# Corrigendum-III
# For
# Request for Proposal (RFP) for Selection of Agency for Supply, Installation & Commissioning of Enterprise Security Solution for Cyber Security Operation Centre (CSOC) Government of Odisha

**RFP No- OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024**

**Corrigendum-III**

## Revised RFP Schedule

| Sl. No. | Items | Date & Time |
|---|---|---|
| **1.** | Last date and time for Submission of Bid through www.enivida.odisha.gov.in | 03-May-2024 by 02:00 PM |
| **2.** | Opening of Pre-Qualification (PQ) – cum- Technical Bid for Package - I | 03-May-2024 at 04:00 PM |
| **3.** | Opening of Pre-Qualification (PQ) Bid for Package-II | 03-May-2024 at 04:00 PM |
| **4.** | Opening of Technical Qualification (TQ)Bid for Package -II | To be Intimated Later |
| **5.** | Date of Technical Presentation for Package - II | To be Intimated Later |
| **6.** | Opening of Commercial Bids for Package – I & Package - II | To be Intimated Later |

## 4.1.Pre-Qualification (PQ) / Eligibility Criteria

| Sl. No. | Basic Requirement | Specific Requirements | Documents Required |
|---|---|---|---|
| 2 | Average Sales Turnover | Annual average Turnover during any three financial years out of the last five financial years ending March – 2023 (as per the last published Balance sheets), should be as follows:<br>a. **Package – I** - Minimum of **Rs. 10 Crores generated from IT Hardware supply and associated maintenance services.**<br>b. **Package – II** - Minimum of **Rs. 10 Crores generated from the Supply of Security Software Solutions.** | Extracts from the audited Balance sheet and Profit & Loss;<br>OR<br>Certificate from the statutory auditor |
| 4 | OEM Experience | The OEM should have implemented at least 5 heterogeneous setups (means BFSI, Government /PSU/Autonomous body). | Documents Required: Customer PO copies, completion certificate (for completed project) and any feedback from the client(Not Mandatory). |
| 6 | Quality Certifications | Bidder/ OEM should have ISO 9001:2015, ISO 27001:2013 / ISO 27001:2022 Certifications | Copy of valid certificate |

**Note:- Other Terms & Conditions mentioned in Pre-Qualification(PQ)/Eligibility Criteria (4.1) remain same as per RFP**

## 21.5.1.1.Specification for Firewall

| S.No. | Technical Specification | Compliance (Yes/No) | Offered Parameter |
|---|---|---|---|
| | **Make :-** | | |
| | **Model :-** | | |
| **1** | **Hardware Specification** | | |
| 1.1 | Device Should be 1RU; 19 Inch Rack-mountable | | |
| 1.2 | The appliance should have multicore processor-based architecture. | | |
| 1.3 | The appliance should have minimum 8 x 10/100/1000 Base T Ethernet Port | | |
| 1.4 | The appliance should have minimum 8 Ports of 1Gbps SFP | | |
| 1.5 | The appliance should have minimum 4 Ports of 10Gbps SFP+ | | |
| 1.6 | The appliance should have minimum 1 x Expandable Slots support with optional 8 x SFP/Copper or 4 x SFP+ Port for future requirement | | |
| 1.7 | The appliance should have minimum 1 x Management port | | |
| 1.8 | The appliance should have minimum internal storage of 1TB SSD for Logs & Reports or better. | | |
| 1.9 | The appliance Should have minimum 16GB DDR4 Memory or better | | |
| 1.1 | The appliance should have Dual Redundant internal Power Supply from Day1 | | |
| 1.11 | The appliance should have Hot Swappable Power Supply | | |
| 1.12 | The proposed solution should have a bandwidth quota and time quota for the manageability of users | | |
| 1.13 | The Firewall should be Network DLP compliant for future upgradation | | |
| **2** | **License Deliverable /Description** | | |
| 2.1 | Need 5 Years / 60 Month H/W Warranty with stateful inspection and firewall policies to control access of ports and hosts or network. | | |

| S.No. | Technical Specification | Compliance (Yes/No) | Offered Parameter |
|---|---|---|---|
| 2.2 | The firewall should have provision for future upgradation of Next generation firewall license which include Next Generation Intrusion Prevention System (IPS), Zero Day Protection / Advance Malware protection, Web Security Essentials / URL Filtering ; Antivirus, URL Filter, Application Filtering, Anti-Spam, user identity, and Basic 24x7 Support | | |
| 3 | **Performance Capacity –Minimum** | | |
| 3.1 | The appliance should have minimum Firewall Throughput of 70 Gbps or better | | |
| 3.2 | The appliance should be able to handle minimum 500K new session per second or better | | |
| 3.3 | The appliance should be able to handle minimum 10 Gbps NGFW Throughput or better | | |
| 3.4 | The appliance should have minimum Antivirus Throughput of 04 Gbps or better | | |
| 3.5 | The appliance should have minimum IPS Throughput of 12 Gbps or better | | |
| 3.6 | The appliance should have minimum Firewall IMIX Throughput of 28 Gbps or better | | |
| 3.7 | The appliance should have minimum VPN Throughput of 13 Gbps or better | | |
| 3.8 | The appliance should have minimum 2000 Number of IPSec VPN Peers supported (Site to Site) | | |
| 3.9 | The appliance should have minimum 2000 Number of IPSec VPN Peers supported (Client to Site) | | |
| 3.1 | The appliance should have minimum 10000 Number of SSL VPN Peers supported (Client to Site) | | |
| 3.11 | The appliance should have minimum 20M Concurrent Session/Concurrent Connection | | |
| 3.12 | The appliance Should support 85+ Web categories for future upgradation of URL filter license | | |

| S.No. | Technical Specification | Compliance (Yes/No) | Offered Parameter |
|---|---|---|---|
| 3.13 | The appliance Should support 5000+ application Signature for future upgradation of APP filter license | | |
| 3.14 | The appliance Should support 25000+ IPS Signature for future upgradation of Next generation IPS license | | |
| 3.15 | The proposed system should have the future option to integrate with cloud-based management system to manage Firewall. Both solutions should be from the same OEM. | | |
| 3.16 | The Proposed solution should have a future flexibility / option to provide complete policy enforcement and visibility of roaming users and should restrict the remote user from disabling it. | | |
| 3.17 | The Proposed solution should have a future flexibility to apply organization policy framework to the remote users and ideally, it should control the Web and Application filter of the remote user | | |
| **Other Terms & Conditions** | | | |
| 1 | Supply, Installation, Integration, testing commissioning and training as per site requirements shall be done by the bidder. | | |
| 2 | The proposed appliance should come from firewall appliance family which has more than 5 years of ICSA labs certification/NSS/NDP/ Indian Standard, IC3S/Common Criteria | | |
| 3 | OEM should be ISO 9001-2015 & ISO 27001:2013 Certified. | | |
| 4 | The Firewall appliance should have certifications like NDPP / ICSA / EAL4 or more | | |
| 5 | The product shall have Indian Standard, IC3S/Common Criteria (provided by STQC in India common-criteria- certification-0 ) or Alternatively from International equivalents, NDPP or NSS or ICSALabs, at least one of them should be provided while bidding. | | |

| S.No. | Technical Specification | Compliance (Yes/No) | Offered Parameter |
|---|---|---|---|
| 6 | Certificate of authorization (MAF) for this bid must be submit with bid. Bidders need to submit MAF from respective OEM is mandatory, otherwise authority should have right to cancel the Bidder. | | |
| 7 | The bidder should be ISO certified organization. | | |
| 8 | The bidder should have their own certified technical engineer of quoted product from the respective OEM for installation & warranty support station in Eastern India. The details of the engineer must be furnished with the bid. | | |
| 9 | The bidder should have their registered office in eastern India to ensure immediate support during downtime. | | |
| 10 | During Technical evaluations or Prior to Price bid open, Bidder need to do 7-15 Days POC if asked; POC will be at our premises and during POC if found product is not complying with mentioned requirement than authorities has the right to reject the bid during technical evaluations. | | |

### 21.5.1.2.Specification for 24 Port Layer-2 Managed Switch

| S.No. | Technical Specification | Compliance (Yes/No) | Offered Parameter |
|---|---|---|---|
| | **Make:-** | | |
| | **Model:-** | | |
| 1 | Switch architecture should be Fixed Form factor/ stackable based | | |
| 2 | Switch should have wire-speed, non-blocking and distributed forwarding on all the ports. | | |
| 3 | Switch should have minimum of 12 x 1000 Mbps RJ45, 6x1G SFP(MM), 6x10G SFP+(SM) plus 4 x1/10G SFP+ (MM)uplink ports.<br>Trans receiver module from day one.<br>( All QSFP/SFP+/SFP Transceiver modules should be from same Switch OEM) | | |
| 4 | Switch should support min 16K MAC addresses and min 1000 active VLANs. Switch should support network segmentation that overcomes the limitation of VLANs using VXLAN. | | |
| 5 | Switch should have full Layer 2 features and support spanning tree protocols standards like STP (IEEE 802.1d), MSTP(IEEE 802.1s) RSTP (IEEE 802.1w) etc. LACP/IEEE802.3ad, ACL, QoS and IGMPv1/v2/v3 from day one. | | |
| 6 | Switch should have Static Routing for IPv4 & IPv6 from day1.Switch should support 802.1x authentication and accounting, IPv4 and IPv6 ACLs and Dynamic VLAN assignment. | | |
| 7 | Should support 1K IGMP Groups. | | |
| 8 | Should support 8 queues per port and security protocols like RADIUS, TACACS/TACACS+, AAA & SSH. | | |
| 9 | Switch should be quoted with 5 years direct OEM TAC support and Next Business Day hardware shipment. | | |

| S.No. | Technical Specification | Compliance (Yes/No) | Offered Parameter |
|---|---|---|---|
| 10 | Equipment should be minimum TEC certified or IPV6 Ready Logo Certified. IPV6 Routing & Management features should be active from Day-1. | | |
| 11 | Comprehensive Onsite OEM Warranty for 5 Years | | |
| 12 | All the required licenses for making the Switches fully functional should be bundled | | |

### 21.5.2.1. Specification for Threat Intel Solution

| S.no | Module | Requirement | Compliance (Yes/No) | Offered Parameter |
|---|---|---|---|---|
| 1 | Platform | Vendor must have Minimum 07 years expertise in anti–malware research/Threat Research | | |
| | | Role Based Access Control | | |
| | | Platform should provide the UI in English languages, however, the platform should crawl with multiple language (Eg.(i) Arabic (ii) Chinese (both simplified and traditional script) (iv) Farsi (Persian) (v) French (vi) German (vii) Japanese (viii) Russian (ix) Spanish ) & support Summarization and translation of the information into English Language | | |
| | | The OEM solution must comply to the following certifications:<br>A. ISO/IEC 27001:2013/2022<br>B. ISO 9001 Compliant | | |
| | | Multitenancy | | |
| | | Solution should provide AI summary of ecosystem to help in risk remediation & better decision making | | |
| | | Should provide negligible noise & false positives Signal to Noise Ratio (SNR) > 90% | | |
| | | The Vendor must have a local representative or distributor in the country who is operating locally for at least 5 years. | | |
| | | AI Summary should be provided on executive dashboard help decision making & remediation steps | | |
| | | Single dashboard should provide visibility of all the required usecases | | |

| S.no | Module | Requirement | Compliance (Yes/No) | Offered Parameter |
|---|---|---|---|---|
| | | Platform should use AI algorithm to provide summary of any post, chatter or article on Darkweb & Surface web posted in any language & also assign a risk score on top of that | | |
| | | Vendors' staff assigned to the project must hold professional certifications related to cybersecurity such as: GNFA, GCIH, CISM, CISA, CISSP.(Preferred) | | |
| | | Display the searched data in various types of views such as list view, timeline based view , MAP based view and Source based View | | |
| 2 | Threat Intelligence Feed Requirement | Threat intelligence feed should identify new global threats feeds from it's own Global Sensors and Honeypots network as well along with premium threat intel sources,  including but not limited to Malicious IP Addresses, Domain, URL, Filename, File hash, Email address, Known C&C (Command and Control) hosts, Geolocation feeds like Lat long, AS Number, ISP, Country, etc. | | |
| | | Platform should provide an IOC Lookup feature, where customer will get IOC Risk Score, Confidence Score, Source details, TA profile & IOA | | |

| S.no | Module | Requirement | Compliance (Yes/No) | Offered Parameter |
|---|---|---|---|---|
| | | The solution shall provide information in following categories (if possible):<br>• Brief description of the revealed vulnerabilities, threats, traces of compromise, as well as current cybercriminal and cyberespionage activity against the Customer's assets.<br>• Network Reconnaissance and Vulnerability Analysis<br>• Malware and Cyber–Attack Tracking Analysis<br>• Staff, Data Leakage Analysis<br>• Underground Activities Analysis<br>• WHOIS Analysis<br>• MX Records Analysis<br>• Subdomains Analysis Email addresses Analysis<br>• Social Network Analysis<br>Additional information on detailed technical analysis results. | | |

| S.no | Module | Requirement | Compliance (Yes/No) | Offered Parameter |
|---|---|---|---|---|
|  |  | The solution should allow to search URL's / Domains and provide the following general information:<br>• Status – Shows whether the requested URL can be classified as malicious, good, or not categorized.<br>• IPv4 count – Number of known IP addresses related to the requested URL.<br>• Files count – Number of known malicious / all files.<br>• Created – URL creation date.<br>• Expires – URL expiration date.<br>• Domain – Name of the upper–level domain.<br>• Registration organization – Name of the registration organization.<br>• Registrar name – Name of the domain name registrar.<br>• Owner name – Domain owner name.<br>• Category – Category of the requested URL. |  |  |
|  |  | The solution should allow to search IP addresses and provide the following general information:<br>• Status – Shows whether the requested IP address generates malicious activity.<br>• Hits – Hit number (popularity) of the requested IP address.<br>• First seen – Date and time when the requested IP address appeared in expert systems statistics for the first time<br>• Threat scope – Probability that the requested IP address will appear dangerous (0 to 100).<br>• Owner name – Name of the requested IP address owner.<br>• Owner ID – ID of the requested IP address owner. |  |  |

| S.no | Module | Requirement | Compliance (Yes/No) | Offered Parameter |
|---|---|---|---|---|
| | | • Created – Date when the requested IP address was registered.<br>• Updated – Date when information about the requested IP address was last updated.<br>• Category – Category of the requested IP address | | |
| | | A) In-house Premium Threat Advisories that cover Ransomware Campaigns and TTPs, Threat Actors and their TTPs, APT Groups, Data Breaches, Vulnerability analysis, Malware campaigns<br>B) Solution should provide near real time alerts on Breaches for various Industries & geographies in the form of NewsFlashes on Dashboard | | |
| | | Threat identified with the solution should have (but not limited) the following attributes:<br>• Date of identification<br>• Risk score<br>• Category<br>• Object associated with threat<br>• Threat name (if known)<br>• Threat description<br>Recommendation (if applicable) | | |
| | | Platform should provide the visibility on the Hacktivists and other state sponsored campaigns | | |
| | | Platform should provide OT/ICS Threat Intel feeds with interactive dashboard. | | |

| S.no | Module | Requirement | Compliance (Yes/No) | Offered Parameter |
|---|---|---|---|---|
| | | Platform should have a Threat Library section, providing detailed intel on global Advanced Persistent Threat Groups, Ransomware groups,Threat Actors, Tools they use, their Aliases, IOCs, Country of Origin, Target Industry & Target Geography for effective monitoring and tracking. | | |
| | | The solution must be able to look for if an Exploit or Code is publicly available or underground discussions, alleged selling, or alleged privately held code observed. | | |
| | | Feeds from the platform should be integrated with client soultions like:<br>SIEM, SOAR, TIP, EDR in STIX TAXII format or via Web API | | |
| | | The Threat feeds must be auto updated at least once every 1 hour for IP addresses, once every 2 hours for domains and URLs , once every day for hashes and once every week for CVEs | | |
| | | The Threat feeds must be collected from multiple third party sources both OSINT and paid, deduplicated and then offered to OCAC via API based. integration. | | |
| | | Feeds from the platform should be integrated with client solution's like: SIEM , SOAR, TIP, EDR in STIX TAXII format or via Web API" | | |
| | | The feeds should not be limited to open-source information but should extend to closed (non-public) information | | |
| | | The feeds should not only provide a series of individual data points but also correlate and analyse disparate data points and draw informed conclusions | | |

| S.no | Module | Requirement | Compliance (Yes/No) | Offered Parameter |
|---|---|---|---|---|
| 3 | Cyber-threat monitoring of surface and dark web | Detect if any data is leaked using OCAC's public assets such as Intellectual Properties, Domains, Subdomains, mail-id and OCAC defined keywords. The solution should have the capability to analyse data from multiple languages as mentioned in technical specification | | |
| | | Crawl through dark web forums to identify if there is any data leak from OCAC or if someone is asking information pertaining to OCAC or OCAC assets. | | |
| | | Identify if any of OCAC employee's and assets credentials are leaked or sold online. The system must update the list as and when any new breaches occur and report at the earliest. Moreover, the proposed solution should support customized and automated alerts and reports with information such as IP address, Machine Name, Threat Vector used etc | | |
| | | Monitor the email IDs of OCAC's top executive for any potential credential leaks | | |
| | | Monitor open security forums, like pastebin, GitHub, Open Bug Bounty etc., ingesting data from multiple code sharing and open security forums and report any such code leaks having mention of OCAC or its public assets such as Intellectual Property, Domains, Subdomains, etc | | |
| | | Perform basic level of vulnerability scanning – like open ports, misconfigured SSLs, leaking object storages in public cloud, XSS vulnerabilities and report the same on a daily basis. Scan all Internet-facing infrastructure and identify/ report on critical security issues. Any misconfigured subdomains and IP address must be monitored closely for possible data leakage | | |

| S.no | Module | Requirement | Compliance (Yes/No) | Offered Parameter |
|---|---|---|---|---|
| | | Maintain a comprehensive inventory and fingerprint of all OCAC Internet- facing digital assets such as domains, related subdomains, respective IP addresses, logo, associated web and mobile applications. OCAC shall be able to add to the assets, if so required | | |
| | | Platform should provide the feasibilty to customize the severity logic for alerts & events based on the Threat lanscape of customer | | |
| | | Apart from Portal & emails, event notification should be available on all of the below channels at a desired frequency on Whatsapp/SMS/Mobile app | | |
| | | Monitor data sharing sites like Pastebin, Scribd etc and report any sensitive data associated with the client | | |
| 4 | Darkweb & Deepweb Monitoring | Bidder should provide an early intelligence on the Compromised endpoints, Cookies & Session keys of customer internal application available for sale in Darkweb Marketplaces | | |
| | | Vendor should also provide clear distinction between internal assetss or internal employees & the other stakeholders like customers & partners in the case of exposed credentials | | |
| | | Intelligence provided must have reference to the source of information including Dark web and Deep web and Paste bin sites, either through a direct link to the source or a cached copy without Customer actually going onto Dark web to look for evidence. | | |

| S.no | Module | Requirement | Compliance (Yes/No) | Offered Parameter |
|---|---|---|---|---|
| | | The Platform must be able to create, monitor, automate alert and report for threat on Dark Web but is not limited to, the following:<br>-Employee compromised credentials<br>-Sensitive information Leakage such as Username Password Secret token access keys<br>-Compromised PII such as Email ID, Phone number and Address.<br>-information about the compromised system such as device ID, host name, IP address etc to help in forensic investigation<br>-Malware and Malicious Infrastructure related to Customer domain<br>-Private / Sensitive Documents relating to the business.<br>-Hacking documents/tools specifically targeting client; -Leaked Source Code.<br>-Intellectual property exposed or leaked<br>-Copyright / Trademark infringement.<br>-Technical Information / Data that could be used to compromise corporate systems.<br>- Mentions of IP Addresses and Infrastructure<br>-Use of BIN and other PII serial numbers to identify client-related accounts and credentials.<br>-Stolen / Compromised Login Credentials and Customer Account Information.<br>- Exposure in 3rd Party Breaches | | |

| S.no | Module | Requirement | Compliance (Yes/No) | Offered Parameter |
|---|---|---|---|---|
| | | The platform should incorporate a range of multi-layered monitoring services and analysis techniques and correlates data across a range of resources including:<br>- .onion sites, I2P sites and alternative networks;<br>- Dark Net blogs, forums, chat rooms;<br>- Infostealer Marketplaces, Logs and Cookies<br>- IRC conversations/Discord;<br>- Black market and criminal auction sites<br>- Ransomware forums<br>- Telegram<br>- Discord<br>- Paste sites | | |
| | | Monitor the global list of websites and mobile applications. Monitor domains like .com/ .org/ .co.in/ .in & other domains and alert the moment any website tries to purpurate the OCAC website | | |
| | | Hacktivist tracking and intelligence correlation - understand the Hacktivist world and alert OCAC of any news that has an impact on OCAC | | |
| | | Monitor to identify fraudulent techniques, scams, data trade and vulnerabilities targeting OCAC systems | | |
| | | The provider should be able to provide the facility to analysis the historical data of the threat actor, threat activity, threat objects (historical data of the IPs, URLs, etc. used by the malicious entity) | | |
| | | The solution must display images in the search results from sources such as Twitter, LIVEUAMAP, Ransomware extortion sites such as ALPHV, Arvin Club etc and link it to the current context. | | |

| S.no | Module | Requirement | Compliance (Yes/No) | Offered Parameter |
|---|---|---|---|---|
| | | Platform should provide intelligence from Internet traffic analysis to look for possible exfiltration or C2 extraction from OCAC PUBLIC IP range. | | |
| | | The solution must provide information on IOC with reliability score, detection quality or risk score. Scores must be justified with rational behind the given scores. Scores must be dynamic to represent the automated real-time risk of the said IOC for confident decision making and response. | | |
| | | The solution must be able to look for Exploit Proof of Concepts on selective technologies & sources like Dark Web and Underground forums and help to prevent Zero day exploits. | | |
| 5 | Brand Intelligence | Social Media Monitoring:<br>The platform should monitor all the major social media platform, including, but not limited to;  Twitter, YouTube,LinkedIn & RSS.<br>All data sources should be collectively analysed for the use of Customer's brand. These should be reviewed by bidder's / OEM's Security Analysts, manually verified, and evaluated to determine the extent of any abuse or fraud.<br>If abuse is suspected, Customer should be immediately notified to take the site down or seek to have the post removed via the normal Incident Response channel. | | |

| S.no | Module | Requirement | Compliance (Yes/No) | Offered Parameter |
|---|---|---|---|---|
| | | Fake Customer Service Contact details<br>- Fake Social Media profiles<br>- Fake Domains/URLs and Web pages<br>- Fake recruitment drives & Hiring Scams<br>- Fake Videos or Images using client Logos | | |
| | | Platform should provide :<br>Website Watermarking<br>Website Defacement monitoring | | |
| | | Solution should provide the visibilty of DNS records, Whois records, MX records, screenshot tagged to a typoquatted domain<br>Solution should provide Domain Watchlisting feature, to get instant alert whenever there's a change in the status of domain<br>The platform should be capable of doing Image, OCR and Logo monitoring to identify profile impersonation<br>Finding domains and emails mentions on Code Repository websites like Github etc<br>CXOs fake social media profiles, posts, pages and groups, takedown is also expected here. | | |

| S.no | Module | Requirement | Compliance (Yes/No) | Offered Parameter |
|---|---|---|---|---|
| 6 | Take Down Service | Platform should monitor & do a Takedown of the following cases (including but not limited to):<br>- Phishing sites & Campaigns<br>- Fake Mobile Apps on Appstore, Playstore<br>-  Fake Customer Service Contact details<br>- Fake Social Media profiles<br>- Fake Domains/URLs and Web pages<br>- Fake recruitment drives<br>- Fake Videos or Images using client Logos | | |
| | | The Bidder/OEM should provide take down support for min 500  take downs for the duration of the contract. | | |
| | | Takedown service should be worldwide. | | |
| | | OEM Should have a takedown mechanism natively in their solution either directly or via native platform integration with any 3rd-party services | | |

| S.no | Module | Requirement | Compliance (Yes/No) | Offered Parameter |
|---|---|---|---|---|
| 7 | Attack Surface management | Platform should discover & then monitor the complete Tech Inventory of customer, including but not limited to:<br>— Cloud Buckets<br>— Domains<br>— IPs<br>— IP Ranges<br>— Subdomains<br>— DNS Records (A, AAAA, CNAME, SOA, MX, NS, TXT etc.)<br>— Digital Certificates<br>— Trackers<br>— Keywords<br>— Technologies<br>— Emails<br>— Executives (Cxx / VPs) | | |
| | | Vendor should provide Vulnerability Intelligence which will include:<br>a) Vulnerability source information, extensive references, links to Proof of Concept code and solutions<br>b) Vulnerability Intel on 3rd party software products<br>c) Vulnerability Prioritisation | | |

| S.no | Module | Requirement | Compliance (Yes/No) | Offered Parameter |
|---|---|---|---|---|
| | | The Platform must monitor all of Customer's Public Infrastructure continuously and provide report on<br>• Exploitable Vulnerabilities from known & Unknown assets<br>• CVE/ SSL Expiry<br>• Shadow IT<br>• Sensitive Open Port<br>• Certificate Issues<br>• Misconfigured Devices<br>• The platform must scan the internet for finding RDP, VNC, xserver | | |
| | | Platform should monitor exposed sensitive codes on all of the platforms listed below:(Not Limited to)<br>Github<br>BitBucket<br>Postman<br>Docker Hub | | |
| | | Bidder should have it's own Internet Scanner & data pipeline to monitor the Attack Surface exposure of the customer, it should not be dependent on any 3rd party to provide this service | | |

| S.no | Module | Requirement | Compliance (Yes/No) | Offered Parameter |
|---|---|---|---|---|
| | | Bidder should Provide Public Assets informations like(Not Limited to)<br>*Screenshot<br>*Web Applications details<br>*WAF and CDN Information<br>*Favicon Detect<br>-Vulnerabilities and Critical Open<br>-Virtual Host (Shadow IT Asset)<br>- Local file inclusion<br>-Path Traversal<br>- Default Logins<br>- Web App Misconfigurations<br>- Insecure Design<br>- Broken Authentication | | |
| 8 | Intelligence on CVEs and Vulnerabilities | The solution should be able to create watch list of software tech stack of OCAC and alert for vulnerabilities on the following type of threats<br>a)New critical vulnerability announcement and real-world risk of the vulnerability at Pre-NVD level.<br>b)Trending Vulnerabilities in specific Industries<br>c)Vulnerabilities exploited in the wild by Malwares<br>d)CVEs with low, medium or high potential for exploitation.<br>e)Exploitation has been reported or confirmed to widely occur. | | |
| | | The vulnerability threat intelligence should be bundled with tools to import vulnerability scan results in CSV format. | | |

| S.no | Module | Requirement | Compliance (Yes/No) | Offered Parameter |
|---|---|---|---|---|
| | | The vulnerability solution must have a dashboard view that identifies all types of vulnerabilities with a risk and exploit rating. | | |
| 9 | Intelligence on Leaked Credentials | The solution must provide the following details in respect of a leaked credentials for a given authorized organizational domain for the following:<br>a) Leaked Username or Leaked Email Address<br>b)Full unsalted hashes in encrypted format (eg SHA1, MD5, SHA256, NTLM)<br>c)Clear text password hint (first 2 characters) or full cleartext password to enable credential owner to identify and remediate their use of the exposed password as part of point a)<br>d)Details on applications URL for which the credential works | | |
| | | The solution should provide information about the breach events such as first and last downloaded date , compromise date linked to these dumps (zero or more.) | | |
| | | The solution must offer details around the compromised host such as computer name, OS username, IP Address, File Path of Malware, AV and Host Firewall details, Malware name etc if available with the credential | | |
| | | The solution must provide relevent dashboards to highlight exposure timelines and exposure details like top domains, technologies, dominant malware etc | | |
| | | The solution must have option to restrict view of cleartext password for limited admin users only | | |
| 10 | Threat Analysis | Detailed execution map with highlighted MITRE ATT&CK techniques | | |

| S.no | Module | Requirement | Compliance (Yes/No) | Offered Parameter |
|---|---|---|---|---|
| | | Detect the documents containing client's assetsfor Microsoft Office (Word, Excel, PowerPoint, Publisher, Outlook) and Adobe Reader | | |
| | | Possibility to export the analysis details in STIX, JSON, CSV formats | | |
| | | Network activities (SMB, SMTP, IP, TCP, UDP, DNS, SSL, FTP, IRC, POP3, SOCKS sessions; HTTP(s), requests and responses | | |
| | | Detailed threat intelligence with actionable context for every revealed indicator of compromise (IOC) | | |
| | | The analysis platform should calculate the reputation score of the sample and reveal its genetics and code attribution. This provides insights into the origin of the sample and can enable its attribution to possible authors. | | |
| 11 | Browser Extension Requirements/ Brower Extension Capabilities Requirement | The solution should be offered with a web browser extension for Chrome, Mozilla Firefox and Chromium-based Microsoft Edge that should scan any webpage in real time, identify relevant entities, and presents a list of entities detected along with their risk scores. | | |
| | | The browser extension must highlight the total number of IOCs(IOCs like IP, URL, hash, domain and CVE) are identified on the page with their associated risk scores. IOCs should be highlighted on the page itself using different color codes for criticial, medium and low severity. | | |
| | | Browser extension must ensure that the information is organized in order by risk score Risk score, Triggered risk rules and evidences that assist in prioritization of | | |

| S.no | Module | Requirement | Compliance (Yes/No) | Offered Parameter |
|---|---|---|---|---|
| | | IOCs being shown on the page for reducing triage time for analyst. | | |
| | | The browser extension must have capability to block potentially malicious links on the webpage being reviewed by the analyst | | |
| | | The browser extension must have the option to enable or disable automatic detection of IOCs like IP, Doamin, URL, hash and vulnerability (CVE) | | |
| | | The browser extension must work with the following solutions Anomaly ThreatStream, ArcSight ESM, ELK (Dashboard only), MISP, Qualys, The Hive Project, VirusTotal etc | | |
| | | The browser extnsion must have the capability to export the IOC such as IP, Domains, URLs, Hash files and vulnerabilities into separate CSV files directly from the browser plugin. | | |
| | | The browser extension must have the capability to upload suspicious file URLs for detonation and analysis to OEM offered sandbox solution. | | |

| S.no | Module | Requirement | Compliance (Yes/No) | Offered Parameter |
|---|---|---|---|---|
| 12 | Sandbox (Win, Linux, Mac & Android) | Dynamic Malware Sandboxing should be available:<br>The service should support malware sandboxing by allowing users to<br>a. Upload suspicious files to the platform and download a detailed file behaviour analysis report and network analysis report for each uploaded file<br>b. The analysis report should contain risk score of the file, relevant indicators of compromise such as IP addresses, domains or C2 URLs, suspicious network connections, usage of potentially malicious API and files downloaded or dropped on the disk upon successful execution<br>c. The sandbox should protect organizational privacy by not uploading the file to any publicly accessible repository or third party<br>B. The sandboxing should support operating systems such as Windows at a minimum.<br>C. The service should support automated analysis of at-least 50 samples per day<br>D. The service provider should provide analyst support for report interpretation and explanation as and when required. | | |
| 13 | Reports | All TTPs described in the reports should be mapped to MITRE ATT&CK, enabling proved detection and response through developing and prioritizing the corresponding security monitoring use cases, performing gap analyses and testing current defenses against relevant TTPs | | |

| S.no | Module | Requirement | Compliance (Yes/No) | Offered Parameter |
|---|---|---|---|---|
| | | Intel on threat actor profiles Including suspected country of origin and main activity, malware families used, industries and geographies targeted, and descriptions of all TTPs used, with mapping to MITRE ATT&CK | | |
| | | Should provide technical descriptions about the latest threats during ongoing investigations, before release to the general public | | |
| | | Detailed descriptions of threats targeting financial infrastructures and the corresponding attack tools being developed or sold by cybercriminals on the Dark Web in various geographies | | |
| | | Should provide C Level executive Summarry which includes in grography, Data exfiltration analysis and victim analysis | | |
| | | The report should include conclusions and recommendations too. | | |
| 14 | Training | The OEM of the solution must provide access to unlimited online training to the offered solution including YARA rules. | | |
| | | The course should teach how to write effective Yara rules, how to test them and improve them to the point where they find threats . | | |
| 15 | Support | The solution must be provided with 24/7 access to the support team via web, email and phone | | |
| | | The solution must include Dedicated or shared intelligence analyst from OEM for continuous product usage support and regular reviews | | |

| S.no | Module | Requirement | Compliance (Yes/No) | Offered Parameter |
|---|---|---|---|---|
|  |  | Professonal Service<br>a) Full-time/ part-time “named” threat intelligence analyst services for threat intelligence operations support<br>b) Daily/Weekly Alert Summary and Monthly Executive Summary Reports (if required)<br>c) On-demand Analyst services for threat research and investigations and custom reports |  |  |

### 21.5.2.2.Specification for Threat Integration Platform

| S.no | Module | Requirement | Compliance (Yes/No) | Offered Parameter |
|---|---|---|---|---|
| | Threat Intel Sharing Platform Capabilities | To establish a comprehensive on premise Threat Intelligence Sharing Platform solution to consume threat intel information from commercial and OSINT threat intel sources including but not limited to CERT-In, NCIIPC etc and provide STIX/TAXII based URL output for consumption into OCAC owned and managed security devices such as NGFW, Web Proxy, IPS, AV, EDR, NDR, SIEM, SOAR, etc. . | | |
| | | The solution should be integrated with multiple threat commercial/OSINT feeds/risk lists from day one. The commercial feed integration steps should be thoroughly documented both by the proposed \platform solution and by the commercial Threat Feed OEM on their respective websites or support portal/knowledgebase. | | |
| | | The proposed Threat Intelligence Sharing Platform must be a commercial Solution and should be modified to the extent of capabilities asked by OCAC as and when required during the duration of the project. | | |
| | | The offered solution must provide threat feed integration with major Next Generation Firewall Provider(NGFW) , EDR/AV, McAfee Web Gateway and SIEM from day one (not limited to mentioned brands). Additional integration with other cyber security solution is in scope of bidder however bidder must factor minimum 30 man days for future customization and integrations. | | |

| S.no | Module | Requirement | Compliance (Yes/No) | Offered Parameter |
|---|---|---|---|---|
| | | The platform should support Threat Intelligence Collection, Evaluation, Ingestion, Processing, Translation, Prioritization, Integration & Aggregation and real time Dissemination. | | |
| | | The platform should support machine readable threat intelligence sharing with no limit on the number of users and devices of OCAC. The solution must support sharing of intelligence, including atomic IOCs, URLs, CVE, hash values etc for consumption by security devices such as NGFW, Web Proxy, IPS, AV, EDR, NDR, SIEM, SOAR, etc. | | |
| | | The solution must support sharing of all types of threat entity supported, including commercial third-party bulletins, IOCs, events, campaigns, actors, and bulletins, signatures, with no loss in fidelity between the original document and the copy received by each stake holders | | |
| | | The solution must support out of the box integration with multiple external threat intelligence sources including but not limited to sources such as MISP / TAXII servers, industry-led (ISAC's), sectorial CERTs, Vendor /OEM CERTs, Government (CERTs) and other partners. | | |
| | | The solution must provide for creating and maintaining IoC and indicators database allowing to store technical and non-technical information about malware samples, incidents, attackers and intelligence. | | |
| | | The solution should provide for automatic correlation to help finding relationships between attributes and indicators from malware, attacks campaigns or | | |

| S.no | Module | Requirement | Compliance (Yes/No) | Offered Parameter |
|---|---|---|---|---|
| | | analysis. There should be provision to enable of disable Correlation on per event or per attribute basis. | | |
| | | The solution should provide for a flexible data model where complex objects can be expressed and linked together to express threat intelligence, incidents or connected elements. | | |
| | | The solution must provide for an intutive web interface accesible via common wed browsers such as Google Chrome, Mozilla Firefox, Microsoft Edge and Safari. | | |
| | | The web interface must allow end-users to create, update and collaborate on events and attributes/indicators. | | |
| | | A graphical interface should allow for an option to navigate seamlessly between events and their correlations. An event graph functionality should also be provided to create and view relationships between objects and attributes. | | |
| | | The solution should provide for advanced filtering functionalities and warning list to help the analysts to contribute events and attributes. | | |
| | | The solution should provide options for analyst to collaborate on events and attributes to propose changes or updates to attributes/indicators. | | |
| | | The solution should have an out of box feed import capability to import and integrate any threat intel or OSINT feed from third parties. OSINT feeds and commercial feeds should be integrated from day one for OCAC to provide feeds like C2 communicating IPs, | | |

| S.no | Module | Requirement | Compliance (Yes/No) | Offered Parameter |
|---|---|---|---|---|
| | | weaponized domains, Log4Shell Potentially Malicious Scanners, Log4Shell Related Scanners, hash info of Recently Active Targeting Vulnerabilities in the Wild, CVE information which are Exploited in the Wild by Recently Active Malware, etc | | |
| | | The solution should have adjustable taxonomy to classify and tag events following custom classification schemes or existing taxonomies. The solution should have a default set of well-known taxonomies and classification schemes to support standard classification as used by ENISA, Europol, DHS, CSIRTs or many other organisations. | | |
| | | The solution must provide option to export the data in various formats such as IPS/IDS Formats (Suricata, Snort and Bro etc), OpenIOC, plain text, CSV, MISP XML and JSON output to integrate with other systems (network IDS, host IDS, custom tools) | | |
| | | The solution must provide for bulk-import, batch-import, free-text import, import from OpenIOC, STIX 2.0(or later), TAXII, ThreatConnect CSV or MISP format. | | |
| | | The solution must support import of human-generated structured data including XLS or CSV via the UI. The solution must support import of machine-generated structured data such as JSON or XML via an API | | |
| | | The solution must have integrated encryption and signing of the notifications via PGP and/or S/MIME depending of the user preferences. | | |

| S.no | Module | Requirement | Compliance (Yes/No) | Offered Parameter |
|---|---|---|---|---|
| | | The solution must support the import of threat intelligence that is stored locally and privately, without any storage in the SaaS service or any external system | | |
| | | The solution must support receipt, creation, and editing of STIX threat entities including -Campaigns, malware, Threat Actors, Incidents, Signatures, Reports, - ATT&CK TTPs and other threat entities supported by latest STIX standards. | | |
| | | The solution must be able to store at least 15 million IOCs including historical across a range of indicator Types, including IP Addresses [v4 & v6], Domains, URLs, File Hashes, email addresses. | | |
| | | The solution must be able to receive and store at least 5,000 events per second from a typical mix of event sources, with an efficient storage mechanism. The solution must be able to store the specified event and IOC volumes for a retention period of one year. The solution must be able to match newly-received IOCs against old events, and newly-received events against old IOCs, where 'old' is up to the one-year retention period. The solution must be able to identify new matches against historic data in near-real-time. | | |
| | | The solution must automatically de-duplicate threat intelligence. The solution must automatically detect and remove false positives | | |

| S.no | Module | Requirement | Compliance (Yes/No) | Offered Parameter |
|---|---|---|---|---|
| | | The solution must include applications to integrate and manage a data feed from the solution to a downstream SIEM. The solution must permit user-definable filters to determine which new intelligence is synchronised to the downstream security system, such as a minimum confidence score or a specific tag. The solution must be able to limit the number of IOCs sent to a control with limited capacity, and automatically prioritise the IOCs to be sent up to this limit. | | |
| | | The webUI must also have an option to search the commercial threat feed OEM directly regarding any IOC and get details like the risk score, related conetext etc without the need to visit the commerical OEM website. | | |
| | | The solution must allow the user to query an IOC and see all matching events and flows within the UI. The solution should allow the user to query an IOC tag and see all events and flows that match IOCs possessing that tag, within the UI. | | |
| | | The solution should be able to provide context around relevant IOCs, such as whether a domain is a Dynamic DNS, on a shared hosting platform, a sinkhole, etc. The solution must be able to show all reporting sources for any given IOC, together with any context they provide such as tags, dates, and confidence scores. The solution must allow OCAC to utilize the it's API to integrate and / or automate data processing using scripts and/or other data stores. | | |
| | | The commercial and OSINT threat feeds once ingested into the solution must display vendor generated tags | | |

| S.no | Module | Requirement | Compliance (Yes/No) | Offered Parameter |
|---|---|---|---|---|
| | | such as current risk score, severity level, OEM triggered risk rules etc | | |
| | | The solution should have Workflow-based automation to perform automation around ad hoc or routineThreat Intel use cases. The solution should be able to trigger automation based on tasks such as analysis, enrichment, validation and any other steps involved in the threat intelligence management process. | | |
| | | The solution must automatically 'age out' indicators in enterprise integrations. The solution should be able to provide a risk or threat score to assist in prioritisation, based on the nature of the threat and the confidence of the indicator detected in the organisation. The solution should support a wide range of integrated products 'out of the box', without the need of extensive custom development for integration, so as to provide a seamless on boarding experience for each member. | | |
| 14 | Training | OEM should provide the training on usability of Platform | | |
| 15 | Support | The solution must be provided with 24/7 access to the support team via web, email and phone | | |
| | | The solution must include Dedicated or shared intelligence analyst from OEM for continuous product usage support and regular reviews | | |

**21.5.2.3.Specification for Web Application Scanning (WAS) Tool**

| S.No. | Minimum Technical Specifications | Compliance Yes/No | Offered Parameter |
|---|---|---|---|
| 1 | The proposed solution should support (DAST) dynamic application security testing. The proposed solution should be deployed on premise with unified/single console & Web application scanning solution as part of this RFP. | | |
| 2 | The proposed solution should specify and explain the proposed licensing model for this solution (DAST) dynamic application security testing. | | |
| 3 | The proposed solution should propose scanner deployment with the ability to deploy unlimited on-prem scanners at no additional cost. | | |
| 4 | The proposed solution should be CVE-compatible and provide at least 10 years of CVE coverage. | | |
| 5 | The proposed solution should track: The Open Web Application Security Project (OWASP) Top 10 number, the Common Weakness Enumeration (CWE) number, and the Web Application Security Consortium (WASC) classification, as applicable. | | |
| 6 | The proposed solution should propose free online on demand training curriculum/courses. | | |
| 7 | The proposed solution must support multi-fqdn scanning. | | |
| **Architecture** | | | |
| 1 | The proposed solution should propose unified console for Web App Scanning procured under this RFP. | | |
| 2 | The proposed solution should be deployed on premise. | | |
| 3 | The proposed solution should offers on premise scanners. | | |
| 4 | The proposed solution should propose scanners that are either self managed or managed by the platform for actions like e.g. updates to vulnerability signatures, code, and other updates. | | |

| S.No. | Minimum Technical Specifications | Compliance Yes/No | Offered Parameter |
|---|---|---|---|
| 5 | The proposed solution should provide a comprehensive API for automation of processes and integration with 3rd party applications . | | |
| 6 | Data should be retained for 180 days in the tool | | |
| **Authentication** | | | |
| 1 | The proposed solution should propose advanced authentication support, such as form based authentication, cookie-based authentication, NTLM support, and Selenium-based authentication, to address most web application requirements. | | |
| 2 | The proposed solution should highlight and analyze vulnerabilities directly in the web app for quicker analysis. | | |
| 3 | The proposed solution should support Browser Extension to helps easily create and manage web application scans, including setting up authentication for web application scanning. | | |
| 4 | The proposed solution should record authentication flows from within your browser to save time. | | |
| **Scanning** | | | |
| 1 | The proposed solution should support multiple geographically distributed scanning engines managed by a central console. | | |
| 2 | The proposed solution should be able to scan both internal and external web applications. | | |
| 3 | The proposed solution should have options for a "quick scan" to get started, determine correct functioning, and so on, versus a deep full scan. | | |
| 4 | The proposed solution should scan and Identify web application vulnerabilities - internally and externally facing. | | |
| 5 | The proposed solution should propose a simple scan setup and management. | | |
| 6 | The proposed solution should propose safe scanning of Web Applications. | | |

| S.No. | Minimum Technical Specifications | Compliance Yes/No | Offered Parameter |
|---|---|---|---|
| 7 | The proposed solution should scan all of applications, including those built using modern web frameworks, such as JavaScript, AJAX, HTML5 and Single Page Applications(Not Limited to) | | |
| 8 | The proposed solution should deliver highly accurate results with minimal false positives and negatives, giving you and your developers confidence that your reports are accurate. | | |
| 9 | The proposed solution should propose automated Web Application Scanning. | | |
| 10 | The proposed solution should rapidly detect cyber hygiene issues. | | |
| 11 | The proposed solution should have capabilities for human-assisted crawling of the application so the scanner can better understand authentication flow. | | |
| 12 | The proposed solution should propose frequent and automated scans. | | |
| 13 | The proposed solution should reduce product sprawl. | | |
| 14 | The proposed solution should identify the relevant Web page and URL where the vulnerability was detected. | | |
| 15 | The proposed solution should have options to reduce the risk that minimum disruptions to service are caused when testing/performed against production applications. | | |
| 16 | The proposed solution should reduce manual work efforts. | | |
| 17 | The proposed solution should propose a high-level scan that analyzes HTTP security headers and other externally-facing configurations on a web application to determine if the application is compliant with common security industry standards. | | |
| 18 | The proposed solution should do rapid security assessments. | | |
| 19 | The proposed solution should detect improperly issued or soon-to-expire SSL/TLS certificates | | |
| 20 | The proposed solution should cover the OWASP Top 10 categories. | | |
| 21 | The proposed solution should propose 3rd-party component scanning. | | |

| S.No. | Minimum Technical Specifications | Compliance Yes/No | Offered Parameter |
|---|---|---|---|
| 22 | The proposed solution should propse scan progress indicators: Percentage, Estimate, Progress Bar. | | |
| 23 | The proposed solution should propose actionable remediation instructions in a language developers understand. | | |
| **Visibility and Reporting** | | | |
| 1 | The proposed solution should include customizable graphical and list based dashboards elements for displaying vulnerabilities and status of the assessed environment. | | |
| 2 | The proposed solution should propose easily verify vulnerabilities with proof and output reporting. | | |
| 3 | The proposed solution should propose the OWASP Top 10 categories report and dashboard. | | |
| 4 | The proposed solution should support the ability to produce reports in the following report formats: CSV & PDF. | | |
| 5 | License to be Provided No .of FQDNs- Minimum 1000 FQDNs | | |

## 20.3. Payment Schedules for Package – II

| Sl. | Project Milestone | Payment (%) | Documents Required |
|---|---|---|---|
| 1 | Delivery of Solution | 60% of the contract value | 1.Original Delivery Challan |
| | | | 2. Required License in the Name of OCAC |
| 2 | Installation, Configuration, Integration & UAT | 30% of the contract value | 1.Installation Certificate duly certified by Nodal officer nominated by OCAC |
| | | | 2. Successful UAT certified by Nodal officer nominated by OCAC |
| 3 | Training (Knowledge Transfer) | 10% of the contract value | To be released in 5 installments after successful completion of Training by OEM for each tool each year for the period of 5 Years |
| | | | Bidder should organize the training from OEM after Installation, Configuration, Integration & UAT |
| 4 | Operation and Maintenance Support | 100% of O&M Cost | To be released in 10 installments after completion of each 6 months for a period of 5 Years |
| | | | The O&M date will start after the successful completion of Installation, Configuration, Integration completion & UAT |
| | | | Submission of Successful O&M completion document certified by Nodal officer nominated OCAC |

## 21.8.2. Form 8: Financial Proposal Package – I

| Sl. No. | Item Description | Qty | Unit | Base Product Cost Including 5 Years OEM Support | Base Installation cost | Total Cost (Excluding Tax) | GST Charges as applicable | Total Product Cost (Including GST) |
|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7= (5+6)*3 | 8 | 9= 7+8 |
| 1 | Firewall (NGFW) in High Availability (HA) (Fully populated from day 1) | 02 | Nos | | | | | |
| 2 | L2 Network Switch 24Port (Fully Populated from day 1) | 01 | Nos | | | | | |
| 3 | Optical Patch Cable, OM4 Multi-modemode,Duplex LC-LC,10 meters (Commscope / Panduit /Molex) | 20 | Nos. | | | | | |
| 4 | Optical Patch Cable, OM4 Multi-modemode,Duplex SC-LC,10 meters (Commscope/Panduit/Molex) | 20 | Nos. | | | | | |
| 5 | CAT6 UTP Patch Cord – Factory Crimped,3 meters(Commscope / Panduit /Molex) | 20 | Nos. | | | | | |
| 6 | CAT6 UTP Patch Cord – Factory Crimped,10 meters (Commscope/Panduit/Molex) | 10 | Nos. | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| 7 | **Total** | | | | | |
| **Grand Total Cost (Amount quoted in words) : - Rupees** | | | | | | |

***Authorized Signatory with Official Seal***

**NOTE :-**

- Prices shall be quoted inclusive of all taxes, duties, freight and forwarding and cost of labour for installation in Indian Rupees i.e INR
- Printed brochures of items quoted should be enclosed.
- The bidder should mention the warranty period against all manufacturing defects.
- In case of any discrepancy between Unit Price & Total Price, the Unit Price will prevail.