on the part of IIT Jodhpur to procure the equipment;
- shall **not** confer any right upon the participating firm for award of any future contract;
- shall **not** automatically qualify the responding firm for participation in any future tender.

The Institute reserves the right to modify the technical specifications, estimated cost, procurement methodology, or procurement timeline based on its requirements.

4. Equipment Details

- Name of Equipment: **Equipment and Software for Cyber Security Centre**

- Quantity: As per the item-wise indicative schedule below.

Sr.	Component/Solution	Indicative Qty
1	Rack Servers	3
2	Storage	1
3	Cyber Security Tools	1
4	Penetration Testing Infrastructure (Phones, Laptops, Routers and Ipads with variety of OS, iOS, Linux, Android and CPUs -- Intel and AMD Processor)	15
5	Rack with PDUs	1
6	Firewall / IPS / Switches / WAP	1 unit
7	Other Security Tools	1 Unit
8	Honeypots	2

- Broad Functional Requirements (The essential functions or capabilities that the equipment should have, without mentioning a specific make, model, or brand):

1. Rack Server

Sr.	Parameter	Indicative Specification / Requirement
1	**Form Factor**	2U rack server.
2	**Processors**	Dual 48-core (3.15 GHz, 48C/96T, 256 MB cache) processors or higher, supporting DDR5 6000 MHz memory.
3	**SPEC CPU 2026 FP**	Quoted CPU model available on the 2026 SPEC CPU Floating-Point Rate rating.
4	**Memory**	24 x DIMM slots, persistent-memory capable, DDR5 6000 MHz; configured 384 GB DDR5.
5	**Disks**	Up to 10 x SFF hot-swap / NVMe bays; configured 2 x 1.92 TB SAS SSD on RAID 1.
6	**RAID Controller**	Embedded / PCIe x16 with 4 GB flash-backed write cache; RAID 0,1,5,6,10,50,60.

Sr.	Parameter	Indicative Specification / Requirement
7	**Network**	Dual-port 10/25G SFP+ and dual-port 1 GbE; dedicated OOB management port.
8	**System Management**	Agent-free OOB monitoring & alerting, firmware/driver management, power capping, zero-touch deployment, self-updating firmware repository, Redfish API and telemetry streaming from the same OEM.
9	**Security & Availability**	TPM 1.2/2.0; hot-swap/redundant drives, fans, PSUs; 45 °C continuous operation; diagnostic LEDs; front USB diagnostics.
10	**Regulatory**	Energy Star 2.1 or higher.
11	**Warranty**	3 years onsite warranty.

2. Storage

Sr.	Indicative Specification / Requirement
1	Scale-up and scale-out architecture for the asked SAN and NAS protocols, scaling to 8 or more controllers with mixing across controller generations.
2	Data-in-place controller upgrades to a higher generation with data intact on existing NVMe media.
3	Purpose-built single OS supporting block, file and Object (S3) protocols.
4	Symmetric/Asymmetric Active-Active block access; file shares accessible from all controllers; up to 20 PB single-namespace file share across 2+ controllers.
5	Minimum 2 controllers for failover; 2+ x 25/100 Gbps interconnect ports per controller.
6	Configured 10 TB usable on NVMe and 10 TB usable on NL-SAS after concurrent dual-drive-failure protection with 1 hot-spare per RAID group.
7	Support HDD and NVMe in the same storage; triple-parity protection option.
8	Minimum 64 GB DRAM cache per controller + 16 GB battery-backed NVRAM (8 GB/controller) mirrored; write protection on power loss.
9	Minimum 150k IOPS and 3 GBps throughput (70:30 R:W) on NVMe with data reduction; 4X performance scalability.
10	Minimum 8 x 10 Gbps and 8 x 32 Gbps ports across controllers; scalability of 400+ HDDs without adding controllers.
11	1000+ redirect-on-write snapshots per volume; hourly snapshot policy retained one month without host-IO impact.
12	Application-consistent protection (snapshots/thin clones) and replication; support for VMware, MS SQL, MongoDB, Oracle, MS Exchange, SAP HANA/MaxDB, PostgreSQL, DB2.
13	Native FC, NVMe-oF, NVMe/TCP, iSCSI, pNFS, NFS (v3/v4/v4.1), CIFS/SMB and Object (S3) protocols.

Sr.	Indicative Specification / Requirement
14	Inline and post-process deduplication & compression for block and file, retained during tiering/replication.
15	Autonomous ransomware & insider-threat detection within controllers; licenses from day 1; offline updates.
16	Synchronous & asynchronous replication licenses between 2 DCs for block and file; 64:1 fan-in and 1:4 fan-out replication.
17	SED-based data-at-rest encryption; WORM (SEC 17a-4) for file data; compliance with HIPAA, FINRA, CFTC, GDPR.
18	QoS to limit IOPS/throughput on LUNs and shares; Zero-Trust framework (RBAC, MFA, multi-admin validation, tamper-proof snapshots, encryption in-flight & at-rest).
19	Cold-data tiering to on-prem or public-cloud object storage preserving efficiencies and single namespace.
20	No-single-point-of-failure design with up to six-nines availability.
21	VMware (vVOLs, VAAI, SPBM) and OpenStack Cinder/Manila integration; OEM-supported Kubernetes CSI driver.
22	Storage virtualization with multi-tenancy and single logical volume across 4+ controllers.
23	5 years warranty with NBD part replacement and non-returnable drives.
24	Proof of Concept at the designated site for at least one week, if requested.
25	OOB management interface; centralized syslog; SNMP v2/v3 monitoring; India-based OEM TAC (min 9 Hrs x 5 Day/week).
26	Operating temperature 0–40 °C; humidity 10–90 % non-condensing; not End-of-Life for at least 5 years (OEM certificate).
27	OEM MAF, 'Non-Malicious Code' certificate, datasheet, Bill of Materials and proof of past supply; migration support from the incumbent storage; dual redundant PSUs with Indian-standard power cords.

3. Cyber Security Tools

SIEM / SOAR / UEBA / EDR — Indicative Specifications	
Area	Indicative Requirement
General & Commercial	Approx. 1000 EPS (SIEM) and 30 EDR endpoints; commercials for 3 years. SIEM, SOAR, UEBA, NBAD/NTA, AI, ML and EDR of a

	single OEM. OEM ≥ 10 years in the India market with R&D and support presence in India.
Architecture	Integrated, scalable, data-driven security platform; micro-service/container architecture, virtualization-ready; real-time stream processing & big-data engine. Deployable on bare metal, VM and cloud with multi-tenancy.
Big Fast Data Platform	Scalable stream processing, multi-petabyte storage, interactive query, real-time search and analytics, trend detection, advanced correlation and machine learning.
Machine Learning & Analytics	Behavioural analytics, real-time pattern and anomaly detection, confidence-based scoring, continuous learning, and minimal false positives.
Data Collection	Agent-less collection via syslog, Windows event logs, NetFlow/sFlow/IPFIX/J-Flow, REST API and cloud sources (AWS, Azure, GCP, Office 365); auto-parsing and normalization with custom-parser support.
Detection & Correlation	Real-time event correlation, identity-oriented monitoring, geolocation and threat scoring/prioritization; detection of known & zero-day threats, insider threats, DoS/brute-force, DGA, TOR/DNS tunnelling and C&C traffic.
Response & Remediation	Automated real-time remediation with endpoint isolation, credential/VPN disabling and policy push; integration with firewalls, NAC and EDR for containment and quarantine.
Alerting & Reporting	Email/text alerts and dashboards; on-demand and scheduled reports; compliance reporting (HIPAA, PCI-DSS, NIST); export to CSV/TSV/PDF.
Integration	REST/SOAP API; integration with leading firewalls (Cisco, Palo Alto, Check Point, etc.), DNS/DHCP/proxy, NAC, EDR, SD-WAN, cloud providers, ticketing (JIRA) and vulnerability tools.
Scalability & Availability	Clustering and distributed architecture, High Availability and Disaster Recovery, data archival/restore, encryption at rest and in transit, RBAC and multi-tenancy.
Endpoint Detection & Response	Lightweight EDR agents for Windows, Linux and macOS providing process/file visibility, malware-footprint detection and endpoint isolation/containment.
Hardware & Deployment	Appliance-based or secured server-based deployment with RAID redundancy, 10G/1G interfaces, role-based access and rapid deployment.

4. Penetration Testing Infrastructure (Phones, Laptops, Routers and Ipads with variety of OS, iOS, Linux, Android and CPUs -- Intel and AMD Processor)

a. Standard Laptop (Indicative Qty: 05)

Sr.	Parameter	Indicative Specification / Requirement
1	**OS**	Windows 11 Pro.
2	**Processor**	Intel Core Ultra 7 155H class (up to 4.8 GHz, 6P+8E, 16 threads) or higher.
3	**Memory**	16 GB DDR5-5600 or higher.
4	**Storage**	512 GB PCIe NVMe SSD or higher.
5	**Display**	14" WUXGA (1920x1200) IPS, 300 nits, anti-glare or higher.
6	**Camera / Audio**	5 MP IR camera (Windows Hello); studio-certified dual speakers & mics.
7	**Ports / Wireless**	2 x Thunderbolt 4, 2 x USB-A, HDMI 2.1; Wi-Fi 6E, BT 5.3, optional 5G/LTE.
8	**Build / Battery**	MIL-STD-810H aluminium chassis; fast charge (50 % in ≤30 min).
9	**Security**	Enterprise BIOS protection, threat isolation, on-chip NPU.

b. Smart Node Handset — Type A (Indicative Qty: 02)

Sr.	Parameter	Indicative Specification / Requirement
1	**RAM & ROM**	8 GB RAM / 128 GB storage, microSD expandable.
2	**OS & Updates**	Android 15 or higher; 6 OS upgrades, 6 years security updates.
3	**Display**	6.7" FHD+ Super AMOLED, 120 Hz.
4	**Build**	Toughened glass, IP67 dust/water resistant.
5	**Cameras**	Triple rear (50 MP OIS + 8 MP UW + 2 MP macro); 13 MP front; 4K@30fps.
6	**Battery / Conn.**	5000 mAh, 25 W charging; 5G/LTE, Wi-Fi ac, BT 5.3, GPS.

c. Smart Node Handset — Type B (Indicative Qty: 02)

Sr.	Parameter	Indicative Specification / Requirement
1	**Display**	6.3" OLED, 1080x2424, 120 Hz.
2	**Processor / RAM**	Flagship-class SoC (Tensor-G4 class or equivalent); 8 GB LPDDR5X.
3	**Storage**	128 GB or higher.
4	**Cameras**	48 MP + 13 MP ultrawide rear; 13 MP front.
5	**Battery / Charging**	5100 mAh; 30 W wired, 10 W wireless.

Sr.	Parameter	Indicative Specification / Requirement
6	**OS / Conn.**	Android 16; 5G, Wi-Fi, BT, NFC; IP68.

d. Tablet (Indicative Qty: 02)

Sr.	Parameter	Indicative Specification / Requirement
1	**RAM & ROM**	12 GB RAM, 256 GB storage, microSD up to 1 TB.
2	**Display**	12.4" WQXGA (2560x1600) TFT, 90 Hz, low-blue-light.
3	**Processor**	Octa-core (Cortex-A78 + A55 class).
4	**Cameras**	Dual 8 MP rear (main + UW), 12 MP front, 4K@30fps.
5	**Battery / Conn.**	10,090 mAh, 15 W charging; 5G/LTE, Wi-Fi 6, BT 5.3, GPS, USB-C.
6	**Build / Pen**	IP68 (tablet + pen), metal frame; included stylus.
7	**OS & Updates**	Android 13/14/15 or higher; minimum 5 years security & OS updates.

e. Smartphone (iOS)

Smartphone (iOS)	
Parameter	**Specification**
Chip / Processor	A19 — 6-core CPU (2 performance + 4 efficiency), 5-core GPU, 16-core Neural Engine.
Operating System	iOS 26 or Higher.
Display	6.3-inch Super Retina XDR OLED, ProMotion adaptive 1–120 Hz, Ceramic Shield 2 front glass.
Memory & Storage	8 GB RAM; 256 GB or 512 GB internal storage.
Cameras	48 MP dual Fusion rear (main + ultra-wide); 18 MP Center Stage front; 4K video up to 60 fps.
Connectivity	5G, Wi-Fi 7, Bluetooth 6, N1 networking chip, USB-C, eSIM.
Battery & Charging	Up to ~30 hrs video playback; up to 40 W wired fast charge; MagSafe / Qi2 wireless.
Durability	IP68 dust/water resistance.

f. Tablet (iOS)

Tablet (iOS)	
Parameter	**Specification**

Chip / Processor	M5 — up to 10-core CPU, 10-core GPU with hardware ray tracing, 16-core Neural Engine.
Operating System	iPadOS 26.
Display	Tandem OLED Ultra Retina XDR, ProMotion adaptive 10–120 Hz.
Memory & Storage	12 GB RAM (16 GB on 1 TB/2 TB); 256 GB to 2 TB storage.
Connectivity	Wi-Fi 7, Bluetooth 6, N1 chip, Thunderbolt / USB 4; optional 5G (C1X modem).
Accessories	Pencil and Magic Keyboard compatible.
Battery & Charging	Up to ~10 hrs use; 40 W fast charge .

g. Desktop

Desktop	
Parameter	**Specification**
Processor	Intel Core Ultra 7 (current generation, e.g. Core Ultra 7 265K / 270K-class, 20–24 cores) or higher. AMD Ryzen 7 equivalent acceptable per the mixed-CPU requirement.
Motherboard / Chipset	Intel 800-series chipset (e.g. B860 / Z890), LGA 1851 socket; PCIe 5.0 support.
Memory	Minimum 32 GB DDR5 (expandable), up to 7200 MHz.
Storage	1 TB NVMe PCIe 4.0/5.0 SSD.
Graphics	Integrated Intel Arc graphics with optional discrete GPU (≥ 8 GB) for security/analysis workloads.
Connectivity	2.5 GbE LAN, Wi-Fi 7, Bluetooth 5.4+, USB-C / USB 3.2, HDMI/DisplayPort.
Operating System	Windows 11 Pro (64-bit); Linux-compatible for penetration-testing use.
Peripherals & Form Factor	27-inch FHD/QHD monitor, keyboard and mouse; tower / small-form-factor chassis with adequate PSU.

h. Router

Router	
Parameter	**Specification**
Software / OS	Full traditional routing stack, SD-WAN / SD-Routing capable, programmable (NETCONF/RESTCONF/YANG, APIs).

Unicast Routing	Static routing, RIPv2, OSPFv2 & OSPFv3, EIGRP, IS-IS, BGP-4 & MP-BGP, Policy-Based Routing (PBR); full IPv4 and IPv6 dual-stack.
VRF / MPLS / Overlay	VRF and VRF-Lite, MPLS, MPLS L3VPN, GRE, DMVPN, FlexVPN, IPsec VPN and SD-WAN overlays.
Multicast	IGMP v1/v2/v3, PIM Sparse/Dense/SSM, MSDP and multicast VPN.
L2 & Redundancy	Integrated Layer-2 switching modules, 802.1Q VLAN, STP; first-hop redundancy via HSRP, VRRP and GLBP.
QoS	Hierarchical QoS, class-based weighted fair queuing, policing, shaping and DSCP/ToS marking.
Security	Zone-based / Next-Gen Firewall, Snort IPS/IDS, URL filtering, ACLs, MACsec, Control-Plane Policing, AAA (RADIUS/TACACS+).
Interfaces	4 × 1 GE (RJ45) WAN ports, 1 NIM slot and 1 PIM slot (optional 5G/LTE), RJ-45/USB console, dedicated management port.
Performance	8-core CPU, up to 32 GB DRAM; up to ~3.8 Gbps IPv4 forwarding and up to 1 Gbps IPsec / SD-WAN throughput.
Management & Telemetry	CLI, SSH, SNMP v2c/v3, Syslog, Flexible NetFlow,WebUI /Application for Management, zero-touch provisioning.

5. Rack with PDUs

42U Rack with PDUs

6. Network Devices

Firewall / IPS / Switches / WAP.

a. Managed L3 Access Switch – 24 Ports

Managed L3 Access Switch – 24 Ports	
Parameter	Specification
Ports & Form Factor	24 × GE RJ45 + 4 × GE SFP ports; RJ-45 serial console and dedicated management port; 1 RU rack-mount; redundant power supply from day 1.
Performance	Switching capacity ≥ 55 Gbps; ≥ 80 Mpps; ≥ 16K MAC addresses; 4000 VLANs.

L2/L3 Functionality	MSTP (native) / RSTP / STP with BPDU Guard, Edge Port/Port Fast, 802.1AX LAG, 802.1q VLAN, LLDP/LLDP-MED, DHCP snooping, jumbo frames.
Authentication	802.1x port-/MAC-based auth and MAB, guest & dynamic VLAN; local user database with RADIUS (RFC 2865), TACACS+ and LDAP integration.
Management	Telnet, SSH, HTTP, HTTPS (IPv4/IPv6); SNMP v1/v2c/v3; GUI + CLI; port-level visibility and host/user quarantine.
Environment & Certifications	100–240 V AC, 50–60 Hz; 0–50 °C; 10–90 % non-condensing. FCC, CE, BSMI, UL, CB, RoHS2, RCM, VCCI.

b. Managed L2 Access Switch – 24-Port PoE

Managed L2 Access Switch – 24-Port PoE	
Parameter	Specification
Ports & Form Factor	24 × GE RJ45 + 4 × GE SFP ports; RJ-45 serial console; 1 RU rack-mount; PoE power budget of 185 W.
Performance	Switching capacity ≥ 55 Gbps; ≥ 80 Mpps; ≥ 8K MAC addresses; 4000 VLANs.
Functionality	MSTP (native)/RSTP/STP with BPDU Guard, Edge Port/Port Fast, 802.1AX LAG, MCLAG, 802.1q VLAN (MAC/IP/Ethertype), 802.1p & DSCP QoS, jumbo frames.
Authentication	Admin authentication via RFC 2865 RADIUS.
Management	Telnet, SSH, HTTP, HTTPS (IPv4/IPv6); SNMP v1/v2c/v3; GUI + CLI; port-level visibility and host/user quarantine.
Environment & Certifications	100–240 V AC, 50–60 Hz; 0–45 °C; 10–90 % non-condensing. FCC, CE, BSMI, UL, CB, RoHS2, RCM, VCCI.

c. Firewall -1

S. No.	Technical Specification
1	Next Generation Firewall (NGFW) with IPS, Anti-Malware, Anti-Bot, DoS/DDoS Protection, URL Filtering, Application Control, and SSL/TLS Inspection.

2	Minimum NGFW throughput: 2 Gbps; Threat Prevention throughput: 1.5 Gbps.
3	Minimum IPsec VPN throughput: 8 Gbps; SSL/TLS inspection throughput: 500 Mbps.
4	Support at least 3.5 million concurrent sessions and 150,000 new sessions/sec.
5	Minimum 8 × 1GbE and 4 × 10GbE SFP+ interfaces with required optical transceivers.
6	Web GUI with centralized management, remote packet capture, and High Availability support.
7	Support minimum 5 Virtual Firewalls (VDOMs/Contexts) from Day-1.
8	Support REST API (JSON/XML) for automation and integration.
9	Role-Based Access Control (RBAC) with SAML/OpenID authentication.
10	Generate reports in PDF/HTML and export logs in CSV.
11	Support High Availability (Active/Standby) with state synchronization.
12	Support IPv4/IPv6, Static Routing, OSPF, BGP, PBR, NAT44/NAT64/NAT66, and PAT.
13	Support TLS 1.3 inspection and certificate validation.
14	Application awareness for 7,000+ applications with QUIC/HTTP3 support.
15	Support endpoint posture validation and policy enforcement.
16	Support multi-ISP load balancing, VPN failover, QoS, and link aggregation.
17	Support Site-to-Site and Remote Access VPN.
18	Support file filtering, antivirus, IPS, anti-evasion, and threat intelligence.

19	Support URL filtering, IP reputation, Geo-IP filtering, Anti-Spoofing, and application-based policies.
20	OEM should provide 3 Years subscription (IPS, AV, URL Filtering, Threat Protection, Support & Firmware Updates).

d. **Firewall-2**

Purpose	Next-generation firewall platform for laboratory perimeter protection and for teaching secure network architecture, segmentation and policy design
Form factor	Compact desktop or 1RU rack-mountable appliance, purpose-built security appliance (not a general-purpose server)
Firewall throughput	Minimum 9 Gbps stateful firewall throughput (1024B/1500B mixed traffic)
Concurrent sessions	Minimum 300,000 concurrent connections
Interfaces	Minimum 8 x 1 GbE copper ports and 2 x 10 GbE SFP+ uplink ports, plus dedicated management and console ports
Threat prevention	Integrated next-generation IPS (Snort 3 or equivalent), file/malware inspection with sandboxing, and reputation-based URL filtering
Application control	Application visibility and control with identity-based policy (AD/LDAP integration)
Encrypted traffic	TLS decryption/inspection and encrypted-traffic analytics without full decryption
VPN	Site-to-site IPsec VPN and remote-access VPN (SSL/IPsec) with MFA integration
Segmentation	Minimum 10 virtual routing instances / VRFs for multi-tenant lab segmentation
Routing & SD-WAN	Static, OSPF, BGP routing; integrated SD-WAN capability
High availability	Active/standby failover support

Management	On-box device manager, centralised management centre (physical or virtual), and cloud-based management option; REST API for automation
Logging & integration	Syslog/NetFlow export to external SIEM; integration with vendor XDR platform and global threat-intelligence feed
Platform integrity	Hardware trust anchor module with secure boot and image signing
Software licence	3-year Threat, Malware and URL filtering subscription bundle
Support	3-year OEM support with next-business-day hardware replacement and 24x7 TAC access

7. Other Security Tools

Security Testing Tools

Purpose	Manual and automated web application security testing, and hands-on teaching of web attack and defence techniques
Licence type	Named-user desktop licence; one seat per concurrent user
Automated scanner	Full automated crawler and vulnerability scanner covering 100+ vulnerability classes including the complete OWASP Top 10
Intercepting proxy	Real-time interception, inspection and modification of HTTP/HTTPS traffic with CA certificate installation
Manual tools	Repeater, Intruder (unthrottled, with Sniper, Battering Ram, Pitchfork and Cluster Bomb attack types), Sequencer, Comparer, Decoder
Out-of-band testing	Collaborator server for detection of blind/out-of-band vulnerabilities (SSRF, blind XXE, blind SQLi), with private Collaborator option
AI assistance	AI-assisted analysis features included in the Professional edition at no additional charge
Project persistence	Save, resume, search and annotate full project state across sessions

Reporting	Exportable HTML and XML vulnerability reports with severity, confidence and remediation guidance
Extensibility	BApp Store extension marketplace and documented extension API (Montoya API) for Java/Python/Ruby extensions
Scope control	Fine-grained target scope, session handling rules and macro support for authenticated scanning
Platform	Windows, Linux and macOS; bundled Java runtime
Licence term	3 Years

API Testing Tools

Purpose	API design, functional testing, security validation and governance; teaching of API security testing workflows
Protocol support	REST, SOAP, GraphQL, gRPC, WebSocket and raw HTTP
Specification support	Import/export of OpenAPI 3.x, Swagger 2.0, RAML and GraphQL SDL definitions
Test automation	JavaScript-based pre-request and test scripts; collection runner with data-driven runs from CSV/JSON
CLI & CI/CD	Command-line collection runner (Newman or equivalent) with JUnit/HTML reporting and native CI/CD pipeline integration
Security testing	Automated API security checks against OWASP API Security Top 10 categories, including broken authentication, excessive data exposure and rate-limiting checks
Governance	Configurable API governance and security rule sets applied automatically to API definitions, with organisation-wide rule enforcement
Authentication	Built-in support for OAuth 2.0, OAuth 1.0a, API key, Bearer token, JWT, AWS Signature, NTLM, Digest and Hawk authentication
Mocking & monitoring	Mock servers and scheduled monitors for availability and contract testing

Access control	SAML/SSO integration, SCIM user provisioning, role-based access control and workspace-level permissions
Audit & compliance	Organisation-wide audit logs of user and API activity
Platform	Windows, Linux and macOS desktop clients plus browser access
Licence term	3 Years

8. Honeypot - Qty2

Supply, install and commission one (1) enterprise deception platform with central console and distributed sensors, licensed for minimum 250 decoy IPs across 32 VLANs plus unlimited endpoint breadcrumbs, on a 3-year subscription. Shall provide full-OS and emulated service decoys covering enterprise IT, OT/ICS (Modbus, S7COMM, DNP3, IEC-104, BACnet, EtherNet/IP) and IoT devices, plus agentless Active Directory identity deception and credential/file lures. Shall integrate natively with Cisco ISE over pxGrid for automated Rapid Threat Containment and with Cisco Secure Firewall via API, with syslog/CEF and REST API fallback to any SIEM; bidder to state for each whether it is a product feature or custom script. Shall operate air-gapped, support role-based multi-tenant access for student batches, permit user-authored custom decoy templates, and export all event and packet data in open formats (JSON, PCAP, CEF). Includes Windows decoy licences (or separately quoted), 3 years 24x7 OEM support with India presence, and 2 days on-site training. Bidder to submit OEM datasheets and Cisco alliance-partner evidence, and to demonstrate live automated containment through the Cisco stack during technical evaluation. Equivalent products meeting all parameters of the attached Technical Specification sheet are eligible.

(The above requirements are indicative and may be revised after evaluation of the responses.)

5. Eligibility Criteria
Interested firms should:

- Be an Original Equipment Manufacturer (OEM) or an authorized distributor/dealer.

- Have experience in supplying similar equipment.
- Have adequate installation and after-sales service support in India.

6. Information/Documents to be Submitted

The interested firms shall submit the following (*Annexure-I*):

1. Company Profile.
2. Details of the OEM.
3. Product Brochure/Catalogue.
4. Detailed Technical Specifications.
5. Compliance with the Broad Functional Requirements.
6. List of previous users/clients with installation reports
7. Details of Warranty.
8. Details of After-Sales Service Support.
9. Authorization Letter from OEM (where applicable).
10. Any additional technical information relevant to the offered equipment.

7. Pro forma Quotation

- Interested firms are requested to submit a Pro forma Quotation (*Annexure-II*) along with their Request For Technical Information and Pro Forma Quotations response. Indicative **Pro Forma** quotation in Indian Rupees (INR), including the cost of the equipment, essential accessories, taxes, duties, freight, insurance, installation, commissioning, training, and any other associated charges. Wherever applicable, the Annual Maintenance Contract (AMC) and/or Comprehensive Maintenance Contract (CMC) charges and spare parts shall be quoted separately as additional charges.
- Expected delivery schedule and other relevant technical and commercial information.

Important Note:

- The **Pro Forma** quotation is required only for cost estimation and budget planning purposes.
- The prices quoted shall be indicative/non-binding.
- The Pro Forma quotation shall not be treated as a financial bid.
- Submission of a **Pro Forma** quotation shall not confer any right or preference in the subsequent procurement process.

8. Presentation/Demonstration

The Institute may invite for a technical presentation or product demonstration. The date and venue shall be communicated separately.

9. Submission :

Interested firms may submit their Proforma Quotations on or before the due date in sealed cover or through email (as applicable).

The envelope/email should be superscribed as:
"Request For Technical Information and Pro forma Quotations for Procurement of Equipment and Software for Cyber Security Centre"

8. Important Dates

Activity	Date
Publication	13-08-2026
Last Date for Submission	28-08-2026
Technical Presentation (if required)	To be informed
Clarification Meeting (if required)	To be informed

10. General Terms & Conditions

1. This **Request For Technical Information and Pro forma Quotations** is issued only for obtaining technical information and **Pro Forma** estimates.
2. The Institute reserves the right to accept or reject any or all responses without assigning any reason.
3. Submission of a Request **For Technical Information and Pro forma Quotations** does not create any contractual obligation.
4. The Institute may seek additional information, technical clarifications, demonstrations, or presentations from any participant.
5. The Institute may modify the technical requirements based on the responses received.
6. The final technical specifications may be prepared by the User Committee after evaluating all **Request For Technical Information and Pro forma Quotations** responses.
7. The subsequent procurement, if any, shall be carried out through an appropriate procurement method in accordance with the GFR 2017 and applicable procurement rules.
8. Participation in this **Request For Technical Information and Pro forma Quotations** does not automatically entitle any firm to participate in or receive any preference during the subsequent tender process.

11. Contact Details
Name: Dr. Susil Kumar Mohanty
Designation: Assistant Professor
Department: CSE
Email: susilmohanty@iitj.ac.in

Indian Institute of Technology Jodhpur
N.H. 62, Nagaur Road, Karwar, Jodhpur - 342030, Rajasthan (India)
☎ *0291-280 1252* | ✉ *office_cse@iitj.ac.in*
Website: Department: https://www.iitj.ac.in/computer-science-engineering |
IITJ: www.iitj.ac.in

Annexure-I

Request For Technical Information and Pro forma Quotations Response Format

1. Name of the Firm:
2. Registered Address:
3. Name of OEM (if applicable):
4. Contact Person:
5. Email:
6. Phone:
7. Product Name and Model:
8. Brief Technical Description:
9. Compliance with Broad Functional Requirements:
10. List of previous users/clients with installation reports:
11. After-Sales Service Details:
12. Any Additional Features:
13. Remarks (if any).

Indian Institute of Technology Jodhpur
N.H. 62, Nagaur Road, Karwar, Jodhpur - 342030, Rajasthan (India)
☎ 0291-280 1252 | ✉ office_cse@iitj.ac.in
Website: Department: https://www.iitj.ac.in/computer-science-engineering |
IITJ: www.iitj.ac.in

Annexure-II

Format for Pro Forma Quotation

Indicative Pro Forma quotation in Indian Rupees (INR), including the cost of the equipment, essential accessories, taxes, duties, freight, insurance, installation, commissioning, training and any other associated charges.

Sl. No.	Description	Qty	Amount (INR)
1	Rack Servers	3	
2	Storage	1	
3	Cyber Security Tools	1	
4	Penetration Testing Infrastructure (Phones, Laptops, Routers and Ipads with variety of OS, iOS, Linux, Android and CPUs -- Intel and AMD Processor)	15	
5	Rack with PDUs	1	
6	Firewall / IPS / Switches / WAP	1 unit	
7	Other Security Tools	1 Unit	
8	Honeypots	2	
9	Essential accessories (if any)		
10	Taxes & duties (GST etc.)		
11	Freight & insurance		
12	Installation, commissioning & training		
13	Any other associated charges		
14	**Grand Total (Indicative)**		

Warranty Period: _____

AMC / CMC Charges (after warranty): _____

Delivery Period: _____

Authorized Signatory

Name: _____

Designation: _____

Company Seal & Signature